

Кибербезопасность, цифровые риски и угрозы

Денис Липов, «Делойт», СНГ

Цифровая революция стимулирует инновации и рост, но также сопряжена с новыми рисками



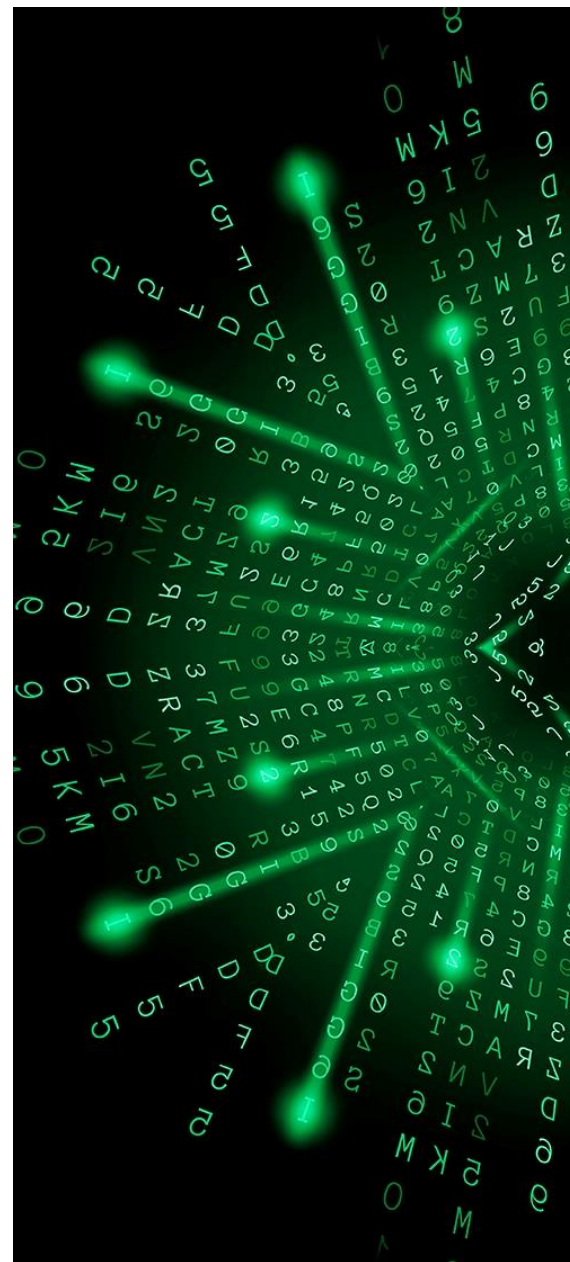
Активное развитие и использование новейших технологий меняет мир и создает новые возможности



Организации меняют ландшафт киберрисков в стремлении к инновациям и повышению эффективности



Не стоит рассчитывать на то, что существуют методы 100%-ной защиты от реализации киберрисков



Ландшафт киберрисков стремительно меняется

Размытие периметра



Инновации, такие как гибридные ИТ-решения, облачные и цифровые экосистемы, размывают границы между организациями и ликвидируют периметр сети, который организация должна защищать.

Изменение облика бизнеса



Инновационные организации создают новые модели доходов и оказания услуг с использованием цифровых технологий, которые сопряжены с киберрисками на каждом уровне, начиная с бизнес-стратегии.

Экспоненциальные технологии



Использование экспоненциальных технологий меняет скорость внедрения инноваций. Вместе с тем повышается скорость возникновения новых киберрисков, а также могут усложниться процедуры реагирования, которые выстраиваются вокруг традиционных подходов к разработкам ИТ-решений.

Интернет вещей



Интернет вещей оказывает положительное и преобразующее влияние на нашу жизнь. Однако он также создает огромное множество подверженных уязвимостям устройств.

Искусственный интеллект



Искусственный интеллект начинает дополнять или заменять экспертов. Это может привести к возникновению новых возможностей и снижению затрат, однако также создает новые риски. Например, чат-боты, которые ведут себя ненадлежащим образом.

