# Использование киберготовности как конкурентного преимущества для вашего бизнеса

**Кристен Бауэр (Cristen Bauer)**

**Мелинда Заннер (Melinda Zanner)**

**Лесси Лонгстрит (Lessie Longstreet), глобальный директор по связям с общественностью и взаимодействию с партнерами**

**марта 2023 г.**

CYBER READINESS INSTITUTE

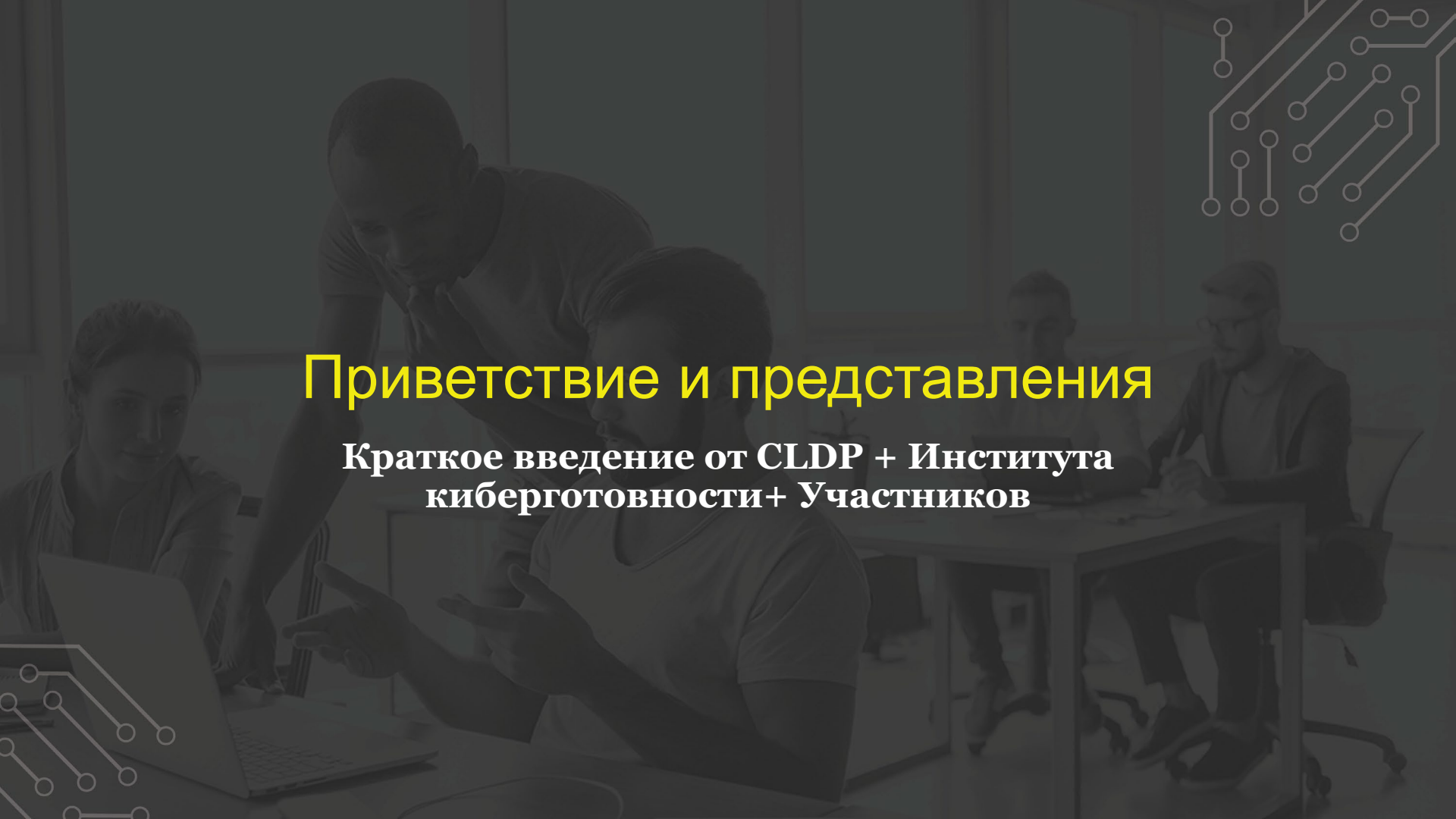
CYBER READINESS
INSTITUTE

# Программа

- Представления + знакомство
- Почему важна киберготовность
- Краткий обзор основных четырех вопросов
- Приоритизация данных + деятельность

--Перерыв--

- Обсуждение приоритезации данных
- Подробный обзор 4-х основ
- Кибер-риски
- Роль кибер-лидера



# Приветствие и представления

**Краткое введение от CLDP + Института киберготовности+ Участников**

# Институт киберготовности

- Включает в себя руководителей мировых компаний и партнеров по цепочке поставок
- Делится передовым опытом кибербезопасности и ресурсами
- Разрабатывает **бесплатный** контент и инструменты для повышения киберготовности малых и средних предприятий.

