Повышение уровня зрелости процессов информационной безопасности как часть цифровой трансформации бизнеса

Валерий Степанов

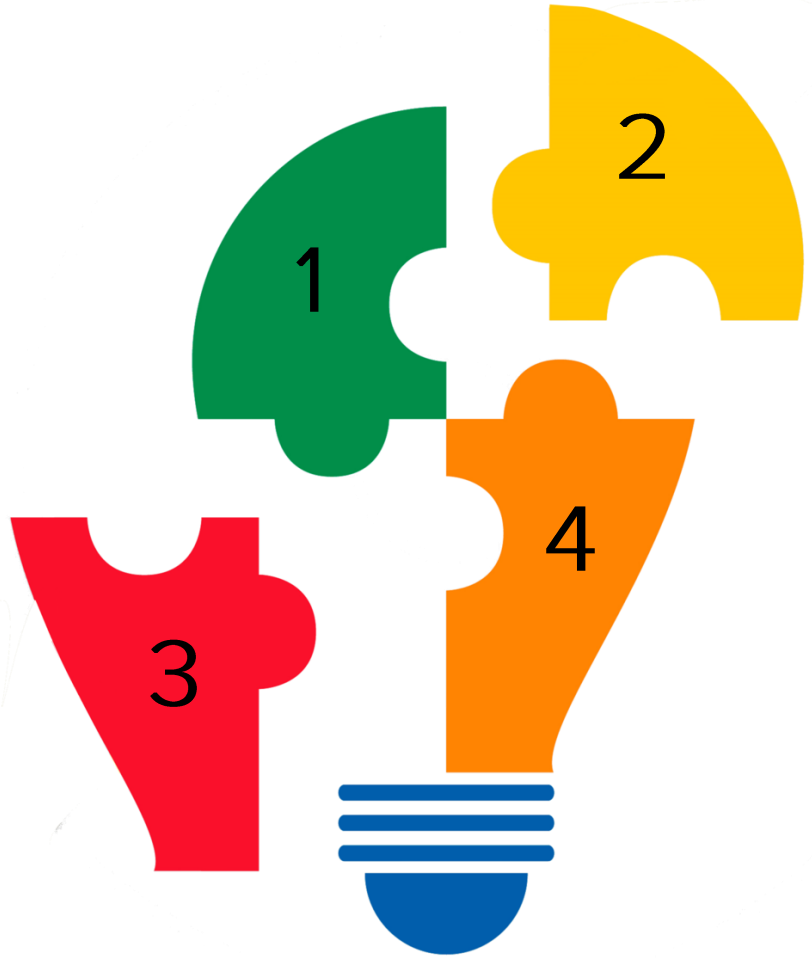
Руководитель отдела аудита и консалтинга департамента систем безопасности, BSS

2020г.

BSS SECURITY

Цифровая трансформация

Цифровизация (Digitalization) – это создание нового продукта в цифровой форме.



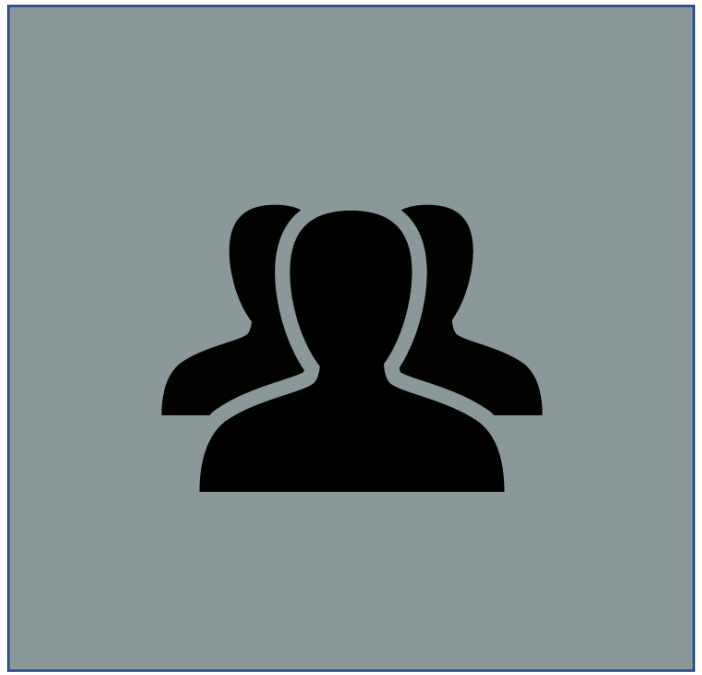
1. Стратегическое планирование
2. Развитие in-house компетенций
3. Фокус на технологии
4. Пересмотр целей и KPI

