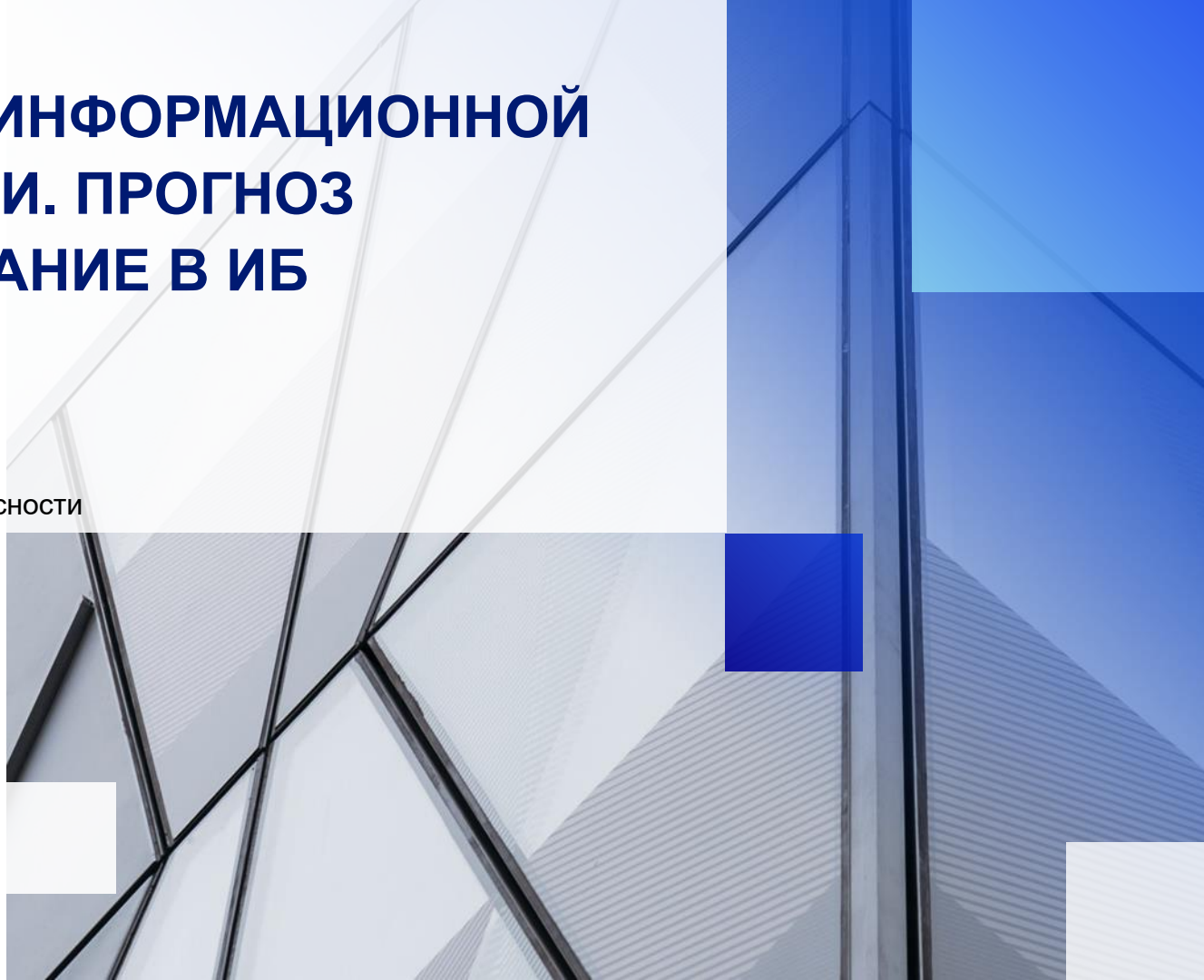
АРХИТЕКТУРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. ПРОГНОЗ И МОДЕЛИРОВАНИЕ В ИБ

Подход IBS

Олег Босенко

Директор дирекции кибербезопасности

2023, Москва



Почему IBS?

