# Обеспечение кибербезопасности вашей организации в условиях кризиса

## Понимание и управление потенциальными последствиями в кибербезопасности во время вспышки COVID-19

**Всемирная организация здравоохранения объявила COVID-19 пандемией, которая оказывает огромное влияние на жизнь людей, их семьи и сообщество в целом.**

Компании сталкиваются с серьезными вызовами и сбоями. Способность преодолевать кризисы и непредвиденные события является важным аспектом операционной устойчивости; особенно во время кризиса здравоохранения.

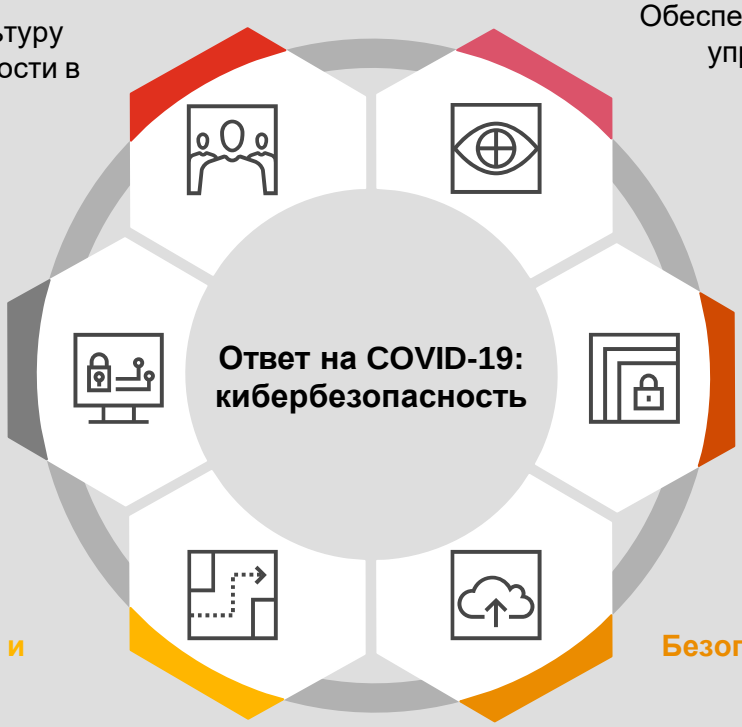
Чтобы обеспечить бесперебойную работу бизнеса в нестабильное время, компаниям необходимо создать и отработать целостную способность реагировать на кибератаки, выстроить механизмы, отвечающие повышенному спросу на удаленную работу и возросшей сложности управления.

### Культура и осведомленность

Усиление внимания на культуру информационной безопасности в организации в период повышенного кибер-риска

### Руководство

Обеспечение эффективного уровня управления в неопределенной среде для поддержания соответствующего уровня безопасности




### Превентивный контроль

Поддержание эффективного контроля обнаружения и контроля защиты во время нестандартных бизнес-операций

### Безопасность данных

Защита конфиденциальной информации при внедрении и использовании различных методов работы

### Управление инцидентами и непрерывность бизнеса

Продолжение использования возможностей управления инцидентами, реагирования на кризисы и обеспечения непрерывности бизнеса в период повышенного организационного стресса

### Безопасность новых технологий

Укрепление безопасности активно внедряемых новых технологий (облачные сервисы, удаленный доступ и т.д.)

pwc

Глобальная сеть PwC неоднократно признавалась лучшей компанией в области консалтинговых услуг по обеспечению непрерывности бизнеса

# План поэтапного реагирования на COVID-19

## Подготовительный этап

- ❑ Удостовериться в готовности Центра обеспечения безопасности (SOC) адаптироваться к более высокому уровню требований в кибербезопасности
- ❑ Ознакомить руководство с протоколами безопасности связи в случае кибер-инцидента (например, управление связями с общественностью, реагирование кризисной команды)
- ❑ Создать механизмы передачи знаний для ознакомления временного / аварийного персонала с процедурами безопасности организации
- ❑ Обеспечить приложениями удаленного доступа и VPN все конечные устройства
- ❑ Настроить управление идентификацией пользователей при удаленном доступе к системам
- ❑ Проверить, будет ли пропускная способность сети поддерживать значительно возросшее использование служб через удаленный доступ или существует повышенная вероятность потери обслуживания (непреднамеренная DoS)
- ❑ Провести переоценку кибер-рисков с учетом новых факторов и изменений
- ❑ Скорректировать процессы и решения по защиты данных

## Этап реагирования

- ❑ Провести инструктаж сотрудников по кибербезопасности, включая использование личных устройств для доступа к корпоративным приложениям
- ❑ Разработать альтернативный процесс устранения обнаруженных критических уязвимостей, в случае реализации в организации блокировки изменений
- ❑ Обеспечить возможность инфраструктуры кибербезопасности расширяться в течение короткого периода времени для удовлетворения быстро меняющихся требований
- ❑ Выявить возможные ограничения доступа, которые могут помешать пользователям удаленно получать доступ к ключевым системам
- ❑ Оборудовать ЦОДы для аварийного переключения сети в целях обеспечения непрерывности бизнеса
- ❑ Разработать решения для оповещения, реагирования, и расследования подозрительных действия пользователей в сети с учетом изменения стандартных шаблонов работы пользователей
- ❑ Расставить приоритеты для служб безопасности, включая рассмотрение вопроса о временном прекращении услуг с низким приоритетом в пользу сохранения важных функций

## Этап восстановления

- ❑ Провести тестирование безопасности на основе уязвимостей, выявленных в течение периода работы в нестандартных условиях
- ❑ Разработать процессы в ответ на воздействие нового кризисного сценария, чтобы минимизировать будущие сбои в бизнесе
- ❑ Проанализировать варианты автоматизированного управления кибербезопасностью для обеспечения устойчивости бизнеса в периоды нехватки персонала
- ❑ Рассмотреть облачные решения для улучшения масштабируемости услуг по требованию в более долгосрочной перспективе
- ❑ Скорректировать архитектуру безопасности, чтобы в будущем она стала более устойчивой или гибкой
- ❑ Оценить возможность применения развивающихся технологий, чтобы дополнительно повысить устойчивость бизнеса
- ❑ Разработать планы на случай непредвиденных обстоятельств для устранения остаточных недостатков в операционной модели

## Наши контакты


**Виталий Соколов**
Партнер
+7 (495) 967 6153
vitaly.l.sokolov@pwc.com

**Михаил Курзин**
Директор
+7 (495) 967-6000
mikhail.kurzin@pwc.com