BSS SECURITY

ДБО – часть трансформации

Банк

Организация



BSS SECURITY

Проблемы ИБ в Банках и их источники

Регуляция ЦБ РФ:

- Новые законы и Положения

Взломы и заражения:

- Устаревшее ПО
- Недостаток СЗИ
- Человеческий фактор

Мошенничество:

- Самописное ПО
- Человеческий фактор

BSS SECURITY

Регуляция ЦБ: Оценка соответствия 382-П

< 0.50	Неудовлетворительная
≥ 0.50, но < 0.70	Сомнительная
≥ 0.70, но < 0.85	Удовлетворительная
≥ 0.85	Хорошая

1. Самооценка Банка = 0,9

2. Независимая оценка соответствия = 0,6

3. После приведения в соответствие = 0,87

BSS SECURITY

Мошенничество:

Кейс с выдачей онлайн кредита

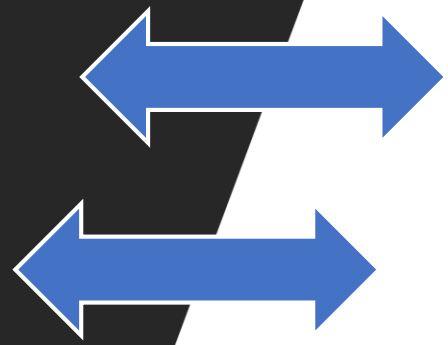
BSS SECURITY

Взаимосвязь процессов ИБ и бизнес-процессов

ИТ-обеспечение и связь

Обслуживание физических лиц (вклады ФЛ)

Обслуживание юридических лиц (подключение к ДБО)



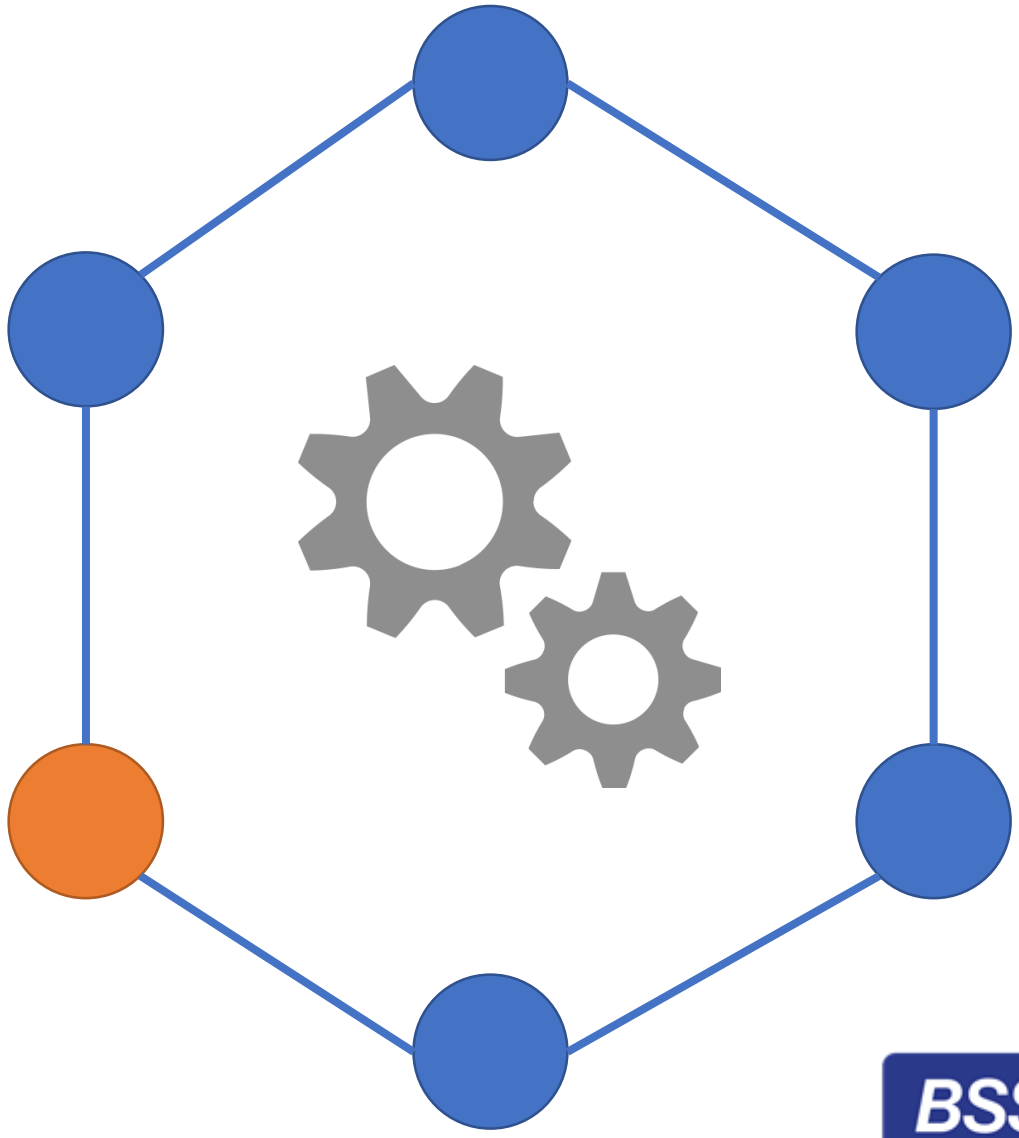
1. Управление инцидентами
2. Управление изменениями
3. Физическая безопасность
4. Управление идентификацией и доступом
5. Идентификация и управление ИТ активами
6. Управление рисками ИБ
7. Управление комплаенсом
8. Управление ЖЦ АС
9. Обеспечение непрерывности бизнеса
10. Управление уязвимостями
11. Обучение и повышение осведомленности

