КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ИТОГИ

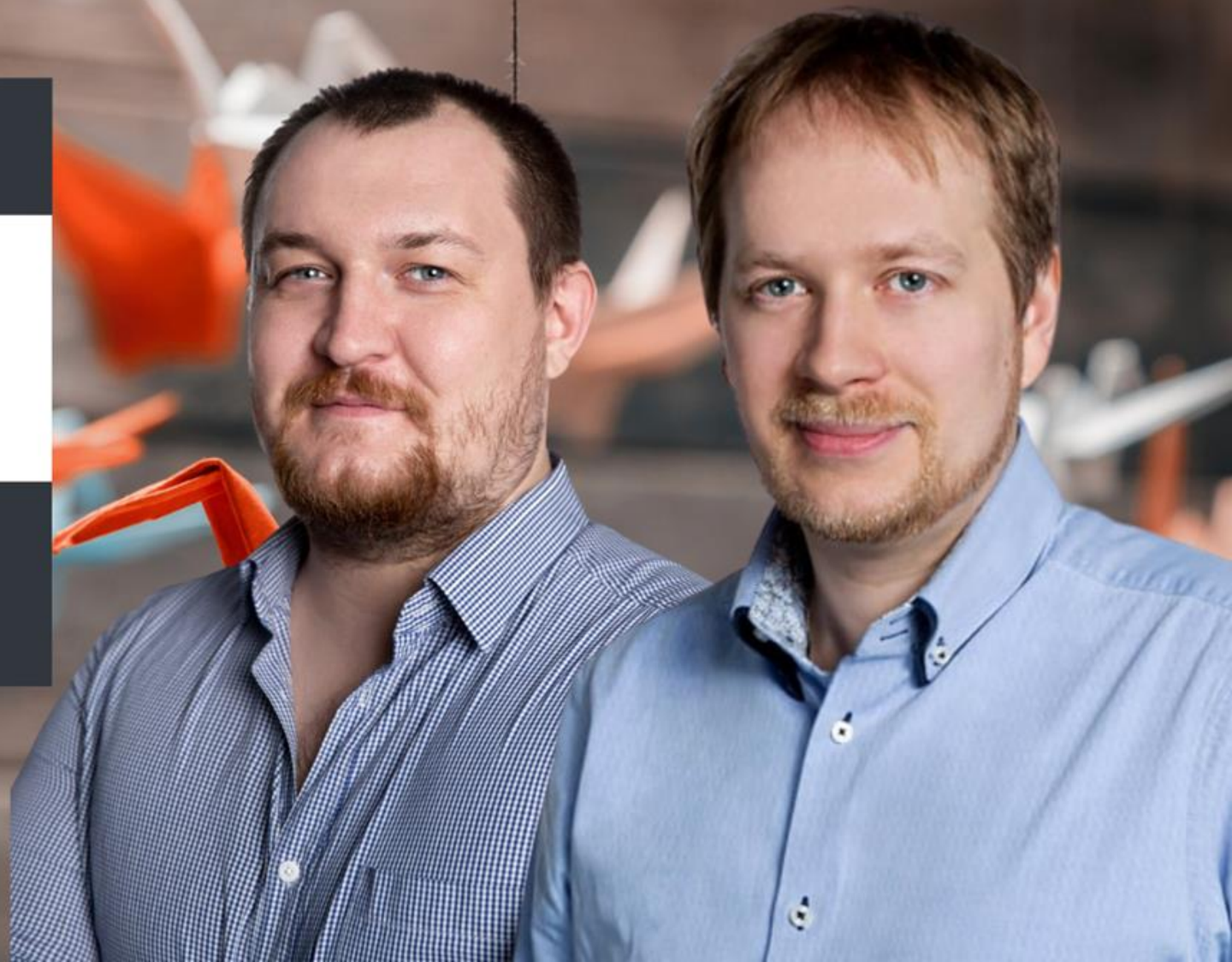
КОД ИБ ИТОГИ | 08 ДЕКАБРЯ 2022

ВЛИЯНИЕ ТЕКУЩЕГО ГЕОКРИЗИСА НА КАРТУ РИСКОВ ИБ

АРТЕМ СИДОРОВ, РОСБАНК

АЛЕКСАНДР КОНДРАТЕНКО, РОСБАНК

МОСКВА



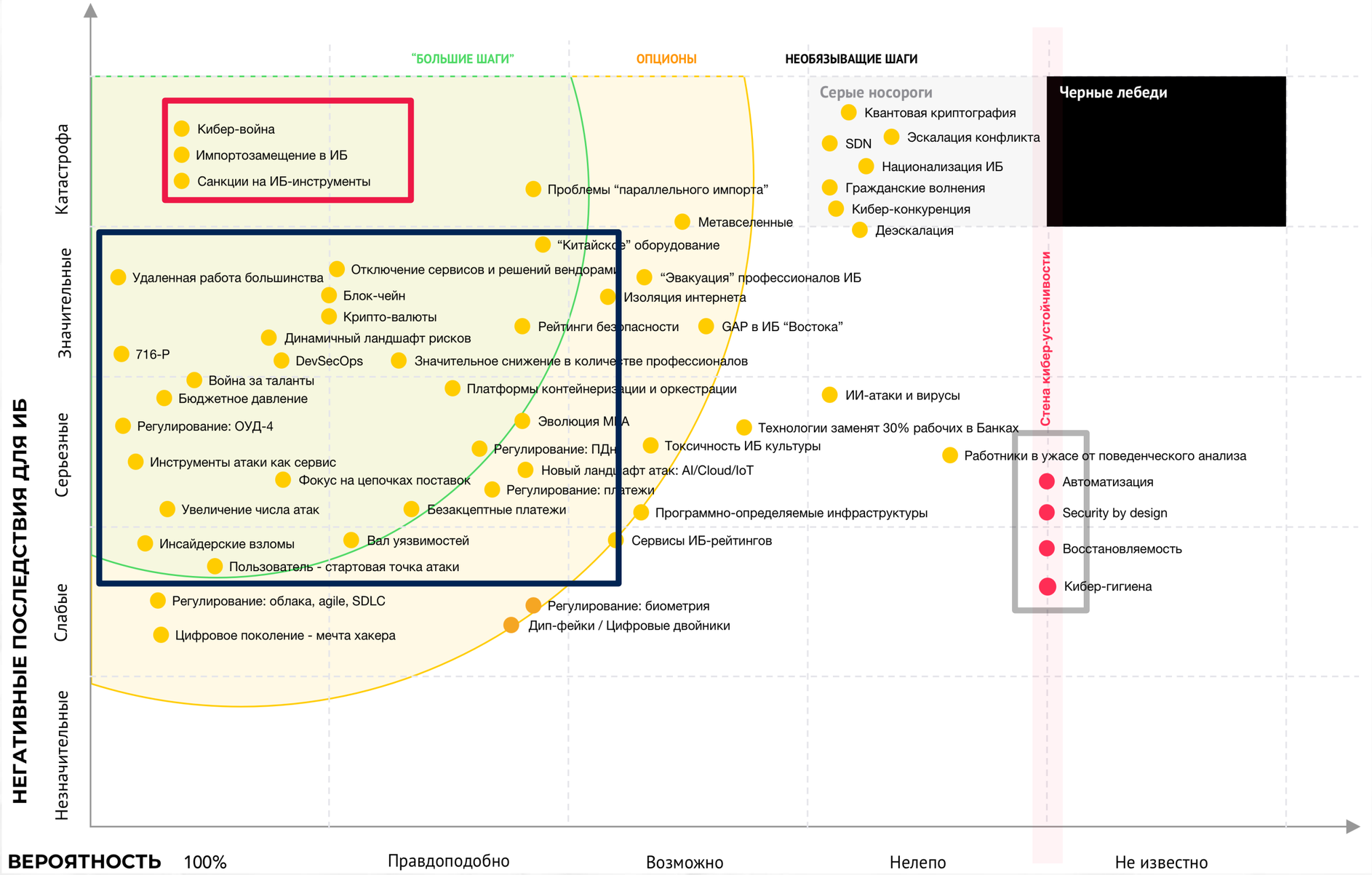
Вызовы ИБ

Внешний контекст

Реализация «**серых носорогов**» в первой половине 2022 года

Большинство прогнозируемых год назад событий в той или иной степени **реализовались или близки к этому**

Некоторые защитные меры от эффектов «черных лебедей»



«Полярный экспресс»

В прошлом году мы отмечали тренд на усилившуюся поляризацию мнений вокруг любого события. Произошедшие события стали «катастрофической» точкой поляризации всего мира. Причем не только в «комментах», а в реальных активных действиях по нанесению деструктивных последствий представителям сторон.

Внутренние злоумышленники с альтернативной точкой зрения наносят реальный и значительный вред компаниям, в которых работают

Значительно снижается доверие open-source, куда авторы вносят специальные деструктивные закладки, направленные на лиц с альтернативной точкой зрения

Активные акторы в кибер-пространстве получают армию соратников (**не мотивированных финансово**), которыми могут управлять для осуществления атак (в первую очередь, DDoS)

«Восточный экспресс»

Если годом ранее мы прогнозировали относительно медленный разворот России в сторону Востока, то с началом 2022 года фактически происходит полный разрыв с «западным» миром, как экономически, так и технологически

94

По данным на 8 сентября в кибервойне участвовали 94 хакерские группы (43 про-российские и 35 про-украинские), из которых 17 спонсируются государствами

Отдельные лица / ИТ-армия Украины
«Просто установи нужный софт»

Хакерские группировки
Разработка, поиск уязвимостей и фишинг

Государственные службы (ГУР, СБУ)
Координация, определение целей

Такие объединения предполагают совсем другой уровень возможностей и выбора целей атаки: атакующих интересуют не только финансы, но и социальный и политический эффекты.