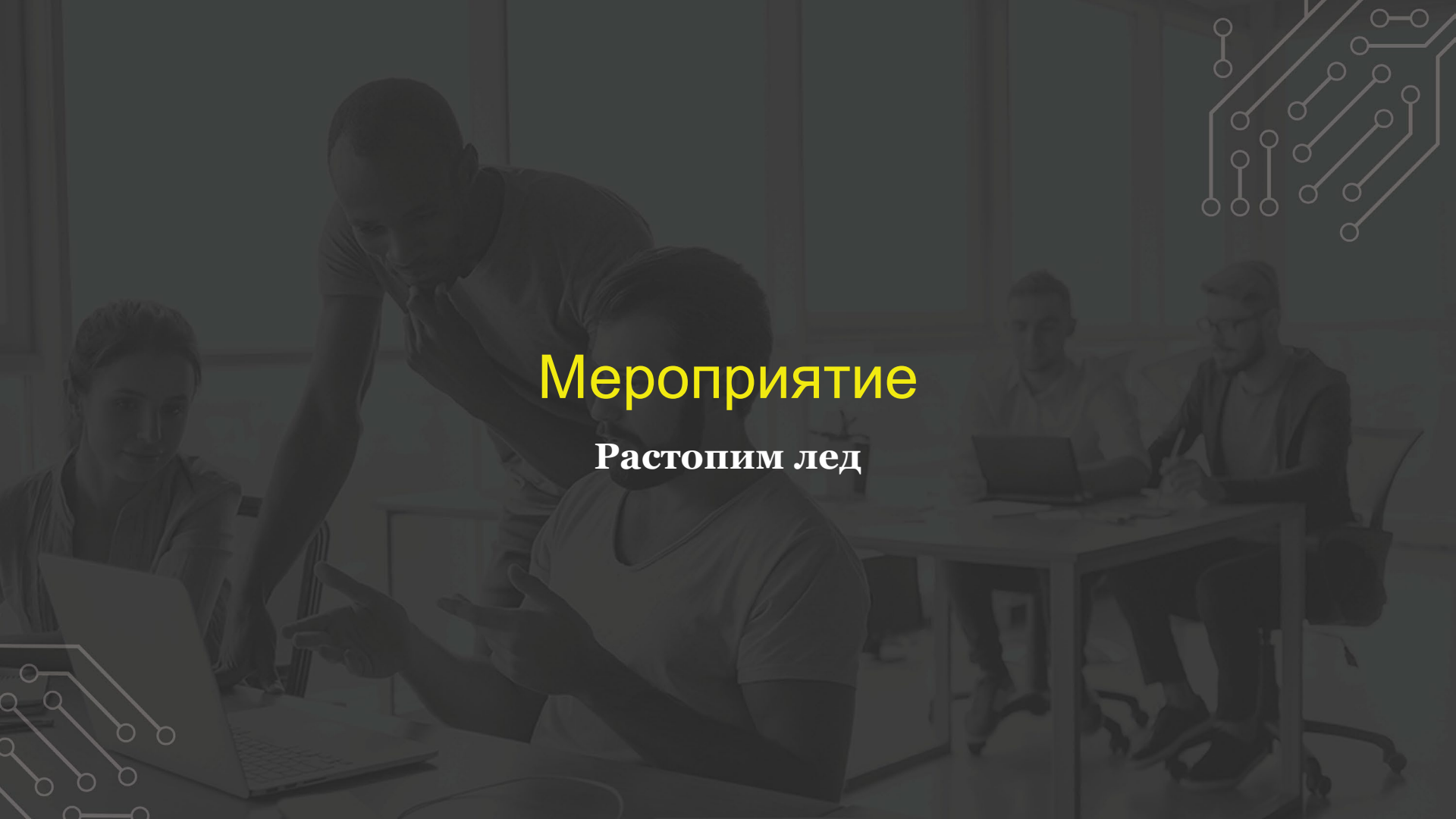
CYBER READINESS INSTITUTE

THE CENTER FOR GLOBAL ENTERPRISE

Principal℠

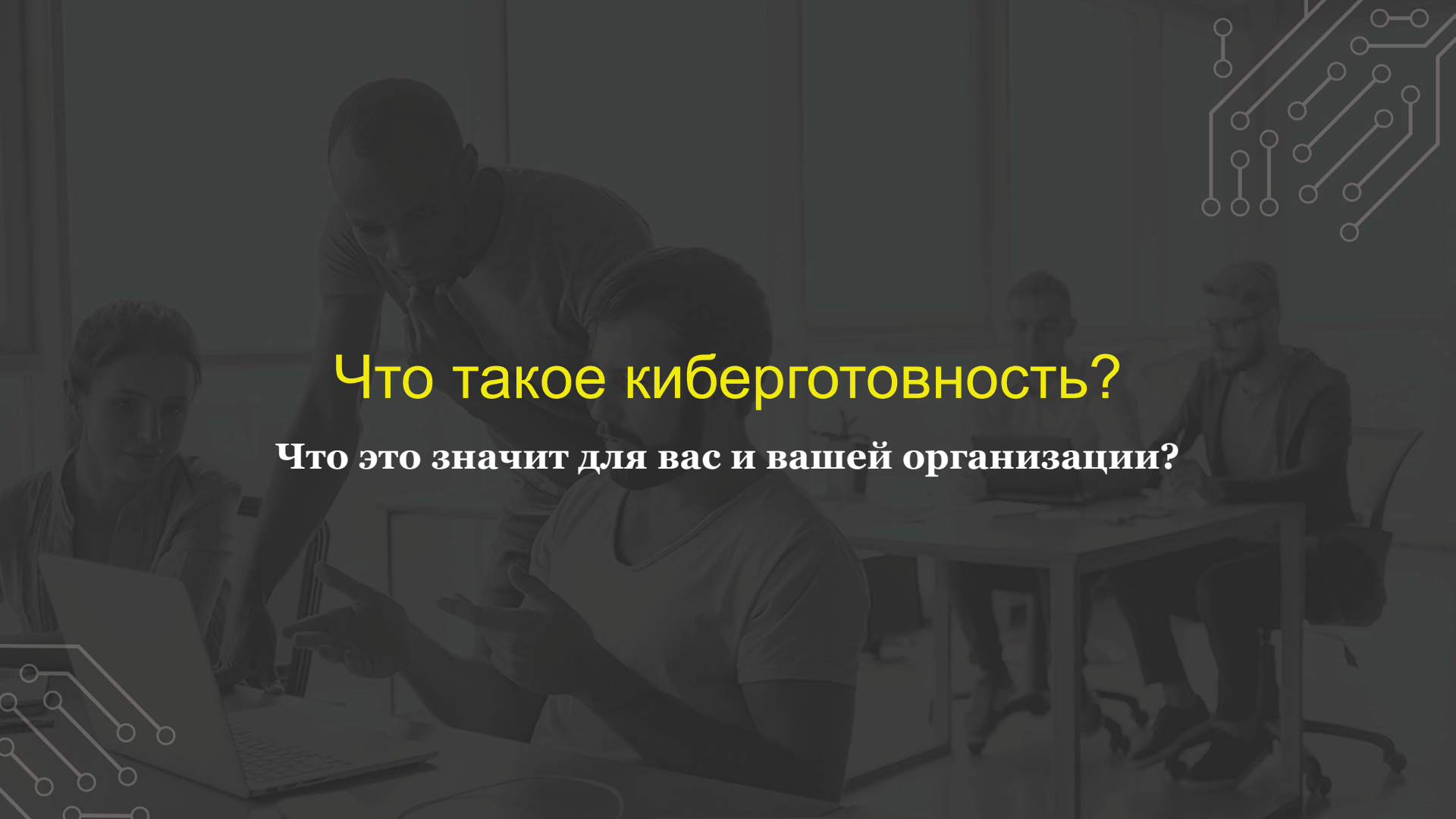
Microsoft

BeCyberReady.com



# Мероприятие

**Растопим лед**



# Что такое киберготовность?

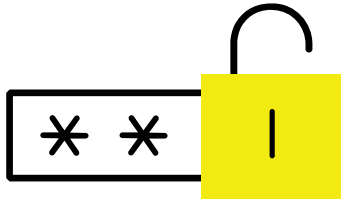
**Что это значит для вас и вашей организации?**

