



г. Нур-Султан, пр. Мангилик ел С 3.5, 4 этаж  
+7 (7172) 47-84-13  
info@cybersec.kz

## КОММЕРЧЕСКОЕ ПРЕДЛОЖЕНИЕ

**ТОО «KazHackStan»** - одна из ведущих организаций в области информационной безопасности в Центральной Азии. Организация за время своего существования завоевала признание специалистов по информационной безопасности по всему миру.

Организация предоставляет широкий спектр услуг в области оценки защищенности, в том числе проведение аудитов ИБ и тестирований на проникновение, анализ защищенности банковских систем и бизнес-приложений, веб приложений, информационных инфраструктур.

Более 70 экспертов. Эксперты «KazHackStan» обладают сертификатами OSCP, OSWP, CNFI, CISA, CCNA Security, ISO 27001—2013, OSCE и СЕН и регулярно принимают участие в международных конференциях, таких как PHDays, ZeroNights, Инфофорум, КодИБ.

Эксперты организации являются авторами публикаций на таких ресурсах как журнал Хакер, NabraHabr, DigitalReport, ProfIT.kz и др.

Наша команда занимала призовые места в соревновании The Standoff на международной конференции по информационной безопасности PositiveHackDays с 2017 по 2020 года.

## СПЕЦИФИКАЦИЯ

### Курс «Кибербезопасность АСУ ТП»

№	Наименование курса	Примечание	Цена за одного чел., тенге (без НДС)
1	Курс «Кибербезопасность АСУ ТП»	За одного слушателя	<b>140 000</b>

#### О курсе:

Первый, не имеющий аналогов в Казахстане, авторский курс по кибербезопасности АСУ ТП. Курс знакомит слушателей с современным подходом в обеспечении безопасной эксплуатации автоматизированной системы управления технологическим процессом (АСУ ТП) на предприятии.

В ходе курса слушатели знакомятся с аспектами информационной безопасности АСУ ТП, для поддержания необходимого уровня безопасности и непрерывности производства.

**Главный тренер:** Виталий Перов – эксперт по аудиту промышленных IT систем, имеет опыт проектирования, разработки, эксплуатации. Обладатель сертификатов от ведущих

производителей промышленных решений Emerson, Wonderware, Schneider Electric, Siemens. Участник международных соревнований The Standoff. Специалист по кибербезопасности в «KazHackStan». Специализируется по аудиту систем на уязвимости. Имеет опыт работы в нефтегазовой и горно-обогатительной сфере.

**Целевая аудитория:**

Курс предназначен для сотрудников подразделений безопасности, руководителей и специалистов подразделений, отвечающих за обеспечение безопасности и техническую поддержку АСУ ТП. Для выпускников\студентов последних курсов (ИТ/ИБ/АСУ), технический и ИТ персонал предприятий.

**Цель курса:** увеличить осведомленность об угрозах и методах защиты критической инфраструктуры.

**Результат обучения:** по итогам курса учащиеся овладеют навыками:

- ориентироваться в ключевых аспектах обеспечения безопасности АСУ на предприятии, основных угрозах и уязвимостях;
- грамотно подходить к выбору и использованию доступных на рынке продуктов и инструментов;
- проектировать безопасную сетевую архитектуру АСУ и расставлять приоритеты для защиты;
- базовые навыки аудита систем АСУ;
- приобретенные знания будут полезны при прохождении собеседования на позиции в таких компаниях как ТШО\КПО\НСОС и пр.

**Форма обучения:** онлайн курс.

**Периодичность проведения курса:** 2 дня.

**Продолжительность:** 7 академ. часов.

**Дополнительная информация:** Курс включает:

- live демонстрацию атак на технологический процесс на реальной SCADA системе
  - Использованию NG файрволов для защиты промышленных протоколов
  - Примеры использования систем и методов защиты критической инфраструктуры
- Неинвазивные методы аудита

**Документ об окончании курса:** Сертификат о прохождении курса: **Курс «Кибербезопасность АСУ ТП».**

**Директор ТОО «KazHackStan»**



**Сатиев О.Ш.**

**Программа**  
**Курс «Кибербезопасность АСУ ТП»**

Модуль 1 Архитектура и текущие угрозы

Модуль 2 Стандарты и рекомендации

Модуль 3 Практика: примеры атак

Модуль 4 Оценка риска и аудит

Модуль 5 Методы защиты

Модуль 6 Практика: применение защитных инструментов

За дополнительной информацией обращаться:

*Баян Оразгалиева*

*87076028997*

*bo@cybersec.kz*