Нестабильность финансовой системы государства – один из приоритетов.

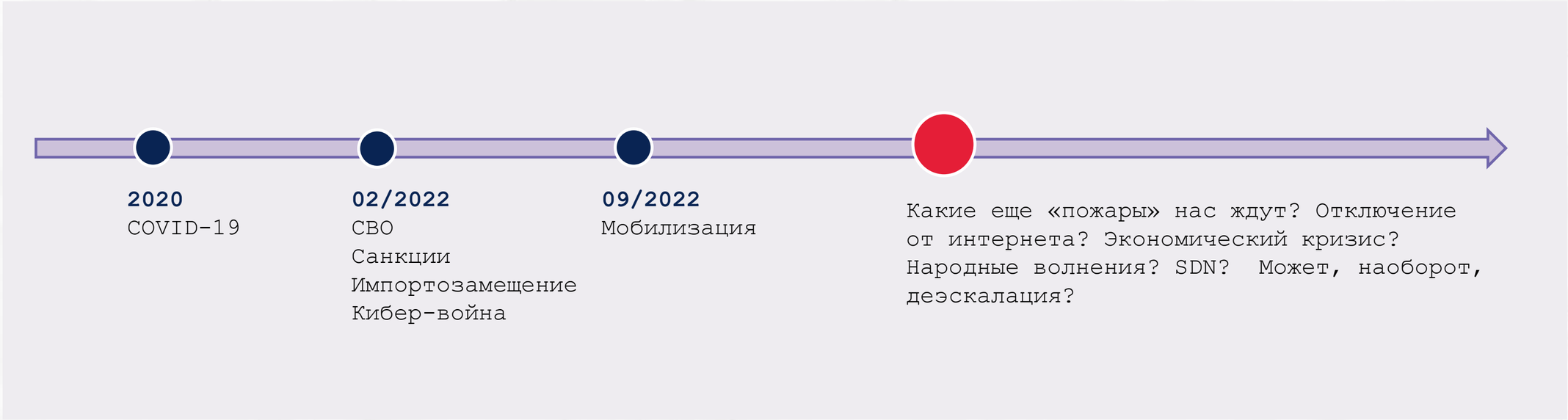
Разрушительный эффект

Ситуация является катализатором изменений во всей сфере ИБ:

- Нормативные требования
- Импортозамещение
- Технологии и техники защиты
- Участие государства в ИБ
- …

Динамичность ситуации

При анализе контекста мы видим значительную динамичность ситуации во всех контекстах: внутреннем, внешнем и групповом



> Чем динамичнее ситуация, тем сложнее её предвидеть. Поэтому в неопределенных ситуациях следует ставить перед собой максимально близкие стратегические цели.
> – **Ричард Румельт**

Группы рисков

Мы внедрили риск-ориентированный подход, используя собственную модель рисков, состоящей из групп рисков. Каждая группа – это мастер-сценарий события с неприемлемым ущербом. В операционной работе риски уточняются в конкретные сценарии по процессам или системам при каждом изменении.

Киберпреступность

- Потенциальные изменения конфигурации ИТ и СЗИ со стороны вендора
- Атаки на цепочку поставок и контрагентов
- Всплески DDOS-атак (влияние на операционную работу сотрудников)
- Внешние инциденты ИБ (информация в СМИ), в т.ч. с участием подрядчиков
- Резкий рост случаев корпоративного шпионажа с участием сотрудника
(53 инцидента за 6 мес.)

Регуляторные риски

- Регуляторная амнистия в части проведения проверок
- Множество новых требований от регуляторов:

ЦБ – 91

ФСТЭК – 252

НКЦКИ (ФСБ) – 153

Организационные сложности

- Постоянный пересмотр бизнес-приоритетов
- Невозможность закупки оборудования и ПО из-за санкций
- Риск непредоставления услуг ИБ внутренним заказчикам

Недостаток человеческих ресурсов

- Уход / иммиграция сотрудников в другие страны
- Мобилизация сотрудников
- Перегрузка сотрудников, срывы сроков задач

Риски в центре принятия любых ИБ-решений

Стратегические семинары

Мы регулярно калибруем стратегию, чтобы находиться в актуальном контексте: куда и как движутся организация, страна и мир

R&O семинары

Мы регулярно определяем факторы риска и возможности, вытекающие из изменения контекста работы функции ИБ

Оценка рисков

Факторы риска и показатели контрольной среды определяют вероятность и потенциальный ущерб от рисков

Выбор защитных мер

Исходя из рисков и возможностей мы выбираем меры защиты для всех контрольных сред, будь то проект, команда, дочка или Банк

Реализация

Выбранные меры защиты от риска формируются в конкретное решение: стратегию, программу, защиту ИБ проекта, KPI, OKR