# Что такое киберготовность?

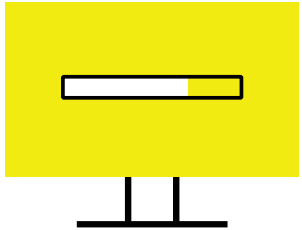
- Принятие практических мер для **предотвращения** кибератак, **сосредоточив внимание на поведении человека**, связанном с проблемами основных четырех компонентов, и **зная, что делать** в случае возникновения инцидента.

CYBER READINESS
INSTITUTE

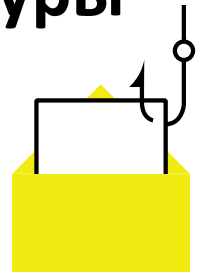
# Сосредоточьтесь на четырех Ключевых элементах изменения культуры



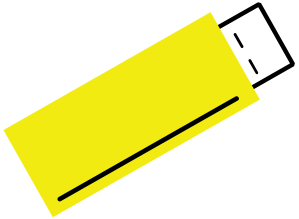
**Пароли и многофакторная аутентификация**



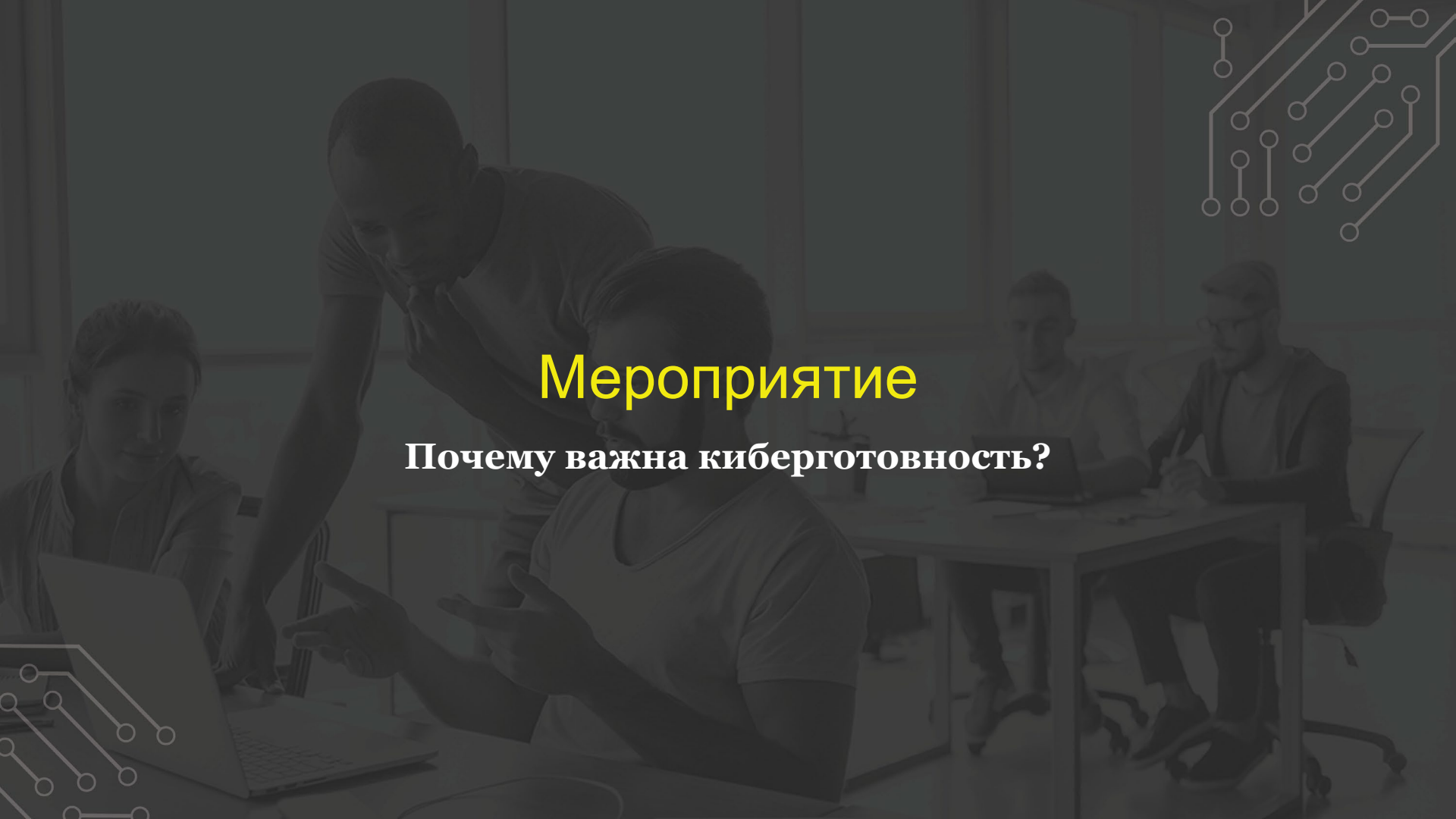
**Обновление программного обеспечения**



**Фишинг**



**USB-накопители и безопасное хранение и передача файлов**



# Мероприятие

**Почему важна киберготовность?**

# Все вовлечены

- Вы можете чувствовать, что держите ситуацию под контролем.
- А как насчет ваших контрагентов?
- Вы можете думать, что у вас нет ничего ценного, но что, если вы являетесь промежуточным пунктом к цели?