BSS SECURITY

Взаимосвязь процессов ИБ и бизнес-процессов

На примере процесса управления доступом

Риск возникновения инцидента информационной безопасности!



BSS SECURITY

Уровень зрелости процессов ИБ и их оценка

Это оценка уровня прогресса, достигнутого в обеспечении безопасности в повседневных и стратегических задачах.

Уровень	Описание
1	Отсутствие регламента. Процесс выполняется не регулярно.
2	Регламент существует. Процесс описан, но выполняется периодически.
3	Регламент существует. Процесс описан, выполняется корректно. Используется достаточное количество ПО для выполнения, поддержки и управления.
4	Регламент существует. Процесс описан, выполняется, управляется и контролируется.
5	Регламент существует. Процесс описан, выполняется, управляется и контролируется. Измеряется при помощи качественных и количественных показателей (метрики и KPI)

BSS SECURITY

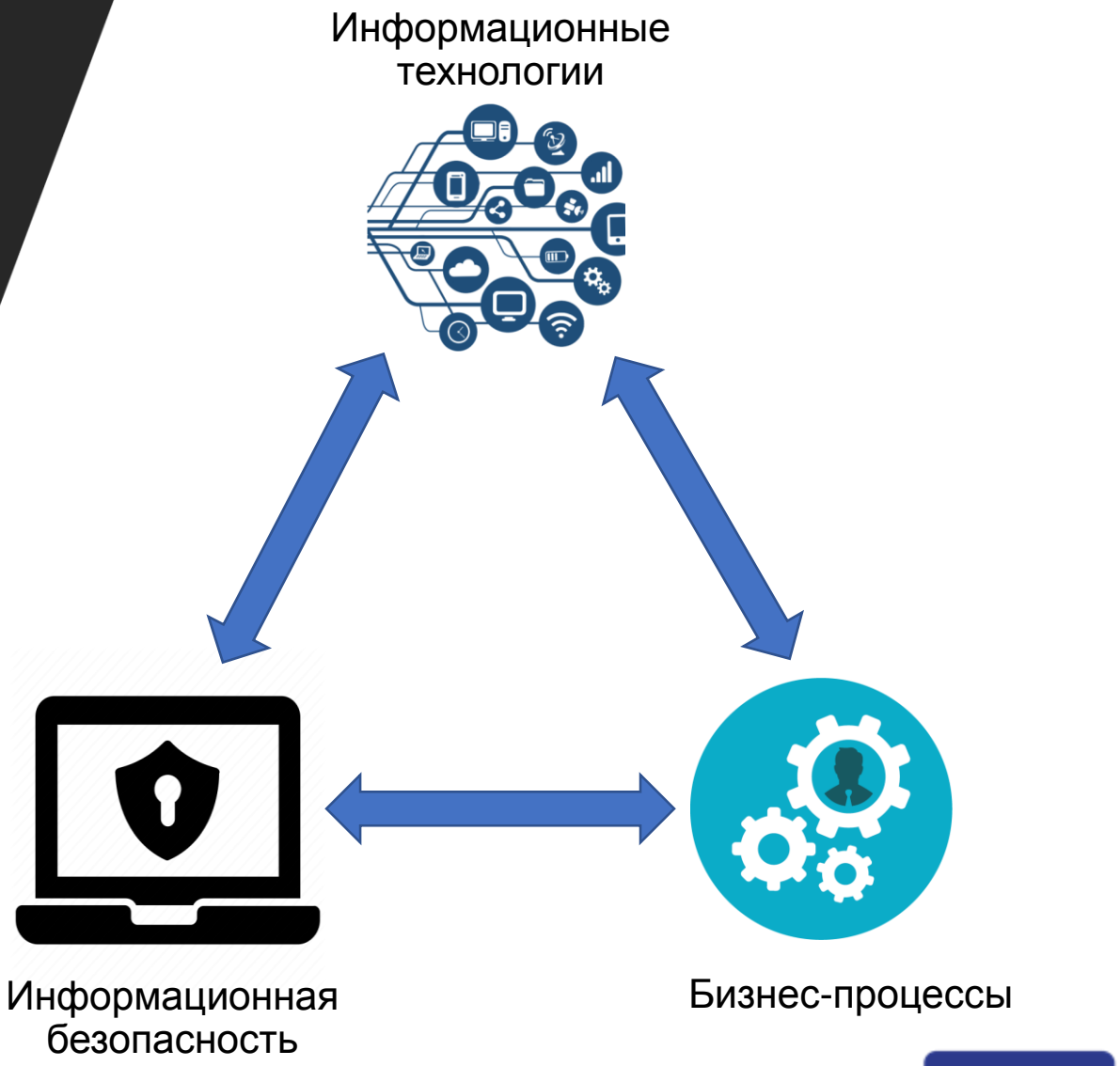
Методы поиска проблемы

Важно: диагностика и идентификация слабых мест возможна только с использованием комплексного подхода

