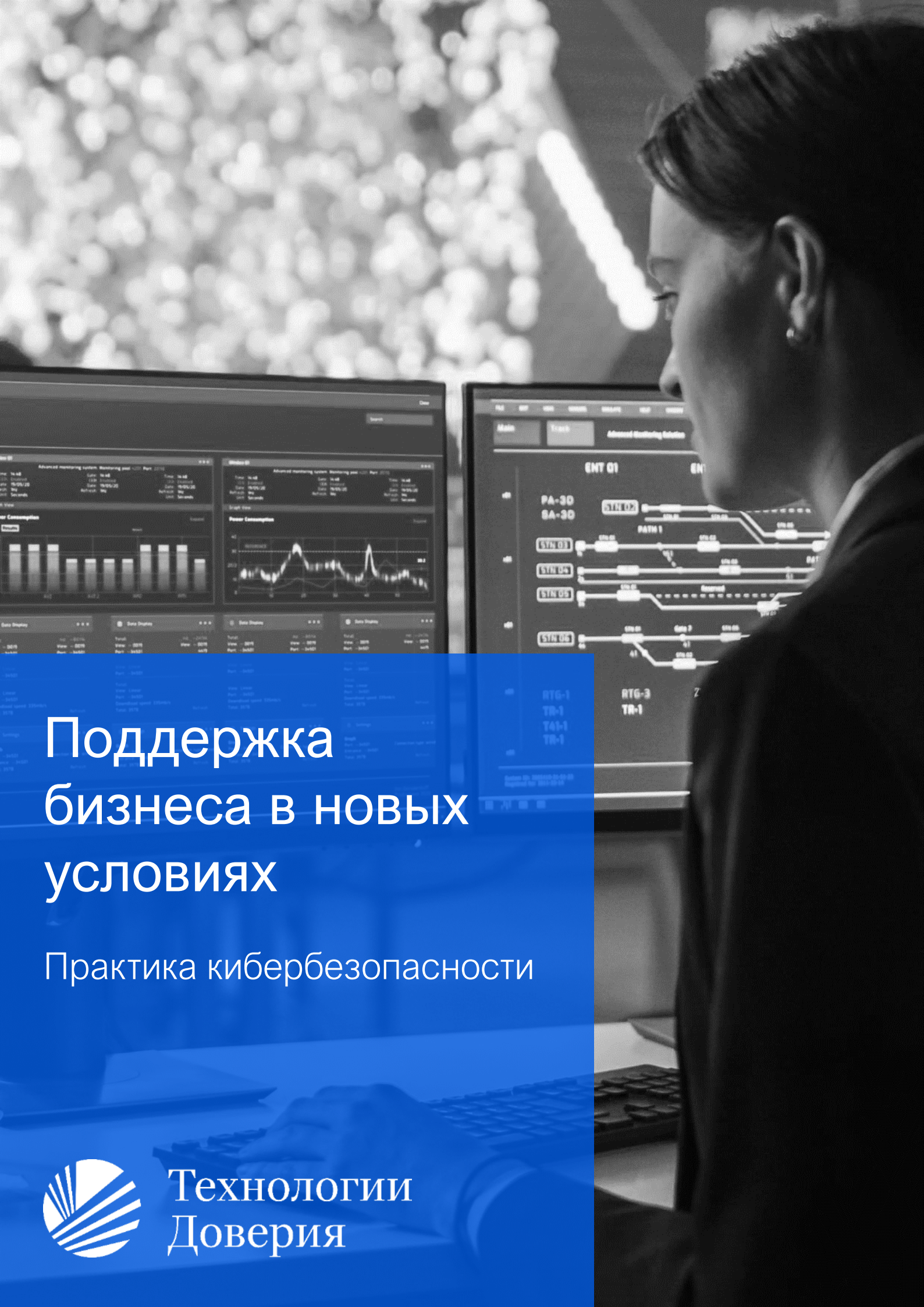

Поддержка бизнеса в новых условиях

Практика кибербезопасности

Технологии Доверия

В настоящий момент российская экономика столкнулась с новыми вызовами:

- Расширение санкций
- Уход компаний с российского рынка, приостановка их деятельности на территории РФ
- Серьезные трудности из-за валютных ограничений
- Существенное усложнение логистических схем

В этих условиях у всех компаний, работающих на российском рынке, возросли риски нарушения кибербезопасности. Среди самых распространенных угроз можно отметить:

- Массовые DDoS-атаки на инфраструктуру и государственные службы, усиливающие риски для цепочек поставок
- Нарушение непрерывности ведения бизнеса и повседневных операций в результате целенаправленных атак со стороны киберпреступников и хакерских групп
- Уход с российского рынка иностранных поставщиков услуг и решений в сфере кибербезопасности, грозящий существенным сокращением возможностей по обеспечению киберзащиты
- Распространение недостоверных новостей и усиление активности по манипулированию информацией, которые могут негативно повлиять на репутацию бренда и затруднить привлечение высококвалифицированных кадров
- Отсутствие технической поддержки зарубежных бизнес-систем, увеличивающее подверженность киберугрозам и вероятность рисковых событий и катастроф
- Целенаправленные кибератаки, направленные непосредственно на коммерческие предприятия, органы власти, финансовые учреждения и энергетическую инфраструктуру

Команда ТеДо готова оказать поддержку в адаптации ваших систем обеспечения безопасности к текущим условиям.