# Тенденции в цепочках поставок повышают риск

- Глобализация – поставщики и торговые партнеры во многих странах
- Аутсорсинг основных бизнес-функций
  - Производство
  - Исследования и разработки
  - Логистика
  - Кадры
- Удаленное и гибридное рабочее место

# Приоритизация того, что защищать

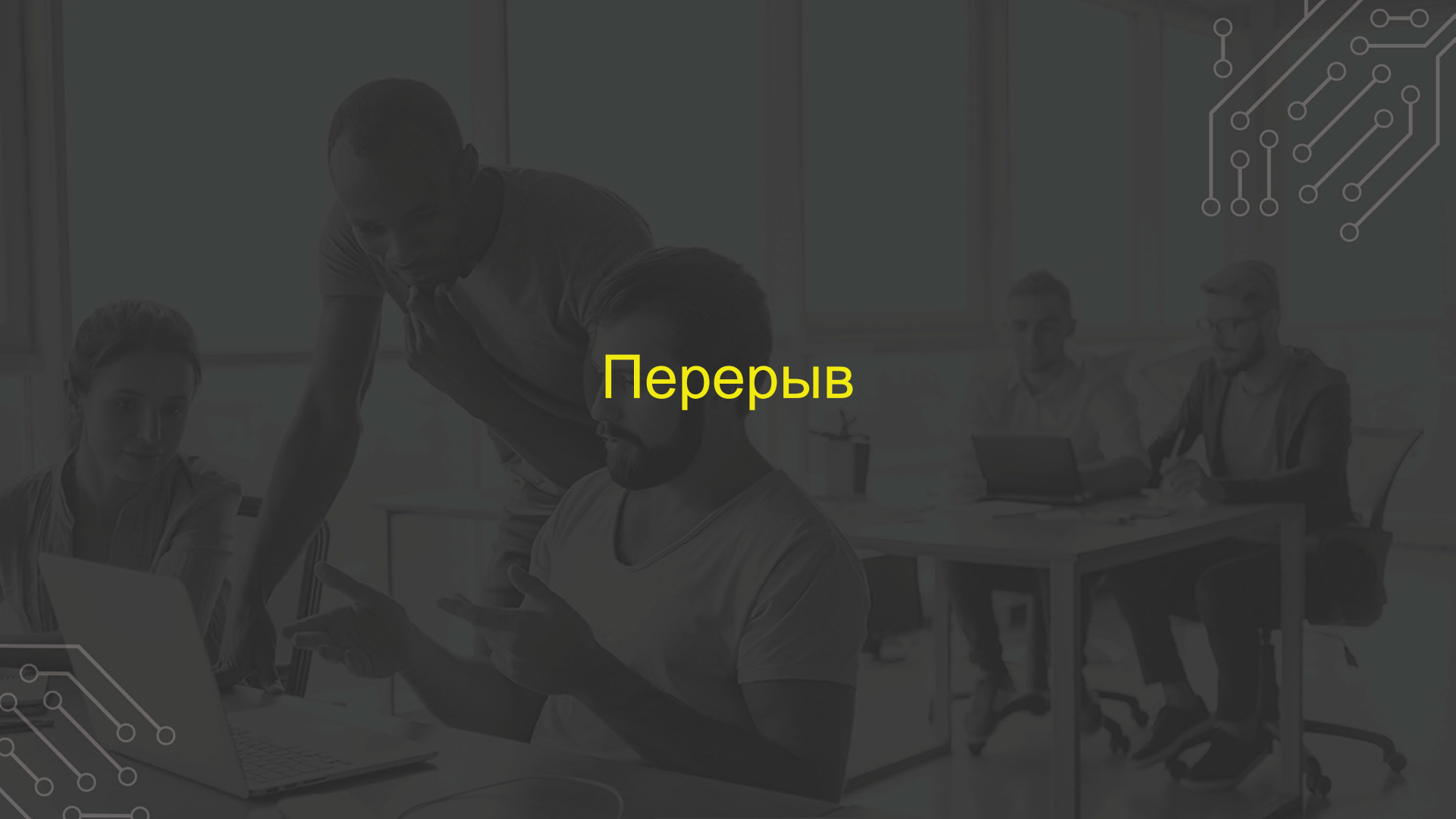
**Вы не можете защитить все одинаково хорошо**

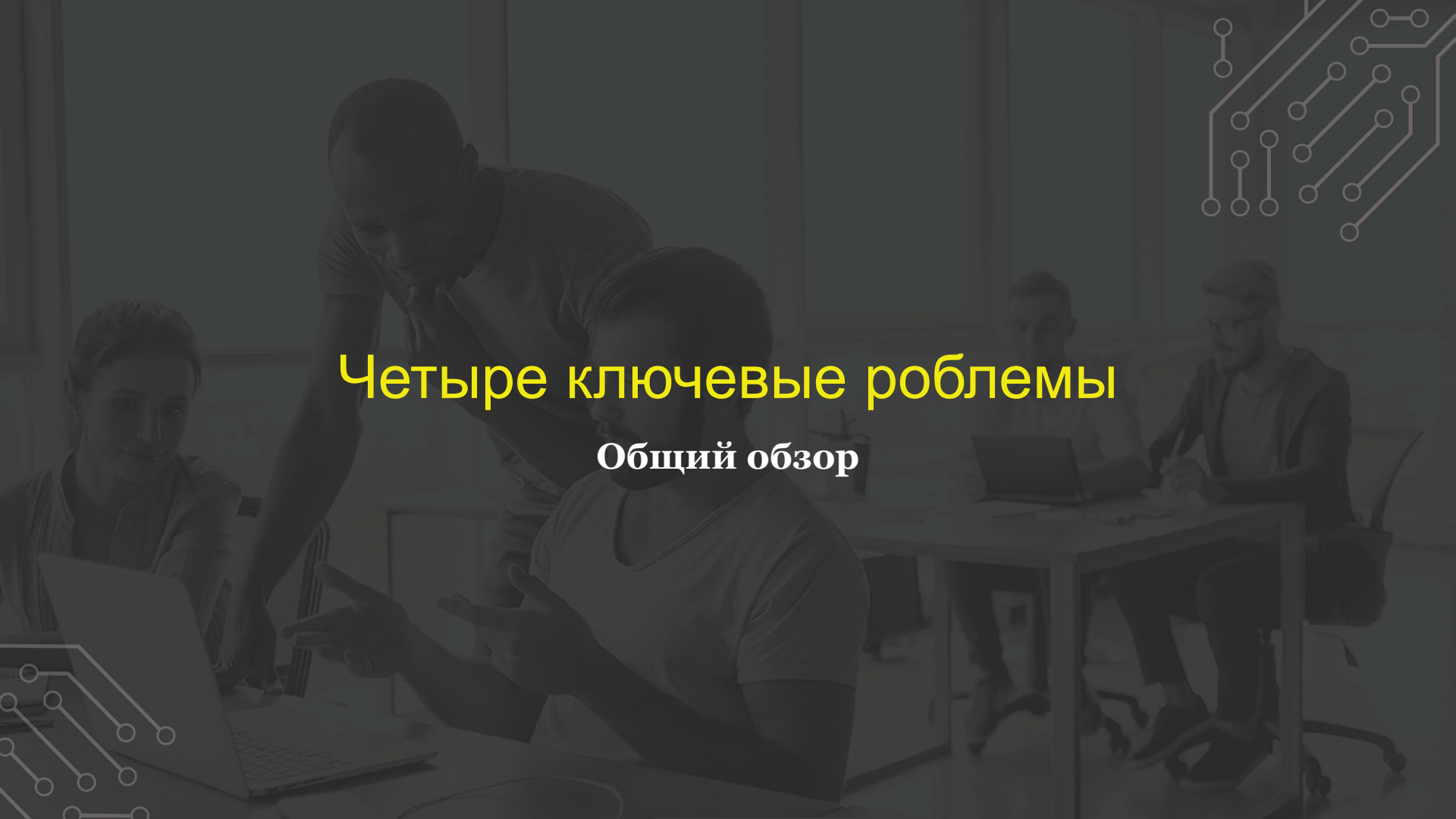
# Потеря данных и обеспечение непрерывности деятельности