Мобильные устройства



Для растущего числа потребителей мобильные устройства — единственный канал взаимодействия, который имеет значение, что повышает вероятность реализации киберугроз, увеличивая поверхность атаки.

Активное развитие и использование новейших технологий создаст новые возможности и киберугрозы, которые сейчас сложно даже представить

Будущее смартфона: эпоха инноваций

«К концу 2023 года смартфоны можно будет использовать как ключи, пропуска, банковские и прочие карты для совершения финансовых транзакций.

Более 75% всех владельцев смартфонов будут использовать одну из форм биометрической аутентификации, а на 80% смартфонов будет установлен как минимум один специальный биометрический датчик».

Будущее смартфона: эпоха инноваций

- Оптимизация текущих процессов
- Оперативный доступ к информации
- Взаимодействие с CRM- и ERP-системами
- Оценка эффективности работы сотрудника

Возможности

Угрозы

- Раскрытие персональных данных и конфиденциальной информации
- Снижение качества и эффективности работы сотрудников
- Репутационный риск (утечка информации/ несанкционированный сбор информации)

Реализованные рисковые события киберпространства:

- Обновленная ОС OxygenOS смартфона OnePlus отслеживала и передавала данные о действиях пользователей без их анонимизации
- Уязвимость в Android-устройствах позволяла захватить управление смартфоном при помощи специально сформированного MMS-сообщения
- Уязвимость в смартфонах позволяла обращаться к электронным ассистентам Google Now и Siri через голосовые команды и загружать вредоносное ПО
- Уязвимость в iOS позволяла подменять приложения из AppStore вредоносными

Дополненная реальность: у пределов действительности

«В 2018 году более 1 млрд пользователей смартфонов будут создавать контент дополненной реальности (AR) не реже одного раза в год. К концу 2018 года появятся десятки тысяч приложений, включающих компонент дополненной реальности; наибольшее распространение получит использование дополненной реальности в приложениях смартфонов».

Дополненная реальность: у пределов действительности

- Создание «виртуальных примерочных», демонстрация товаров в интерьере
- Выведение информации о достопримечательности/маршруте на экран, перевод знаков/указателей
- Ускорение поиска товаров/материалов на складе, оптимизация маршрута при перемещении
- Создание промокампаний и приложений в рамках продвижения продукта/повышения узнаваемости бренда



Возможности



Угрозы

- Раскрытие конфиденциальной информации (местоположение пользователей, права доступа, платежные данные)
- Поддельные приложения с вредоносным содержанием, заложенным в компоненты ДР

Реализованные рисковые события киберпространства:

- Уязвимость в приложении PokemonGo позволяла получить доступ к учетным записям Google пользователей приложения
- Всего через четыре дня после выхода PokemonGo была создана поддельная версия со встроенным вредоносным ПО
- Публикация данных фитнес-трекера Strava позволила обнаружить данные о передвижении пользователей на территории военных баз и в их окрестностях

Защищенность, бдительность и устойчивость организации

Создаваемая ценность

Инновации

Обмен информацией

Доверие

Стратегическое управление

Управление киберрисками на уровне высшего руководства с учетом стратегических целей организации и меняющегося ландшафта рисков, приоритизация инвестиций



Защищенность

Защита от кибератак, включая политики, процедуры, технические средства и контрольные процедуры



Бдительность

Система раннего оповещения, которая позволит распознавать потенциальные угрозы до их реализации и своевременно выявлять атаки и нарушения кибербезопасности



Устойчивость

Способность быстро реагировать на атаки и восстанавливать работу систем с минимальным влиянием на деятельность организации, репутацию и бренд

Ключевые направления развития кибербезопасности 1/3



Защищенность



Сегодня

- Интеграция кибербезопасности в бизнес-стратегию организации
- Защита ключевых информационных активов
- Создание эффективной системы управления кибербезопасностью