Аудит ключевых процессов

Тестирование на проникновение

Информационная безопасность – ваш друг



BSS SECURITY

Наши клиенты

ТОП-10: ПАО Сбербанк, Банк ВТБ (ПАО), Банк ГПБ (АО), ПАО Банк «ФК Открытие», АО «Россельхозбанк», АО «ЮниКредит Банк», ПАО «Промсвязьбанк»

ТОП-30: Банк «ВБРР» (АО), ПАО «АК БАРС» БАНК, ПАО «УРАЛСИБ», ПАО КБ «Восточный», АО АКБ «НОВИКОМБАНК», ПАО АКБ «Связь-Банк», Банк «Возрождение» (ПАО), ПАО КБ «УБРиР», АО «Райффайзенбанк»

ТОП- 50: ПАО «МТС-Банк», АО «Кредит Европа Банк», АО «Нордеа Банк», ООО «ХКФ Банк», АО «Банк ДОМ.РФ»

ТОП-100: ПАО КБ Центр-инвест, АО «Тойота Банк». «СДМ-Банк» (ПАО), АКБ «ФОРА-БАНК» (АО)

BSS SECURITY

СБЕРБАНК

ГАЗПРОМБАНК

ВОЗРОЖДЕНИЕ БАНК
БАНК, КОТОРЫЙ ВСЕГДА С ТОБОЙ

ВТБ

Связь Банк

ДОМ РФ БАНК

СКБ-БАНК

Кредит ЕвропаБанк

РоссельхозБанк

СОВКОМБАНК

открытие БАНК

ВБРР

МТС Банк

UniCredit Bank

РОСГОССТРАХ БАНК

БПС-СБЕРБАНК

Уральский Банк реконструкции и развития

БАНК САНКТ-ПЕТЕРБУРГ

Ак Барс Банк

Nordea

Контакты

security@bssys.com