CYBER READINESS
INSTITUTE

# Упражнение: Приоритизация того, что защищать

- 10 минут каждому на заполнение рабочего листа
- Поощряйте обсуждение за каждым столом или с людьми поблизости (если это уместно)
- Содействовать обсуждению трех основных систем и типов данных, которые необходимо защищать — 20 минут.


Перерыв

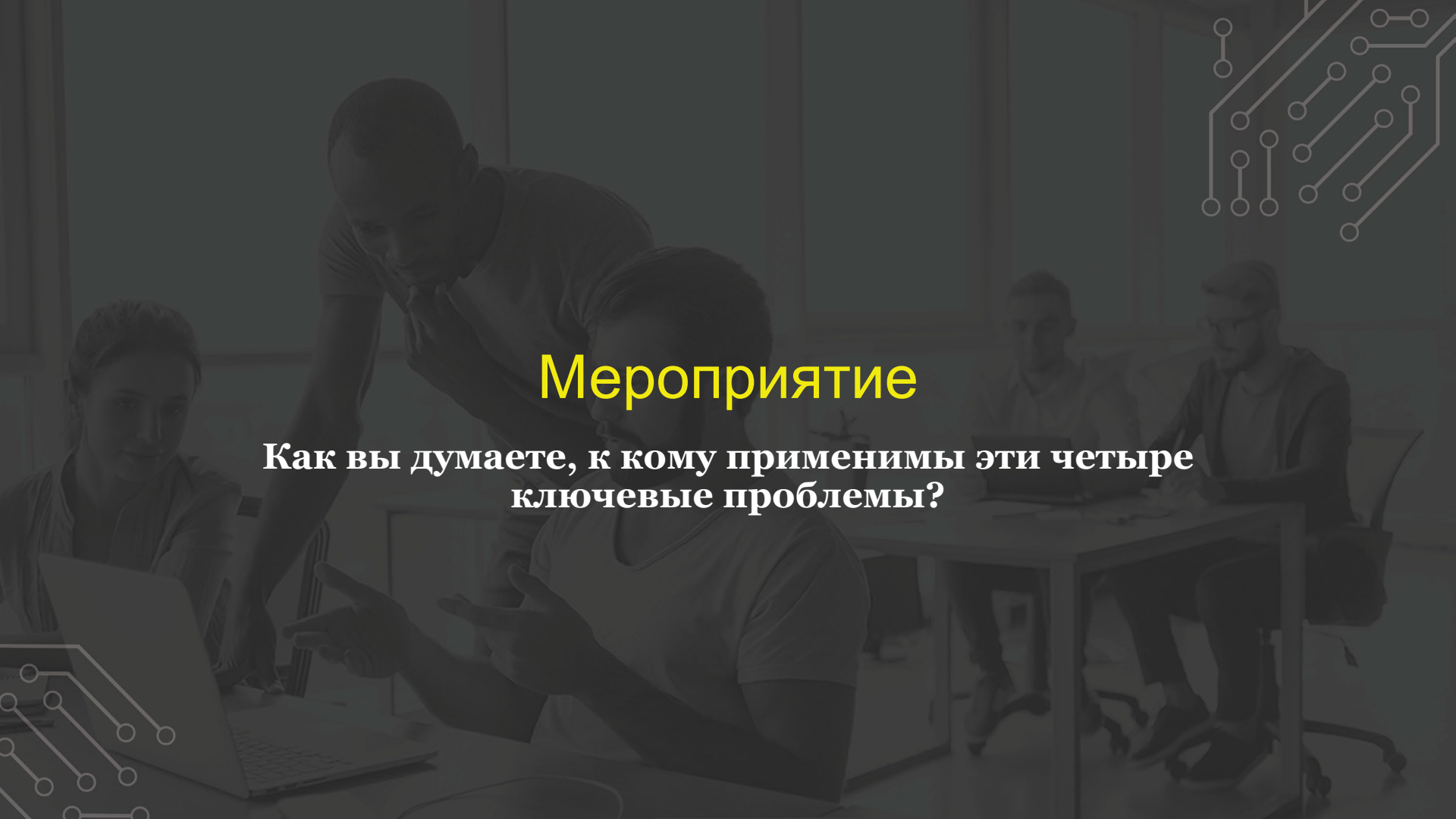


# Четыре ключевые роблемы

**Общий обзор**

# Четыре ключевых элемента

- **Пароли +:** То, как компьютер узнает вашу личность. Они являются важным привратником на пути к вашим данным и системам, и наиболее распространенным способом аутентификации вашей личности. Все чаще используется в сочетании с многофакторной аутентификацией, также называемой двухэтапной проверкой.
- **Обновление программного обеспечения:** Исправления проблем и ошибок в программных продуктах. Хакеры часто пользуются уязвимостями программного обеспечения, атакуя устройства, которые не были обновлены.
