«КИБЕРБЕЗОПАСНОСТЬ НА ПРЕДПРИЯТИИ»

Рассматриваем ключевые векторы — от открытых данных и внешнего периметра до внутренних систем и цепочки поставок, переводя последствия и результаты в язык финансовых показателей.

26-27 марта 2026, Москва

Тема 1. Роль и место подразделения информационной безопасности в организации.
Обзор законодательства в области информационной безопасности. Требования нормативных документов для бизнеса, последствия их нарушения. Дорожная карта по минимизации рисков.

Тема 2. OSINT: открытые данные как источник риска.
Входные точки для атаки. Как из публичных источников злоумышленник собирает профиль компании и находит цель. «Живые» примеры поиска чувствительной информации о любой компании, ее влияние на безопасность организации.

Тема 3. Периметр компании: цифровые двери, которые всегда проверяют первыми.
Что видит злоумышленник снаружи, какие сервисы чаще всего становятся входом и как это конвертируется в деньги.
Моделирование ситуации со стороны злоумышленника, публично доступная информация для проведения атак, наиболее часто используемые бреши для получения доступа к внутренней сети.

Тема 4. Социальная инженерия: атака на сотрудников как бизнес-актив.
Сотрудники предприятия - ключевое звено атаки, связанные финансовые потери (кейсы, фишинг). Цифровая гигиена -количественное и качественное представление о роли цифровой гигиены в компании, принятие необходимых мер, оценка полноты внедренных мер.

Тема 5. Рынок кибератак.
Как работает «атака как сервис». Соотношение стоимости реализации атаки и ее последствий, и тех минимальных мерах, внедрение которых позволит сделать этот баланс наименее привлекательным для злоумышленника.
Тенденция удешевления взлома с удорожанием восстановления нанесенного ущерба, рост прямых убытков и скрытых расходов.

Тема 6. Внутренний взгляд: как атака развивается внутри компании.
Внутренний пентест: алгоритм действий хакера после первого входа.
Логика атакующего внутри сети: развитие атаки, повышение привилегий и доступ к критическим системам (1С, Банк-клиент и прочие).
Базовые меры информационной безопасности, усложняющие работу злоумышленника.

Тема 7. Аппаратный хакинг и физический доступ: слабые звенья в инфраструктуре организации.
USB, IoT, RFID и другие простые методы обхода защиты, которые могут дорого обойтись бизнесу. Нестандартные, но при этом не менее опасные угрозы, которые часто упускаются из виду внутри сети организации, даже с достаточно зрелым уровнем информационной безопасности.

Тема 8. Цепочка поставок и партнёры: риск, который компания часто недооценивает.
Как уязвимости подрядчиков и сервис-провайдеров превращаются в прямые убытки. Современный бизнес практически никогда не существует в одиночку, всегда есть партнеры и контрагенты, которые помимо взаимовыгодного партнерства нередко становятся источниками больших проблем. В рамках данного модуля будут разобраны примеры таких случаев, оценка насколько эти ситуации применимы к ним и что делать, если оно так.

Тема 9. Финансовая оценка рисков: перевод уязвимостей в деньги.
Практическая методика: как посчитать убытки от простоя, потери данных, штрафы и репутационные риски.

Условия участия →

Вид участия:	Стоимость руб. / участник		
	Ранняя оплата **до 17 февраля**	Средняя оплата **до 11 марта**	Поздняя оплата **после 11 марта**
Очное участие (руб./1 участник)	89.700 (63.750)*	99.700 (72.750)*	125.700 (80.750)*
Онлайн участие, руб./ группа (количество участников не ограничено*)	97.900 (72.900)*	107.900 (80.900)*	127.900 (92.900)*
Видеокурс, руб./ группа (количество участников не ограничено*)	97.900 (72.900)*	107.900 (80.900)*	127.900 (92.900)*

* Для представителей органов власти, государственных и муниципальных учреждений.
При очном участии 3-х представителей и более, предоставляется **доступ к видеокурсу**.

* Стоимость в таблице указана за обучение с выдачей Удостоверений о краткосрочном **повышении квалификации** или Свидетельства об участии **группе из 5 (пяти) сотрудников**.
В случае уменьшения количества слушателей, стоимость не меняется. Стоимость обучения каждого дополнительного участника (при условии получения Удостоверения о краткосрочном повышении квалификации**),** составляет 20% от стоимости обучения группы.

✓ **Удостоверение о краткосрочном повышении квалификации** выдаётся на основании **Лицензии** на осуществление образовательной деятельности от 21 марта 2016 года №037282.

Видеокурс – предоставляется **3-х месячный доступ** к образовательному порталу для просмотра высококачественной видеозаписи конференции, без ограничения по количеству просмотров, в том числе одновременных. У вас есть возможность обучить **всех профильных сотрудников организации**, а также заранее выслать вопросы, на которые докладчики ответят в процессе выступлений. Участие включает в себя **Удостоверения о краткосрочном повышении квалификации на 5 (пять) сотрудников.**

Онлайн участие – высококачественная трансляция в режиме реального времени. Вы будете видеть и слышать спикеров и участников, присутствующих очно, слышать задаваемые участниками вопросы, и демонстрацию учебно-методического материала. У вас есть возможность задавать вопросы докладчикам посредством чата, встроенного в плеер трансляции. Видеосъёмка ведётся на несколько камер, монтаж осуществляется в прямом эфире. У вас есть возможность обучить **всех профильных сотрудников организации**, а также заранее выслать вопросы, на которые Докладчики ответят в процессе выступлений. Участие включает в себя **Удостоверения о краткосрочном повышении квалификации на 5 (пять) сотрудников.**

Место проведения: Москва, Измайловское шоссе 71, ТГК «Измайлово», корпус «Вега».
Дата проведения: 26-27 марта 2026г.

Для участия в совещании необходимо:

1) Предварительно запросить, а затем выслать заполненную регистрационную заявку на E-mail: **info@icped.ru**
2) Получить на адрес своей электронной почты следующие документы: Счет на оплату регистрационного взноса, проект Договора, проект Акта.
3) Оплатить счет и переслать копию платежного поручения (с отметкой банка) по эл.почте.
4) Подписать Договор в двух экземплярах и привезти его на конференцию.

Тел.: +7 (495) 230-16-86. Сайт www.icped.ru