30+
квалифицированных
специалистов

- Собственная методология прогнозирования развития кибербезопасности, поддержанная моделированием в связке с НПА и решениями регуляторов
- Устойчивое партнерство с основными отечественными ИБ-компаниями, производителями средств ИБ*
- Лицензии ФСТЭК, ФСБ на виды деятельности в области информационной безопасности

Комплексные проактивные решения по обеспечению кибербезопасности для защиты систем любого назначения и уровня сложности. Формирование защиты от угроз ИИ

* НПА – нормативно правовые акты, **ИБ – информационная безопасность

Кибербезопасность в IBS

Направления деятельности

Актуальные особенности кибербезопасности

- Взрывной рост количества сложных кибератак (в том числе с применением методов социальной инженерии) и утечек конфиденциальной информации
- Появление нового типа угроз, связанных с применением искусственного интеллекта, машинного обучения
- Активизация госрегулирования в области ИБ, издание целого ряда новых нормативных документов ужесточение ответственности за нарушения
- Санкции. Уход из России ряда крупных вендоров. Переход на отечественные, в том числе сертифицированные решения. Импортозамещение
- Тенденция к росту рынка ИБ, количества ИТ-стартапов, расходов на ИБ (закупка защищенных ОС, СЗИ, сопутствующих услуг)

Проблематика существующей архитектуры

1

Необходимость разработки и внедрения новых архитектурных решений по кибербезопасности и уточнения процессной модели ИБ в связи с уходом с отечественного рынка иностранных вендоров ИТ и ИБ и появлением угроз ИИ

2

Снижение эффективности применяемых средств кибербезопасности в условиях резко изменившейся с февраля 2022 года обстановки

3

Наличие у недружественных государств базовой информации о построении ИБ, а также информации о базовых настройках импортного оборудования ИБ и ИТ

4

Реактивный характер архитектуры кибербезопасности (реакция на инцидент) на настоящем этапе

Парадигма изменения архитектуры кибербезопасности

Подход IBS

Базовый вектор развития ИБ

As is – реактивная кибербезопасность
Основа – реакция на угрозы и инциденты

» На базе методологии от IBS »

To be – проактивная кибербезопасность
Блокирование и недопущение угрозы до ее активизации

Основные направления формирования проактивной архитектуры кибербезопасности

- Создание перспективных систем и средств кибербезопасности с поддержкой ИИ
- Создание систем и средств проактивной кибербезопасности, блокирующих угрозы ИИ
- Прогнозный стратегический консалтинг и моделирование информационной безопасности на базе прогноза
- Формирование методологии проактивной архитектуры кибербезопасности на базе собственных продуктов и продуктов партнеров

Периметр комплексного рассмотрения кибербезопасности

- **Техническая политика и политика внешнего информационного взаимодействия**
- **Корпоративная культура защищенного информационного обмена и нормативное регулирование кибербезопасности**
- **Методология оценки и минимизации рисков информационных процессов**
- **Физическая защита информационных объектов и информационного периметра**
- **Мониторинг действий персонала и анализ поведенческой ситуации**
- **Финансовое и материальное обеспечение кибербезопасности**

Угрозы связанные с искусственным интеллектом

Прогрессирование кибератак в количественном и качественном соотношении, масштабе ущерба

Рост возможностей внутреннего нарушителя в несанкционированном доступе к информации

Риск повреждения или уничтожения баз данных и ML за счет взлома механизмов AI

Повышение риска вывода из строя производственных систем

Повышение информированности нарушителей за счет оперативного доступа к больших объемам информации о кибератаках

Появление новых классов атак на имидж

Предпосылки реализации прогнозирования в ИБ

- Тотальная цифровая трансформация
- Развитие отечественного ИТ-рынка
- Наличие источников информации о прогрессировании кибератак
- Проактивная политика в области кибербезопасности
- Импортозамещение в целях обеспечения устойчивости бизнеса в текущих геополитических условиях. Соблюдение требований регуляторов
- Применение методики и алгоритмов риск-ориентированного подхода

