

**KASPERSKY**

**Kaspersky  
Industrial CyberSecurity:  
программы обучения и повышения  
осведомленности**



[www.kaspersky.ru/ics](http://www.kaspersky.ru/ics)

В рамках инновационных образовательных программ «Лаборатория Касперского» делится экспертными знаниями и опытом в сфере информационной безопасности промышленных систем, а также уникальными сведениями о киберугрозах для АСУ ТП.

Около 80% всех инцидентов безопасности вызвано человеческим фактором. Если в результате инцидента происходят повреждение критически важных систем или полная остановка производственных процессов, такие ошибки могут привести к значительным тратам и представлять опасность для жизни и здоровья людей.

В современной среде, где ландшафт угроз непрерывно эволюционирует, а объем целевых атак, использующих человеческий фактор, растет, одна из лучших мер защиты – автоматическое соблюдение сотрудниками правил безопасности.

Чтобы добиться этого, нужно, чтобы все сотрудники владели базовыми знаниями о киберугрозах и навыками безопасной работы. Специалисты, напрямую занятые защитой информационных и производственных систем (ИТ/ОТ), должны к тому же уметь эффективно управлять рисками кибербезопасности, выявлять и предотвращать инциденты и устранять угрозы.

Программы обучения и повышения осведомленности Kaspersky Industrial CyberSecurity созданы, чтобы помочь операторам критических инфраструктур, поставщикам сервисных услуг и производственным предприятиям препятствовать сбоям и повреждениям промышленных систем в результате инцидентов информационной безопасности и кибератак.

## ОБУЧАЮЩИЕ ПРОГРАММЫ

Программа повышения осведомленности о киберугрозах	Программы обучения и развития навыков в области кибербезопасности	
Для инженеров/рабочих на производстве:	Для специалистов по ИТ/ОТ:	Для специалистов по безопасности ИТ/ОТ:
Базовые навыки в области кибербезопасности	Кибербезопасность современных промышленных систем	Тестирование на проникновение в АСУ ТП для специалистов
Для руководителей:		Цифровая криминалистика в АСУ ТП для специалистов
Игровые тренинги по промышленной кибербезопасности		

## ОСВЕДОМЛЕННОСТЬ О КИБЕРУГРОЗАХ В ПРОМЫШЛЕННОЙ СРЕДЕ

Для учебных программ используются интерактивные модули очного и онлайн-обучения, а также игровые тренинги для всех рядовых сотрудников, линейных менеджеров и руководителей, которые взаимодействуют с промышленными компьютерными системами.

Сегодня организации тратят миллионы, чтобы повысить осведомленность сотрудников о киберугрозах, но руководители департаментов информационной безопасности редко остаются довольны результатами. Почему так происходит?

Большинство соответствующих тренингов носят общий характер, затянuty, изобилуют техническими подробностями или фокусируются на негативных аспектах. Эти программы не учитывают способность самостоятельно принимать решения и учиться и в результате оказываются неэффективными. К тому же они не отражают реальных угроз кибербезопасности, с которыми сталкиваются сотрудники промышленных предприятий.

Зная об этом, организации ищут более совершенные подходы, которые стимулировали бы правильное поведение сотрудников и были направлены на решение проблем, типичных для конкретной среды. Только такие подходы обеспечивают ощутимую и измеримую пользу от инвестиций в обучение.

Обучающие программы «Лаборатории Касперского» по повышению осведомленности в области промышленной кибербезопасности эффективны, поскольку:

- Направлены на изменение поведения. Они поощряют стремление каждого сотрудника к безопасной, ответственной работе. В результате создается корпоративная среда, в которой соблюдение правил кибербезопасности является естественной частью работы.
- Сочетают мотивирующие приемы, игровой подход и другие методы обучения, а также имитацию атак, основанную на реальных ситуациях в промышленных средах, и интерактивные тренинги для формирования навыков кибербезопасного поведения.

### ПОДРОБНОЕ ОПИСАНИЕ

#### **Глубина охвата и ясность изложения.**

Обучение охватывает широкий ряд проблем безопасности: от базовых правил безопасной работы до атак с использованием вредоносного ПО. Поднимаются вопросы утечки данных и безопасного использования социальных сетей. Для обучения применяется набор простых упражнений.