Услуги по поддержке бизнеса в области кибербезопасности в новых условиях

1. Архитектура кибербезопасности
2. Управление киберрисками
3. Кибербезопасность в цепочке поставок
4. Разработка стратегии M&A и выстраивание процессов при обособлении бизнеса
5. Стратегия кибербезопасности в кризисных условиях
6. Реализация регуляторных требований ИБ финансового сектора

1. Архитектура кибербезопасности

Изменения в архитектуре кибербезопасности в кратко- и среднесрочной перспективе в условиях резкого изменения геополитической ситуации вокруг Российской Федерации

Оперативные задачи

- Проактивное выявление пробелов в механизмах детектирования и противодействия вредоносной активности
- Анализ инфраструктуры кибербезопасности с целью оценки последствий от введения санкций
- Непрерывный мониторинг безопасности внешнего периметра
- Анализ защищенности и тестирование на проникновение

Стратегические задачи

- Разработка стратегии перехода к альтернативным решениям в области кибербезопасности
- Разработка или корректировка стратегии развития центра мониторинга кибербезопасности организации
- Исключение зависимости от иностранных производителей в области ключевых мер защиты

Результаты

- Оперативное повышение эффективности защиты и мониторинга кибербезопасности
- Комплекс действий, направленных на прогнозируемое изменение архитектуры кибербезопасности в условиях санкций, включая:
  - Кадровые изменения
  - Сравнение и выбор альтернативного набора средств защиты
  - Совершенствование процессов обеспечения кибербезопасности
  - План достижения целевого состояния / разработку дорожной карты
  - Бюджетную оценку
- Внедрение российских продуктов класса SIEM, DLP, BAS, WAF, IDM в рамках импортозамещения силами экспертов ТеДо

Максим Иванов

Исполнительный директор
Практика кибербезопасности
Тел. + 7 (915) 198-0362
maxim.ivanov@tedo.ru

2. Управление киберрисками

Повышение эффективности инвестиций в контрольную среду ИБ с учетом актуальных приоритетов руководства компании и профиля киберриска

Задачи

- Выявить стратегические киберриски
- Установить коммуникацию о текущем профиле киберриска на уровне совета директоров и руководства компании
- Построить систему отчетности об изменениях профиля киберриска в ходе реализации мер по его снижению
- Оптимизировать и приоритизировать операционные расходы на ИБ
- Интегрировать киберриски в модель управления рисками операционной деятельности
- Создать набор KPI и KRI, позволяющий оценивать оперативную эффективность контрольной среды ИБ

Результаты

- Обновленный процесс управления киберрисками, объединяющий усилия ключевых игроков (владельцев риска, ДИБ и ДИТ)
- Количественно оцененный профиль ключевых киберрисков
- Набор цифровых информационных панелей для визуализации профиля киберриска и усилий по его снижению
- Финансово обоснованные инициативы по снижению профиля киберрисков

Константин Бельцов

Менеджер
Практика кибербезопасности
Тел. +7 (909) 659-7412
konstantin.beltsov@tedo.ru

3. Кибербезопасность в цепочке поставок

Оценка уровня киберрисков поставщиков и партнеров в цепочке поставок

Задачи

- Оценить влияние успешных кибератак на ключевых поставщиков на операционную устойчивость компании
- Выявить уровень киберзависимости от поставщиков и партнеров
- Улучшить процесс управления рисками третьих сторон, поставщиков и партнеров
- Оценить эффективность перехода на аутсорсинговое решением «Риски третьих сторон в виде сервиса» (Third-Party-Risk Management-As-a-Service)

Результаты

- Передовая методика и инструментарий для процесса оценки рисков третьих сторон, поставщиков и партнеров
- Понимание уровня киберзависимости компании от поставщиков и партнеров в цепочке поставок
- Четкий план по снижению рисков, связанных с киберустойчивостью в цепочке поставок
- Доступные цифровые информационные панели, отражающие профиль риска третьих сторон

Константин Бельцов

Менеджер
Практика кибербезопасности
Тел. +7 (909) 659-7412
konstantin.beltsov@tedo.ru

4. Разработка стратегии M&A и выстраивание процессов при обособлении бизнеса

Обеспечение кибербезопасности бизнеса при недоступности глобальных сервисов, процессов и ресурсов

Задачи

- Выделение направлений ИБ из глобальных бизнес-процессов
- Разработка киберстратегии в процессе M&A
- Оценка избыточных бизнес-процессов в рамках регуляторных требований
- Переход на российское или доступное в условиях санкций ПО
- Оптимизация затрат на ИБ
- Консервация бизнес-процессов
- Cyber Due Diligence поглощаемых компаний