- **Фишинг:** Приходит в виде электронных почтовых сообщений, телефонных звонков, текстов. Они пытаются обманным путем заставить пользователя предоставить личную информацию, пароли, банковскую информацию, деньги, данные и т.д. злоумышленнику, который притворяется знакомым или доверенным лицом.
- **USB-накопители (универсальная последовательная шина) и безопасный обмен файлами:** Тип съемного носителя, который может хранить и передавать файлы с одного устройства на другое. USB-накопители являются частыми целями злоумышленников и могут заразить ваш компьютер без вашего ведома, пока не станет слишком поздно. Облачный обмен файлами, как правило, безопаснее, но вашей организации необходимо установить правила.

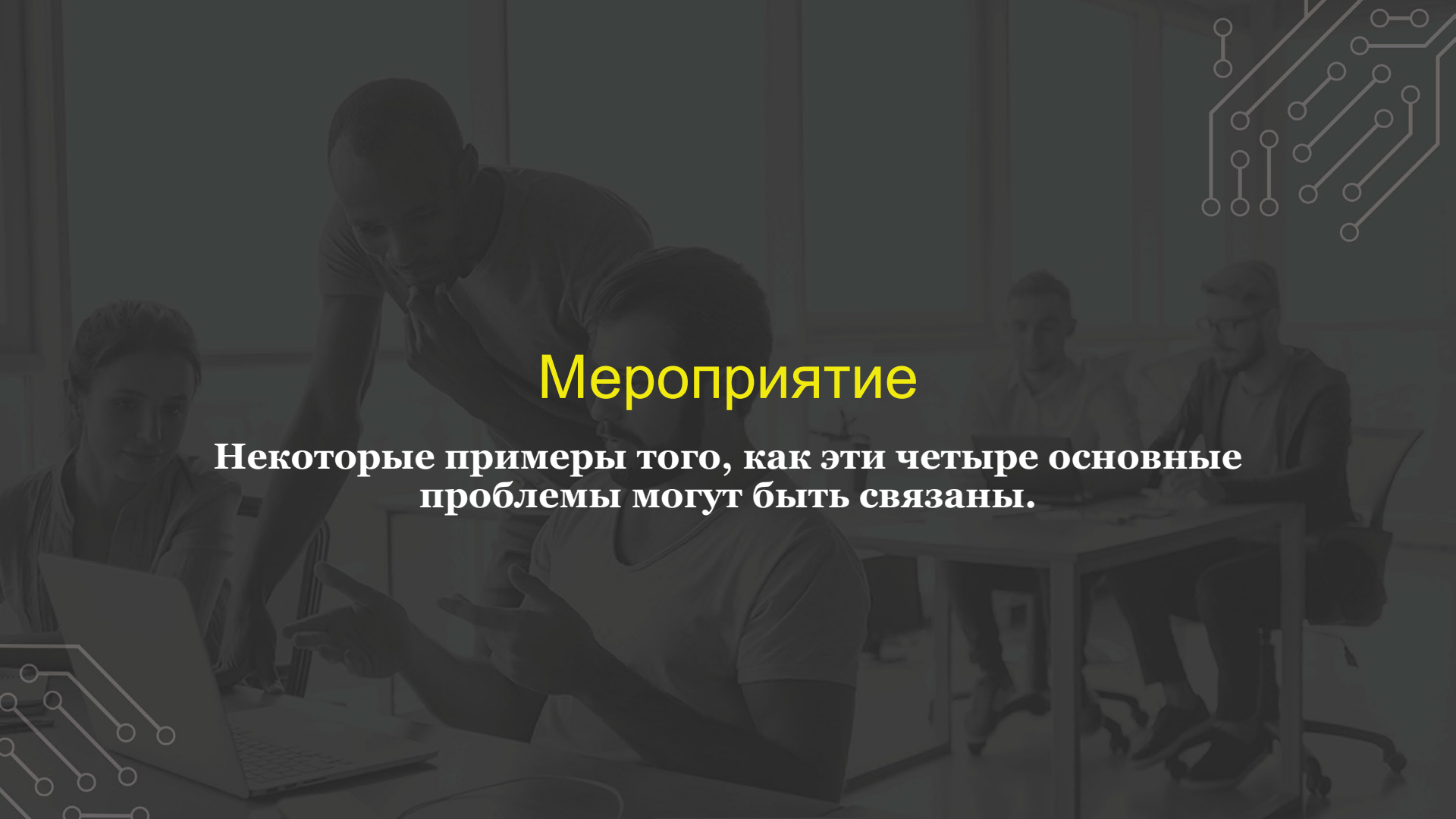


# Мероприятие

**Как вы думаете, к кому применимы эти четыре ключевые проблемы?**

# Ключевые четыре элемента применимы ко всем

- **Каждый сотрудник и подрядчик**
  - Все уровни
  - Все роли и функции
- **Каждое устройство, используемое для доступа к сетям и данным организации**
  - Компьютеры, предоставленные компанией
  - Смартфоны и планшеты, предоставленные компанией
  - Персональные компьютеры
  - Персональные смартфоны и планшеты



