BIS SUMMIT 2018
ST. PETERSBURG

БЕЗОПАСНОСТЬ
ЦИФРОВОЙ ЭКОНОМИКИ
СЕВЕРО-ЗАПАДНОГО РЕГИОНА

Скородумов Анатолий Валентинович

Белые пятна информационной безопасности 2018

ПАО Банк Санкт-Петербург

Сфера ИБ последние годы активно развивается

Причины:

- Требования законодательства и регуляторов
- Увеличение числа и разнообразия кибератак
- Рост потерь от кибератак
- Повсеместный переход на электронные (безбумажные) способы информационного обмена
- Рост осознания важности вопросов ИБ
- Восприятие ИБ, как одного из критериев качества продукта или услуги

Мы так и не научились оценивать риски ИБ

2009 волна несанкционированных списаний в системах ДБО

Наличие на компьютерах пользователей вирусов + **Наличие на компьютерах пользователей криптоключей** = ?

2017 несколько широкомасштабных атак вирусов-шифровальщиков

Постоянные атаки вирусов-шифровальщиков + **Возможность распространения вирусов через уязвимости в ПО** = ?

Прошло 8 лет и ??????????????????????????????

Комплаенс-безопасность - удел большинства

Причины отсутствия процесса по оценке рисков:

- Сложность существующих методик оценки рисков ИБ
- Отсутствие специалистов нужной квалификации
- Отсутствие статистики по инцидентам ИБ и потерям от них
- Отсутствие развитых средств автоматизации по оценке рисков ИБ
- Сложность современных ИТ-систем

80% компаний не смогут наладить у себя эффективный процесс оценки рисков ИБ в ближайшие годы

- Необходимая базовая РАБОЧАЯ модель угроз для ИТ-инфраструктуры организации, отраслевые модели угроз.
- Необходим стандарт(ы) с документами более низкого уровня и описаниями best practice для обеспечения эффективности Комплаенс-безопасности

Неусвоенные уроки 2017 года

1. Существует высокая вероятность, что в результате кибератаки значительная часть ИТ-инфраструктуры вашей организации будет выведена из строя за считанные минуты
2. Минимизировать риски данной угрозы до приемлемого уровня не представляется возможным
3. Попасть под такую кибератаку может практически любая организация

«Белые пятна» классической системы ИБ

Повышение осведомленности персонала

Невозможно обеспечить «достаточный» уровень осведомленности персонала.

Управление уязвимостями

Мы не сможем обновлять системы раньше, чем будут выходить готовые эксплоиты под эти уязвимости.

С учетом скорости обновлений в прикладных АС, их количества и сложности мы не сможем обеспечить эффективное выявление уязвимостей в них

Управление правами доступа

Количество и скорость изменений в бизнесе, в ПО и функциях подразделений не позволяет поддерживать ролевую модель в актуальном состоянии