Чтобы сделать процесс обучения интересным и актуальным, мы используем разнообразные дидактические методы: работу в группах, интерактивные модули и игры на основе реальных сценариев из промышленной среды.

**Гибкий формат.**

Однодневный курс повышения осведомленности о киберугрозах можно изучать на территории предприятия или на любой другой площадке, а игровые тренинги по промышленной кибербезопасности Kaspersky Industrial Protection Simulation (KIPS) доступны в очной форме и онлайн. Чтобы создать учебную среду, максимально приближенную к реальной, мы подготовили отдельные варианты KIPS для различных отраслей, например водоочистой и энергетической.

**Непрерывная мотивация.**

Создаем благоприятные условия для обучения за счет игрового и соревновательного подхода, а затем закрепляем материал в течение года, моделируя атаки через интернет и проводя оценочные и образовательные кампании.

**Изменение убеждений.**

Сотрудники, которые прошли наши программы, осознают, что тоже играют важную роль в защите организации от конкретных угроз: они понимают, как не стать жертвой, подвергнув себя и свое рабочее место опасности или открыв злоумышленнику доступ для атаки.

**Развитие корпоративной культуры безопасности.**

Готовим руководителей к тому, чтобы возглавить борьбу за безопасность. Для построения корпоративной среды, в которой кибербезопасность разумеется сама собой, нужен личный пример руководства, а не попытки навязать правила.

**Позитивный подход и совместная работа.**

Показываем, как соблюдение правил кибербезопасности повышает эффективность и продуктивность работы всей организации и помогает улучшить сотрудничество с другими отделами, в том числе службами безопасности информационных и производственных систем.

**Измеримость.**

Предоставляем инструменты для измерения навыков сотрудников и проводим оценку на корпоративном уровне, анализируя отношение коллектива к кибербезопасности в повседневной работе.

## **ОБУЧЕНИЕ И РАЗВИТИЕ НАВЫКОВ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ**

Эти курсы охватывают широкий ряд тем по кибербезопасности, напрямую занятых защитой промышленных систем и технологий. Все курсы проводятся в региональных офисах «Лаборатории Касперского» либо на территории заказчика.

Участники приобретают практические навыки и знания в сотрудничестве с экспертами мирового класса, которые делятся собственным опытом прогнозирования, предотвращения, обнаружения и устранения киберугроз.

Курсы включают как теоретические, так и практические лабораторные занятия. По завершении каждого курса участники могут пройти сертификацию для подтверждения своего уровня знаний.

## РОСТ УРОВНЯ ЭКСПЕРТНЫХ ЗНАНИЙ В ОРГАНИЗАЦИИ

Предлагаемые курсы позволяют организациям повышать уровень знаний в области кибербезопасности по трем основным направлениям:

- основы кибербезопасности АСУ ТП;
- тестирование на проникновение в АСУ ТП;
- цифровая криминалистика в АСУ ТП.

### Кибербезопасность современных промышленных систем

Позволяет специалистам по IT/OT лучше понять ландшафт угроз и векторы атак, направленных на промышленную среду, и вооружает практическими рекомендациями по внедрению эффективных средств защиты АСУ ТП.

### Тестирование на проникновение в АСУ ТП для специалистов

Обучает специалистов по защите IT/OT выполнять тщательное, всестороннее тестирование на проникновение в промышленных средах и подготавливать экспертные рекомендации по устранению последствий атак.

### Цифровая криминалистика в АСУ ТП для специалистов

Обучает специалистов по защите IT/OT проводить эффективную криминалистическую экспертизу в промышленных средах, а также выполнять анализ и подготавливать рекомендации на экспертном уровне.