# Мероприятие

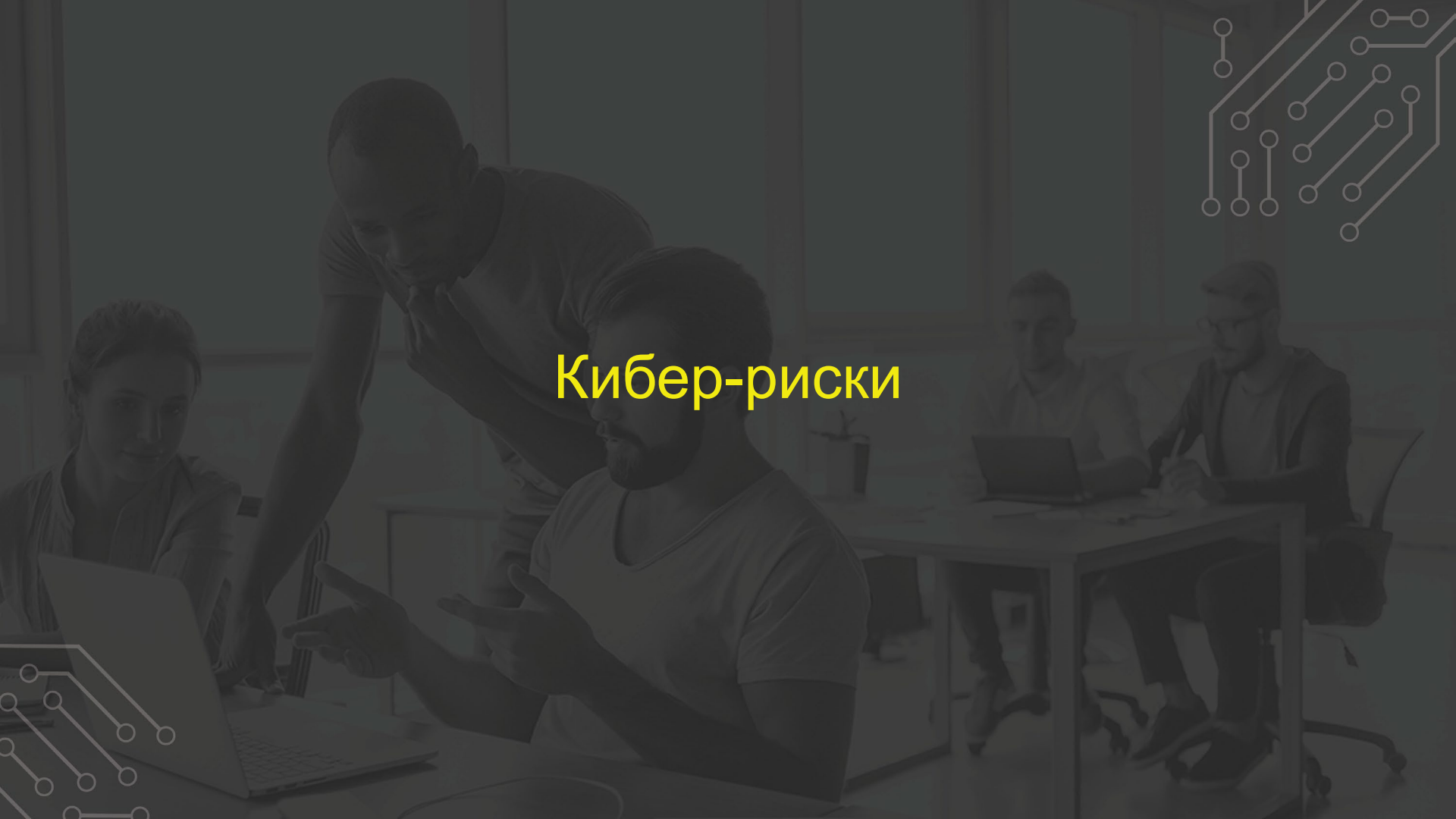
**Некоторые примеры того, как эти четыре основные проблемы могут быть связаны.**

# Пример: Атака программ-вымогателей

- Проводится злоумышленником с целью заблокирования данных организации с целью получения выкупа.
- Злоумышленники могут получить доступ различными способами, включая фишинг, неисправленное программное обеспечение и посещение вредоносных или взломанных веб-сайтов.
- Включает эксфильтрацию данных, участие в распределенных атаках типа «отказ в обслуживании» (DDoS),
и антидетектирующие компоненты
- Воздействие может быть масштабным и подрывающим

# Пример: Компрометация деловой электронной почты (BEC)

- Злоумышленник захватывает ваш почтовый сервер и может отправлять фишинговые электронные письма, используя ваши учетные записи.
- Вы получаете фишинговое письмо от своего начальника или коллеги с просьбой перейти по ссылке или отправить пароль.
- Поскольку компании используют облачное хранилище файлов, BEC становится все более распространенным явлением.



# Кибер-риски

CYBER READINESS
INSTITUTE

# Подход Института киберготовности

- Назначить Кибер-лидера в вашей компании
- Сосредоточить внимание на образ действий сотрудников
- Использовать рекомендации и инструменты по превентивным мерам и практическим действиям по реагированию на инциденты
- Создать «Культуру киберготовности»
- Обеспечение безопасности цепочки поставок

CYBER READINESS
INSTITUTE

# Создание культуры киберготовности

**Цель:**

Внедрение киберготовности в то, как люди выполняют свою работу

**Люди** - это ключ

**Процессы** должны быть практичными и простыми

**Технологии** должны повышать кибербезопасность, одновременно повышая производительность труда

CYBER READINESS
INSTITUTE

# Результаты программы киберготовности

- **76%** компаний, завершивших Программу, сообщают, что она оказала **сильное или очень сильное влияние**

CYBER READINESS
INSTITUTE

# Превратите свою киберготовность в конкурентное преимущество

- Многонациональные компании оценивают программы защиты данных и кибербезопасности потенциальных поставщиков или торговых партнеров.
- Инвесторы проводят полную документальную проверку деятельности перед инвестированием
- Компании Apple, GM и Министерство обороны США совместно с Институтом киберготовности (CRI) реализуют программы, направленные на повышение киберготовности своих поставщиков.