Структура входных данных

По результатам обследования для прогноза информационной безопасности

- **Организационная структура и актуальная карта процессов ИБ**
- **Контроль и мониторинг ИБ**
- **Нормативное обеспечение ИБ**
- **Анализ инцидентов ИБ и анализ функционирования инцидент-менеджмента**
- **Техническое состояние, функциональность и техническая готовность системы ИБ**
- **Планируемые мероприятия по ИБ, в том числе связанные с реорганизацией бизнеса**

Возможности прогнозирования ИБ

Структурирует информацию по видам угроз

Учитывает ситуацию развития ИТ-технологий

Позволяет оценить угрозы и заблаговременно принять меры по устранению или минимизации рисков возможных киберугроз

Анализирует готовность отражения прогрессирующих кибератак компаниями разных отраслей

Позволяет отследить характер и динамику изменения поведения злоумышленников

Преимущества прогнозной модели анализа ИБ

1. Провести детальный анализ текущего состояния защищенности информационных систем от киберугроз
2. Структурировать информацию по возможным рискам кибербезопасности
3. Оценить вероятные потери до/после применения методов нивелирования рисков кибербезопасности
4. Смоделировать варианты информационной защиты для объектов, наиболее подверженных к различного рода киберугрозам
5. Сформировать прогноз развития характера киберугроз
6. Сфокусировать внимание на особо критичных рисках и угрозах в прогнозный период
7. Оценить эффективность ИБ ОКИИ при изменении и нарастании атак

ПК* моделирования эффективности ИБ

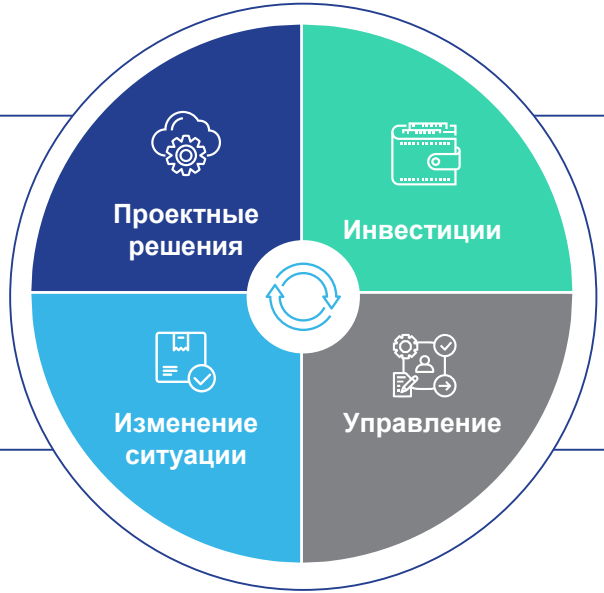
Концепция применения

* Программный комплекс

Эффект от применения ПК моделирования ИБ

Оценка эффективности различных архитектурных решений

Оперативная выработка решений в рамках СУИБ



Оценка эффективности инвестрешений на этапе их подготовки

Возможность управления ИБ на базе одного комплексного решения

ПК* моделирования эффективности ИБ объекта КИИ

Концепция применения

Анализ эффективности проектных решений с учетом оценки рисков

Ведет оценку рисков ИБ в agile-формате

Встраивается в инфраструктуру ИБ ОКИИ

Анализ эффективности функционирования ИБ ОКИИ и моделирование вариантов действий

Центр ситуационного управления ИБ ОКИИ

Автоматически взаимодействует с ГОССОПКА (при необходимости)

Первичное обучение на киберполигоне
Обучение на массиве реальных данных

Формирование управленческих решений СУИБ

* Программный комплекс

Модель реализации кибербезопасности