## ПОДРОБНАЯ СТРУКТУРА ПРОГРАММ ОБУЧЕНИЯ

Темы	Продолжительность	Результаты/навыки
<b>Кибербезопасность современных промышленных систем</b>		
<ul style="list-style-type: none"> <li>• Обзор существующего ландшафта угроз, проблем безопасности, проявлений человеческого фактора, сетевых атак на АСУ ТП.</li> <li>• Сетевая безопасность IT-систем и АСУ ТП: особые соображения.</li> <li>• Практический пример, демонстрирующий использование методов предотвращения, обнаружения и устранения угроз.</li> <li>• Соответствие промышленным стандартам и правовым нормам.</li> <li>• Топологии сетей и принципы работы технологий сетевой безопасности.</li> <li>• Роли и структура рабочих групп по кибербезопасности.</li> <li>• Распространенные ошибки в области кибербезопасности.</li> </ul>	1–2 дня	<ul style="list-style-type: none"> <li>• Понимание существующего ландшафта киберугроз для промышленных сред и методов борьбы с атаками, направленными на вашу отрасль или организацию.</li> <li>• Идентификация и выявление инцидентов информационной безопасности.</li> <li>• Проведение простых расследований.</li> <li>• Составление и осуществление эффективного плана реагирования на инциденты.</li> </ul> <p>Программа содержит тщательно отобранные компоненты и адаптируется для проведения в течение 1 или 2 дней.</p> <p>Участники могут получить сертификаты.</p>

Темы	Продолжительность	Результаты/навыки
<b>Тестирование на проникновение в АСУ ТП для специалистов</b>		
<ul style="list-style-type: none"> <li>• Знакомство с компонентами, типами архитектуры и развертыванием АСУ ТП в различных отраслях, включая следующие:               <ul style="list-style-type: none"> <li>– выработка и распределение электроэнергии;</li> <li>– добыча нефти и газа;</li> <li>– транспортировка.</li> </ul> </li> <li>• Практические методы тестирования на проникновение в АСУ ТП в этих и других отраслях.</li> <li>• Составление плана тестирования на проникновение в АСУ ТП: соображения и ограничения.</li> <li>• Сбор информации.</li> <li>• Анализ уязвимостей в системах SCADA и ПЛК.</li> <li>• Анализ результатов и подготовка отчетов.</li> <li>• Практические лабораторные работы.</li> </ul>	5 дней	<ul style="list-style-type: none"> <li>• Понимание уязвимостей АСУ ТП и умение их анализировать.</li> <li>• Умение составлять эффективный план тестирования на проникновение в АСУ ТП.</li> <li>• Умение выполнять безопасное и эффективное тестирование на проникновение в SCADA, ПЛК и другие элементы АСУ ТП.</li> <li>• Умение подготавливать экспертные рекомендации по устранению последствий угроз.</li> </ul> <p>Участники могут получить сертификаты.</p>
<b>Цифровая криминалистика в АСУ ТП для специалистов</b>		
<ul style="list-style-type: none"> <li>• Знакомство с компонентами, типами архитектуры и развертыванием АСУ ТП в различных отраслях, включая следующие:               <ul style="list-style-type: none"> <li>– выработка и распределение электроэнергии;</li> <li>– добыча нефти и газа;</li> <li>– транспортировка.</li> </ul> </li> <li>• Идентификация проблем и ограничений АСУ ТП.</li> <li>• Методы цифровой криминалистики в применении к АСУ ТП.</li> <li>• Составление плана криминалистической экспертизы в АСУ ТП.</li> <li>• Ручной сбор и сохранение данных для проведения криминалистической экспертизы: работа с протоколами ОСПВ и АСУ ТП.</li> <li>• Анализ артефактов и проверка отклонений.</li> <li>• Подготовка отчетов.</li> <li>• Практические лабораторные работы.</li> </ul>	4 дня	<ul style="list-style-type: none"> <li>• Выполнение эффективной криминалистической экспертизы в АСУ ТП.</li> <li>• Составление эффективного плана криминалистической экспертизы в АСУ ТП.</li> <li>• Сбор физических и цифровых улик и их правильная обработка.</li> <li>• Применение средств и инструментов цифровой криминалистики к SCADA и ПЛК.</li> <li>• Выявление следов вторжения посредством анализа обнаруженных артефактов.</li> <li>• Воссоздание хронологической картины инцидентов с помощью меток времени.</li> <li>• Умение подготавливать экспертные отчеты и действенные рекомендации.</li> </ul> <p>Участники могут получить сертификаты.</p>



Решения для защиты крупного бизнеса: [kaspersky.ru/enterprise](https://kaspersky.ru/enterprise)

© АО «Лаборатория Касперского», 2017. Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.