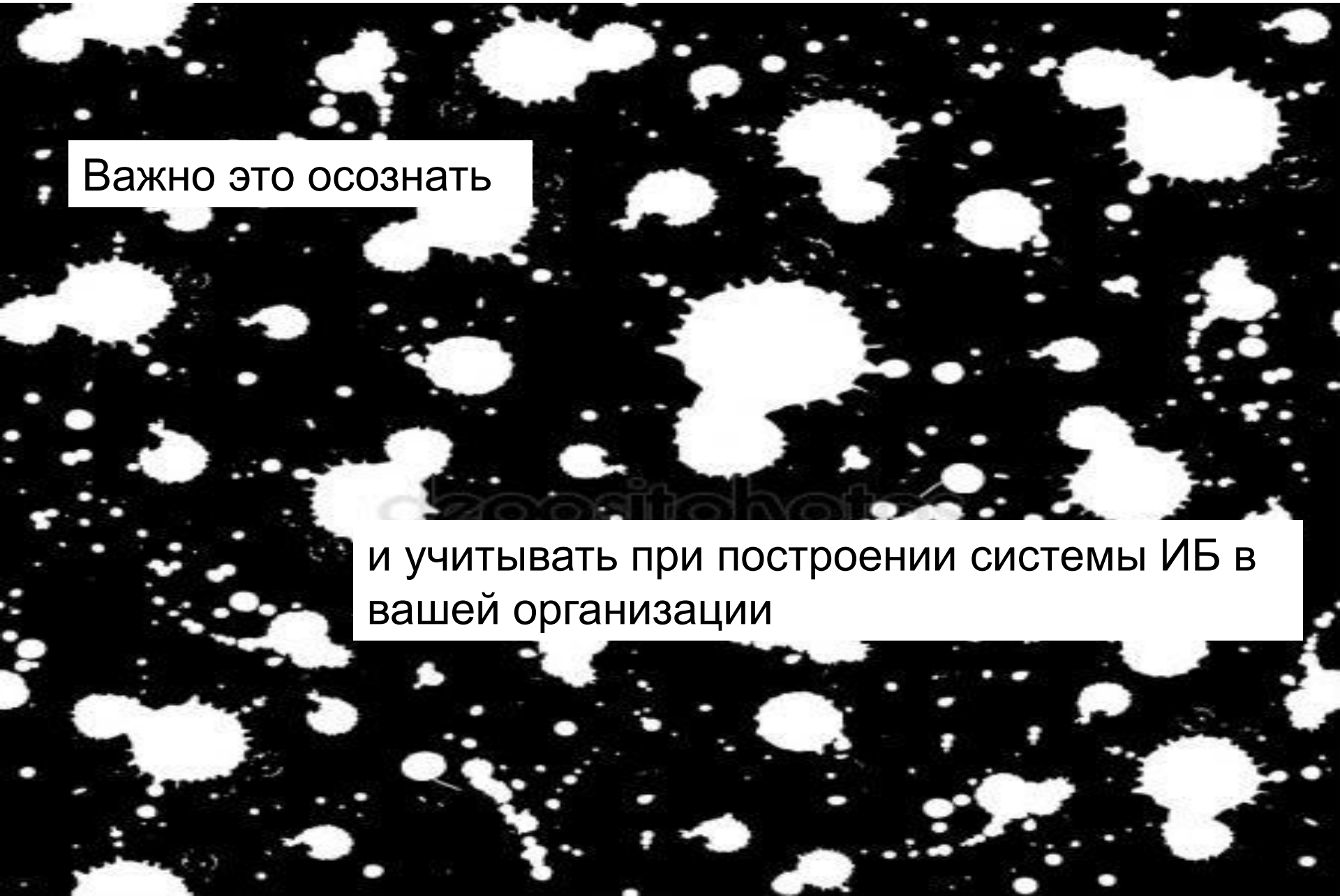
Новые реалии требуют новых подходов

- Методы ограничений и запретов работают не всегда и не везде
- Необходимо оценивать не столько безопасность той или иной технологии, а последствия «взлома» этой технологии
- Необходимо внедрять несколько аналогичных технологии ИБ с возможностью отказа от одной из них в случае компрометации
- ИТ и ИБ должны работать как одно целое
- Построить эффективную защиту возможно только во взаимодействии с ведущими российскими и международными компаниями по ИБ
- Акцент на киберустойчивость

Киберустойчивость – выживут только подготовленные

- Пересмотр планов обеспечения непрерывности бизнеса
- Пересмотр выбранных принципов резервирования систем и данных
- Совершенствование методов мониторинга, выявления и реагирования на инциденты ИБ: мониторинг внутренней сети организации и рабочих станций, сбор и корреляция максимального количества событий, использование систем выявления аномалий
- Проведение киберучений
- Донесение до руководства основных принципов киберустойчивости

Белые пятна в ИБ – объективная реальность



BIS SUMMIT 2018
ST. PETERSBURG

Скородумов Анатолий Валентинович
E-mail: skorodumov@mail.ru

ПАО Банк Санкт-Петербург