Результаты

- Обеспечен достаточный уровень функции ИБ
- Выстроен список бизнес-процессов с учетом рисков и регуляторных требований
- Реализована архитектура на основе доступных решений
- Сформирована дорожная карта инициатив ИБ, связанных с обособлением / локализацией бизнеса.
- Разработан план привлечения внешних поставщиков услуг и аутстафинга персонала
- Сформирован бюджет и целевая структура функции ИБ

Объекты исследования:

- Функции ИБ
- Средства защиты ИБ
- ИТ-ландшафт и архитектура
- Штатное расписание и компетенции
- Бюджет ИБ

Максим Иванов

Исполнительный директор
Практика кибербезопасности
Тел. + 7 (915) 198-0362
maxim.ivanov@tedo.ru

Олег Валеев

Менеджер
Практика кибербезопасности
Тел. +7 (963) 661-6873
oleg.valeev@tedo.ru

5. Стратегия кибербезопасности в кризисных условиях

Пересмотр стратегических целей и задач на пути развития кибербезопасности, адаптация операционной модели к новым условиям

Задачи

- Оценка степени влияния ИБ на деятельность компании с учетом тактических и стратегических решений, нацеленных на выход из кризиса
- Анализ запущенных и планируемых к запуску стратегических ИТ и ИБ-инициатив на предмет релевантности с учетом изменившегося ландшафта киберрисков и угроз
- Формирование дорожной карты развития ИБ
- Трансформация операционной модели ИБ (сорсинг, ФОТ, модель управления ИБ, модель взаимодействия внутренних функций между собой)
- Обоснование инвестиционных решений в ИБ на основе риск-ориентированного подхода
- Повышение осведомленности в вопросах реагирования на инциденты ИБ

Результаты

- Проведена переоценка инвестиционных решений в области ИБ
- Разработана / адаптирована дорожная карта стратегических инициатив с учетом новых условий и вводных данных
- Пересмотрена операционная модель ИБ

Максим Иванов

Исполнительный директор
Практика кибербезопасности
Тел. + 7 (915) 198-0362
maxim.ivanov@tedo.ru

Константин Бельцов

Менеджер
Практика кибербезопасности
Тел. +7 (909) 659-7412
konstantin.beltsov@tedo.ru

6. Реализация регуляторных требований ИБ финансового сектора

Повышение киберустойчивости финансовых организаций, снижение регуляторные рисков и приведение процессов ИБ в соответствие требованиям Центрального Банка РФ

Задачи

- Оценка степени реализации требований, которые установлены нормативными документами Центрального Банка РФ в области информационной безопасности для финансового сектора (ГОСТ Р 57580.1, 719-П, 683-П, 747-П, 757-П, 716-П и др.).
- Оценка выполнения требований к платежным приложениям, которые установлены Профилем защиты ОУД.4 на основе ГОСТ 15408.3.
- Реализация требований по результатам оценки соответствия для повышения уровня ИБ и достижения необходимого уровня защиты, установленного нормативными документами Центрального Банка РФ.
- Моделирование угроз по методике ФСТЭК от 2021 года для обоснования выбора технических и организационных мер, а также нейтрализации актуальных угроз.
- Разработка организационно-распорядительной документации для описания бизнес-процессов организации.

Лицензия

- Компания TeDo обладает лицензией на деятельность по технической защите конфиденциальной информацией

Результаты

- Разработана модель угроз и нарушителей
- Проведена внешняя оценка соответствия ГОСТ Р 57580, которая установлена Положениями Центрального Банка РФ
- Реализованы меры, которые требуется выполнить в соответствии с регуляторными требованиями
- Разработан необходимый комплект внутренних документов по информационной безопасности

Максим Иванов

Исполнительный директор
Практика кибербезопасности
Тел. + 7 (915) 198-0362
maxim.ivanov@tedo.ru

Олег Валеев

Старший менеджер
Практика кибербезопасности
Тел. +7 (963) 661-6873
oleg.valeev@tedo.ru

Контакты

Анна Черникова
Партнер технологической практики
Тел. +7 (495) 967-6000
anna.chernikova@tedo.ru

Максим Иванов
Исполнительный директор
Практика кибербезопасности
Тел. + 7 (915) 198-0362
maxim.ivanov@tedo.ru

Константин Бельцов
Менеджер
Трансформация кибербезопасности
Тел. +7 (909) 659-7412
konstantin.beltsov@tedo.ru

Олег Валеев
Старший менеджер
Кибербезопасность
финансовых организаций
Тел. +7 (963) 661-6873
oleg.valeev@tedo.ru

«Технологии Доверия» (www.tedo.ru) предоставляет аудиторские и консультационные услуги компаниям разных отраслей. В офисах «Технологий Доверия» в Москве, Санкт-Петербурге, Екатеринбурге, Казани, Новосибирске, Ростове-на-Дону, Краснодаре, Воронеже, Владикавказе, Перми и Нижнем Новгороде работают 3 000 специалистов. Мы используем свои знания, богатый опыт и творческий подход для разработки практических советов и решений, открывающих новые перспективы для бизнеса.