Завтра

- Оценка киберрисков в момент принятия решения об использовании новейших технологий
- Акцент на управлении киберрисками, а не на отказе от новейших технологий
- Защита данных от утечек и искажения

Ключевые направления развития кибербезопасности 2/3



Бдительность



Сегодня

- Осведомленность о нарушении кибербезопасности в организации
- Акцент на всей экосистеме (отрасль, контрагенты, провайдеры услуг)
- Тестирование на проникновение, оценка защищенности



Завтра

- Применение передовых технологий для проактивного выявления угроз кибербезопасности
- Понимание экспоненциальных угроз кибербезопасности и подготовка к ним

Ключевые направления развития кибербезопасности 3/3



Устойчивость



Сегодня

- Планирование восстановления в случае реализации киберинцидентов
- Регулярная проверка способности организации к восстановлению



Завтра

- Разработка сценариев реагирования, специфичных для различных категорий угроз и инцидентов
- Разработка интегрированного плана реагирования, охватывающего все ключевые подразделения

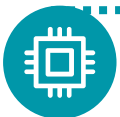
Ключевые принципы кибербезопасности



Интеграция кибербезопасности
в стратегию организации



Защита ключевых информационных активов



Выявление кибератак и эффективное
реагирование на них с целью минимизации
ущерба



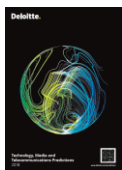
Создание защищенной, бдительной
и устойчивой организации



Контакты и дополнительная информация



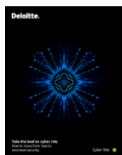
Денис Липов
Директор
Департамент управления
рисками
«Делойт», СНГ
dlipov@deloitte.ru



[Technology, Media and Telecommunications Predictions 2018](#)



[Оценка киберрисков на основе бизнес-целей организации](#)



[Take the lead on cyber risk](#)



[Общий регламент по защите данных \(GDPR\)](#)

deloitte.ru

О «Делойте»

Наименование «Делойт» относится к одному либо любому количеству юридических лиц, включая их аффилированные лица, совместно входящих в «Делойт Туш Томацу Лимитед», частную компанию с ответственностью участников в гарантированных ими пределах, зарегистрированную в соответствии с законодательством Великобритании (далее — ДТТЛ). Каждое такое юридическое лицо является самостоятельным и независимым юридическим лицом. ДТТЛ (также именуемая «международная сеть «Делойт»») не предоставляет услуги клиентам напрямую. Подробная информация о юридической структуре ДТТЛ и входящих в нее юридических лиц представлена на сайте www.deloitte.com/about.

«Делойт» предоставляет услуги в области аудита, консалтинга, финансового консультирования, управления рисками, налогообложения и иные услуги государственным и частным компаниям, работающим в различных отраслях экономики. «Делойт» — международная сеть компаний, в число клиентов которой входят около четырехсот из пятисот крупнейших компаний мира по версии журнала Fortune. «Делойт» имеет многолетний опыт практической работы при обслуживании клиентов в любых сферах деятельности более чем в 150 странах мира и использует свои обширные отраслевые знания и опыт оказания высококачественных услуг для решения самых сложных бизнес-задач клиентов. Более 264 тысяч специалистов «Делойта» по всему миру привержены идеям достижения результатов, которыми мы можем гордиться. Для получения более подробной информации заходите на нашу страницу в [Facebook](#), [LinkedIn](#) или [Twitter](#).

Настоящее сообщение содержит информацию только общего характера. При этом ни компания «Делойт Туш Томацу Лимитед», ни входящие в нее юридические лица, ни их аффилированные лица (далее — «сеть «Делойт»») не представляют посредством данного сообщения каких-либо консультаций или услуг профессионального характера. Прежде чем принять какое-либо решение или предпринять какие-либо действия, которые могут отразиться на вашем финансовом положении или состоянии дел, проконсультируйтесь с квалифицированным специалистом. Ни одно из юридических лиц, входящих в сеть «Делойт», не несет ответственности за какие-либо убытки, понесенные любым лицом, использующим настоящее сообщение.