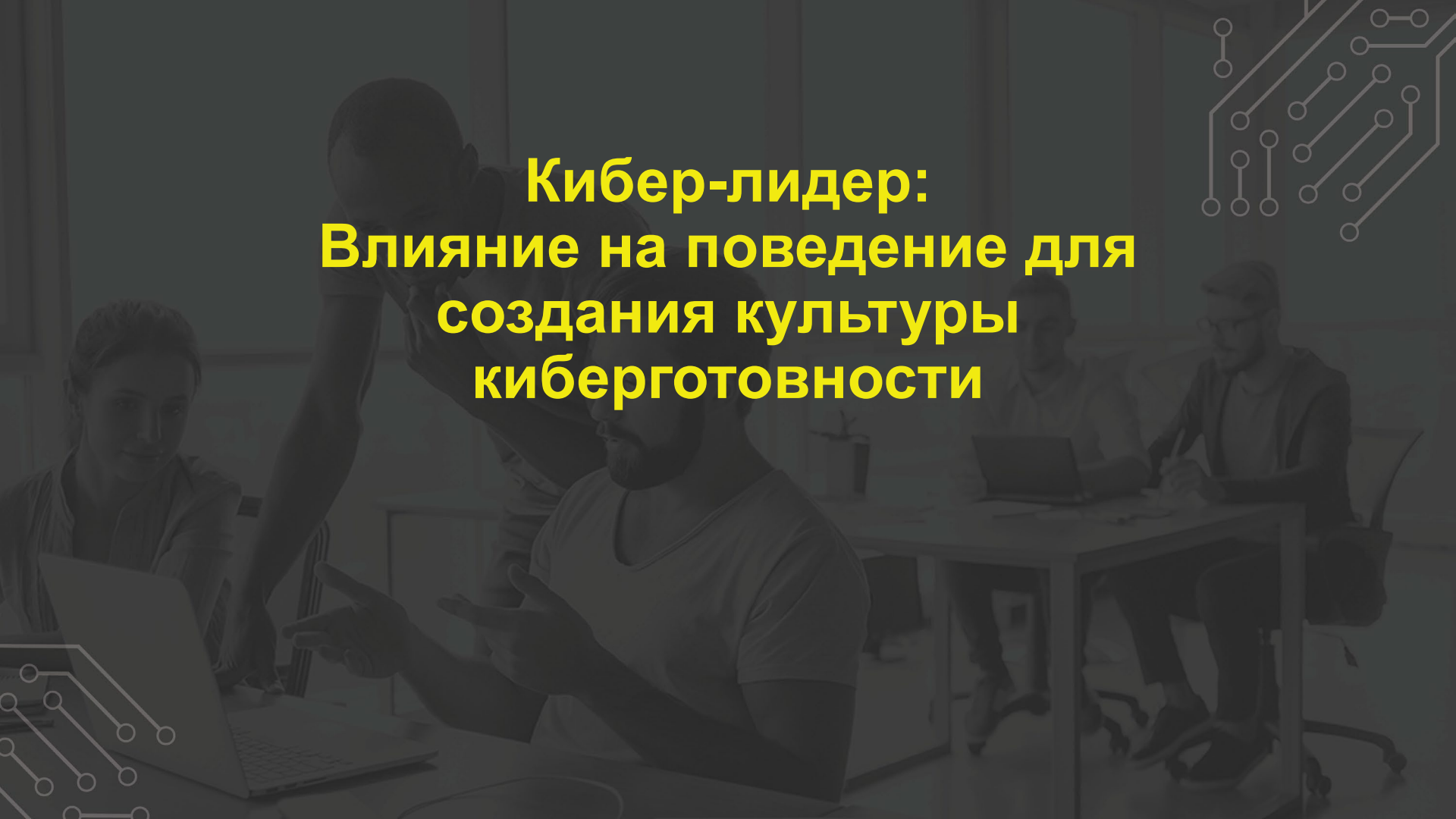
# Опрос: Ваши киберриски

Что вас больше волнует в вашей компании:

- Потеря данных или компрометация данных
- Непрерывность деятельности
- Оба в одинаковой степени

# Начнем: Риск-ориентированный подход

- **Расставьте приоритеты**, какие системы и данные важнее всего защищать
- Определите **наиболее вероятные** способы их потери или повреждения.
- Определите, что нанесет **наибольший ущерб**
  - Рассмотрите ущерб от **потери данных** или публичного раскрытия данных
  - Учитывайте ущерб от простоя систем в течение нескольких дней или недель (**непрерывность деятельности**).
- Оценить **прямые финансовые затраты**, **затраты на восстановление и репутационный ущерб**



# Кибер-лидер: Влияние на поведение для создания культуры киберготовности

CYBER READINESS
INSTITUTE

# Роль владельца/менеджера малого бизнеса в поддержке кибер-лидера

CYBER READINESS
INSTITUTE

# Основные задачи Кибер-лидера

- Возглавить создание культуры кибер готовности в вашей организации путем внедрения практических политик и обучения ваших сотрудников важности линии поведения в обеспечении готовности к кибербезопасности.

- Помощь вашей организации в разработке надлежащего плана подготовки к инцидентам кибербезопасности

# Люди - это ключ

- Киберготовность — это ваши сотрудники и их образ дейсвий
- Цель состоит в том, чтобы:
  - Внедрить киберготовность в то, как каждый человек выполняет свою работу
  - Развить хорошие кибер-привычки
  - Создать культуру киберготовности в организации
- Для этого процедуры и политики по кибербезопасности должны быть максимально практичными.

# Превосходство в качестве кибер-лидера

Кибер-лидер должен иметь:

- сильные управленческие навыки и навыки работы с людьми
- способность эффективно стимулировать изменения и создавать культуру киберготовности
- спокойное отношение к технике - технические знания менее важны
- способность справляться с этой ролью наряду с повседневными обязательствами
- приверженность важности кибербезопасности и признание серьезного воздействия кибератак
- поддержку руководителей вашей организации и соответствующий уровень полномочий

# Советы по обучению и общению

Изменение поведения требует начальной подготовки, подкрепляемой частыми короткими сообщениями.

- Советы по обучению:
  - Используйте относящиеся к делу сценарии, актуальные для сотрудников
  - Имейте четкое представление о разнице между повышением осведомленности, достижением приверженности или обучением внедрению
- **Советы для постоянного общения:**
  - Сосредоточьтесь на развитии одной привычки за раз по ежемесячной теме кибер-готовности
  - Отправляйте короткие еженедельные оповещения, чтобы освещать новые кибер-угрозы и подчеркивать важность кибер-готовности.


Вопросы?

CYBER READINESS
INSTITUTE

# Change Behavior. Be Cyber Ready.

**Contact us to learn more:**

**llongstreet@cyberreadinessinstute.org**

**Visit us at** BeCyberReady.com

@cyber-readiness-institute
@Cyber_Readiness
@CyberReadinessInstitute