

# Цифровая трансформация

Влияние на Cyber\_Security

19 августа 2021



Можно выделить несколько ключевых направлений цифровой трансформации:

Разработка новой цифровой бизнес-модели.

1. Создание цифровых товаров и услуг.
2. Управление жизненным циклом продукта.
3. Автоматизированный сбор, хранение и обработка информации.
4. Внедрение цифрового проектирования.
5. Управление производственными процессами, цепочками и сетями поставок.
6. Выполнение административных функций.
7. Автоматизация ручного труда посредством использования роботов, ботов и электронного документооборота.

Выбор технологий для конкретного бизнеса зависит от того, зачем выполняется цифровизация, каких целей необходимо достичь.

В бизнесе цифровая трансформация способствует оптимизации и повышению точности работы и предполагает переход компаний на электронные платформы.

Выделяют 3 этапа такой трансформации:

1. Автоматизация.
2. Цифровизация.
3. Цифровая трансформация.

На последней стадии изменяется вся система управления бизнесом, начиная с методов производства и заканчивая стратегией в разрезе экономики, IT – технологий и соответственно КБ

## Появляются новые бизнес-процессы

1. Роботизированная автоматизация процессов (RPA).
2. Интеллектуальная автоматизация с привлечением ИИ.
3. Углубленная аналитика и большие данные (Deep Learning and Big Data).
4. Новые средства бизнес-моделирования, имитационное моделирование (Simulation modelling).

Все эти изменения несут в себе новые и новые угрозы и риски КБ

Гибкие методологии в управлении проектами стали стандартом де-факто для технологических компаний, а затем начали распространяться за пределы отделов разработки и в другие сектора промышленности, в том числе Agile-практики теперь применяются и в области безопасности.

В настоящее время знание методов и практик Agile считается обязательным, как для менеджеров по информационной безопасности, так и для специалистов, особенно в случаях, когда те являются членами команд разработки.

Активно внедряются принципы DevOps создается непрерывный конвейер разработки, доработки, изменения продукта и как следствие рост количества уязвимостей в разрабатываемых системах.

Возможно, что самый существенный качественный скачок в подходах к защите компаний – смещение фокуса защиты от инфраструктуры к основным, формирующим прибыль бизнес-процессам.

С одной стороны, это повышает уровень абстракции и дает необходимую гибкость на нижних уровнях, таких как ИТ-инфраструктура и программные платформы, с другой – обеспечивает интеграцию мер защиты во все ключевые процессы компании и предотвращение потерь.

Такой подход наблюдается все чаще и требует высокой организационной зрелости, и квалифицированного руководителя КБ, который хорошо понимает бизнес и входит в руководство компании.

Рост количества используемых мобильных приложений и сервисов, объема обрабатываемых данных, развитие технологий искусственного интеллекта и облачных услуг не только увеличивает доступный злоумышленникам ландшафт, но и делает ущерб от кибератак все более значимым для операционной деятельности. Стоимость ущерба стремительно растет и в абсолютных значениях.

Именно поэтому в последние годы бизнес в фокусе внимания держат вопросы кибербезопасности и инвестируют в КБ значительные ресурсы. Именно поэтому неуклонно растет и роль служб кибербезопасности.

Одновременно сбор и обработка огромных массивов данных, в первую очередь персональных, привели к необходимости введения более жесткого государственного и даже наднационального регулирования, что в свою очередь породило особый класс задач для КБ, связанных с так называемой «бумажной» безопасностью.

КБ оказалась, с одной стороны, под давлением бизнеса, который требует ускорения изменений и гибкости, а с другой – под прессом регуляторных требований, задающих достаточно жесткие рамки и предполагающих определенную дополнительную бюрократизацию процессов. Грузом становится и наследие в виде классических систем защиты, и ограниченность ресурсов, в первую очередь в области квалифицированных кадров.

Наборы навыков	Процессы	Решения
Continuous Configuration and automation	Автоматизированное конфигурирование и обновление	<ul style="list-style-type: none"> <li>• Chef</li> <li>• Ansible</li> <li>• Twistlock</li> </ul>
Владение языками для создания скриптов и взаимодействия через REST API	Автоматизация без скриптов невозможна	<ul style="list-style-type: none"> <li>• Python</li> </ul>
Cloud-native приложения	Новый вид организации вычислений	<ul style="list-style-type: none"> <li>• Kubernetes</li> <li>• Docker</li> </ul>
Управление потребляемым сервисом	Ненужный сервис тратит деньги и создает риски	<ul style="list-style-type: none"> <li>• CloudHealth Technologies</li> <li>• CloudCheckr</li> </ul>
CI/CD	Быстрое развертывание лишает традиционные патчи смысла	<ul style="list-style-type: none"> <li>• Gitlab</li> </ul>