

beeline **cloud**

вебинар

# Как повысить уровень ИБ в любой КОМПАНИИ

Самое главное, о чем все и всегда забывают

# Спикеры



**Александр Митусов**

Руководитель по сопровождению продуктов  
кибербезопасности, beeline cloud



**Алексей Горелкин**

Генеральный директор,  
Phishman

# Программа вебинара

- 01 Слабое звено в ИБ: с какими проблемами сталкиваются компании
- 02 Как повысить уровень ИБ в организации
- 03 Что такое Cloud SA и как грамотно выстроить процесс кибергигиены
- 04 Демо: как настроить тестовые атаки, примеры шаблонов, конфигурация правил
- 05 Пошаговый путь к киберустойчивости организации
- 06 Вопросы и ответы

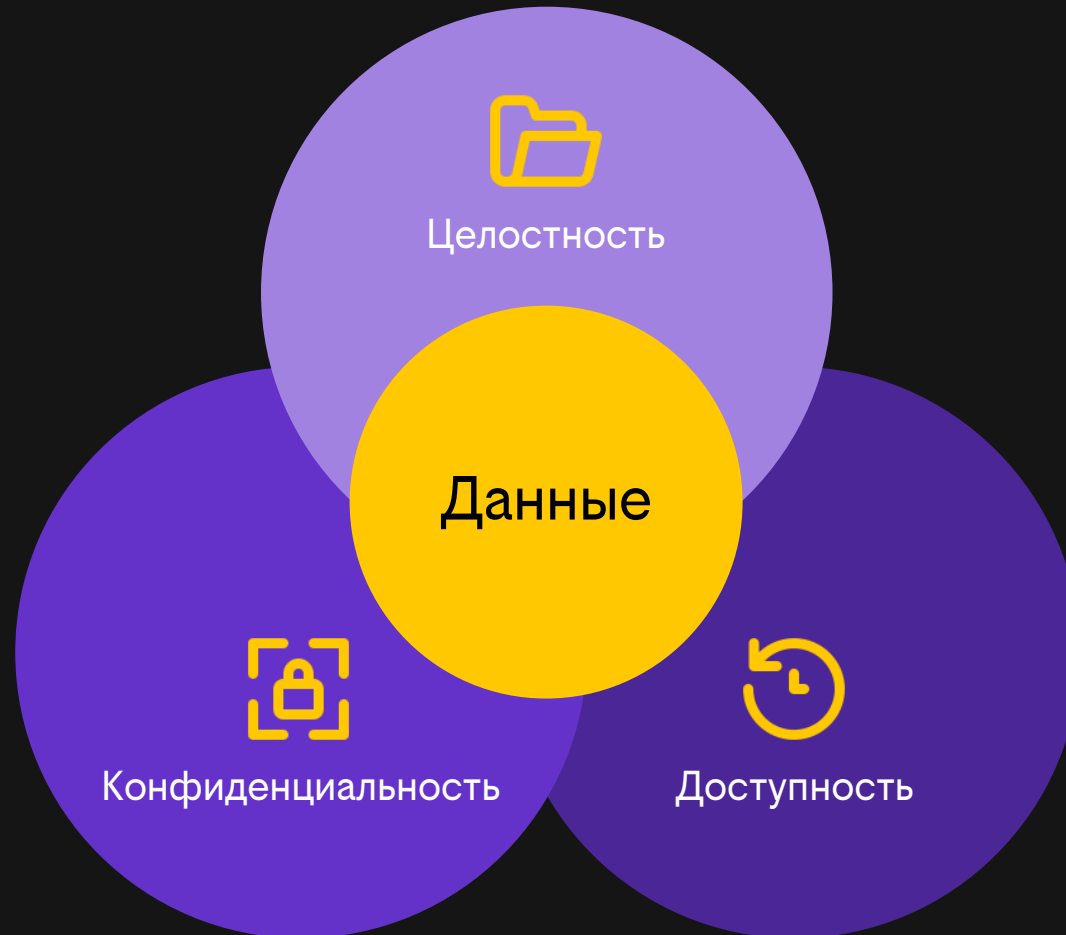


# Алексей Горелкин

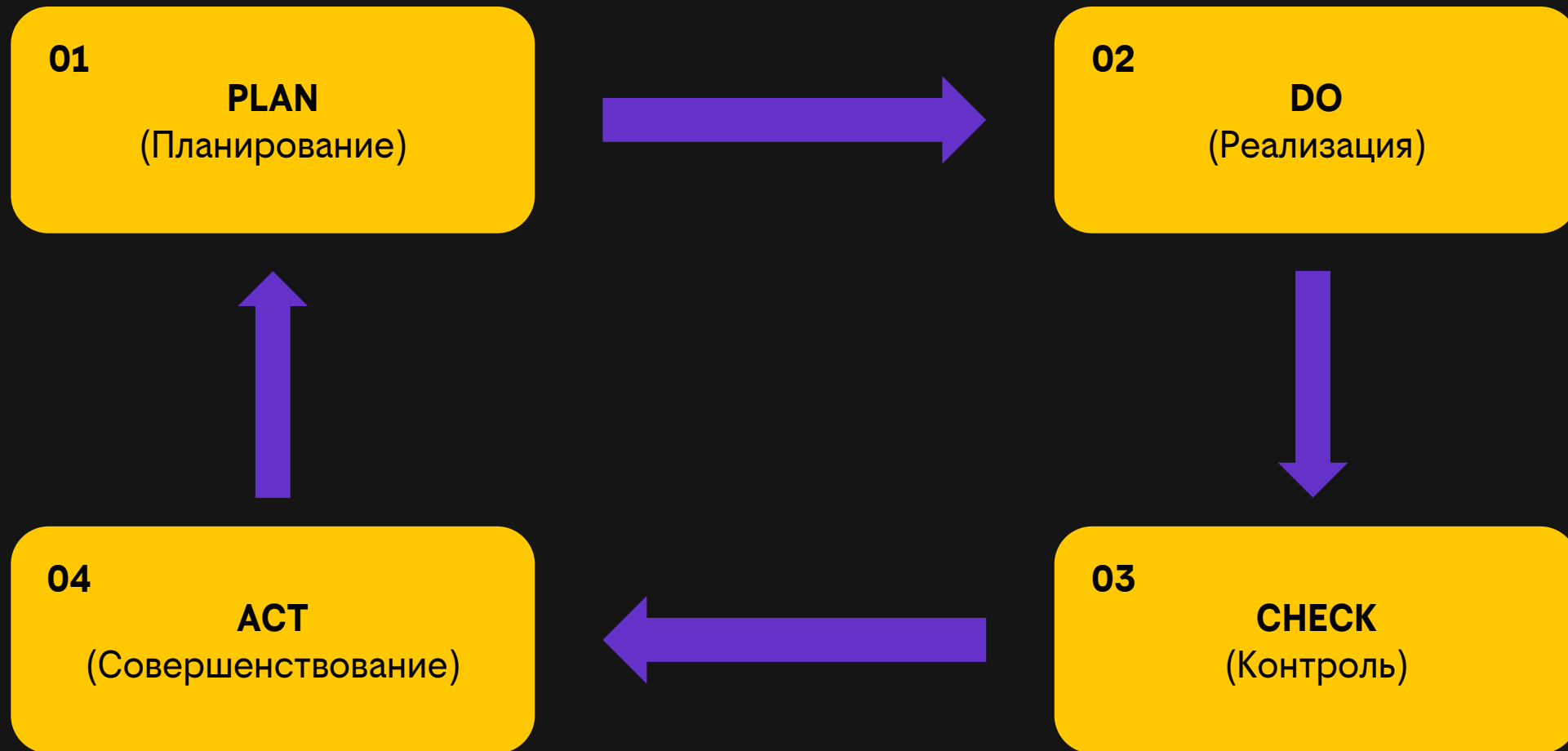
Генеральный директор,  
Phishman

01

# Что такое информационная безопасность



# Что такое информационная безопасность



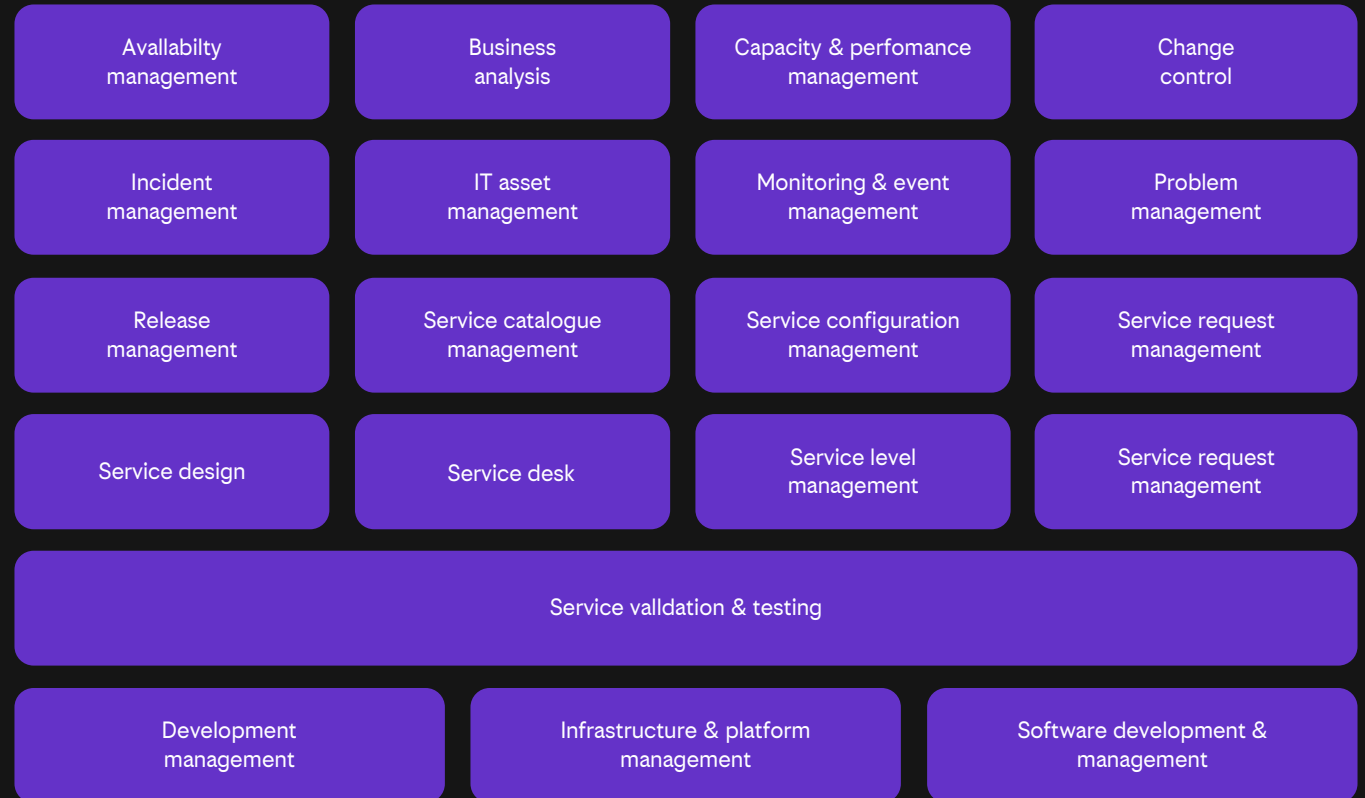
# Где ИБ в ИТ

## General management practices



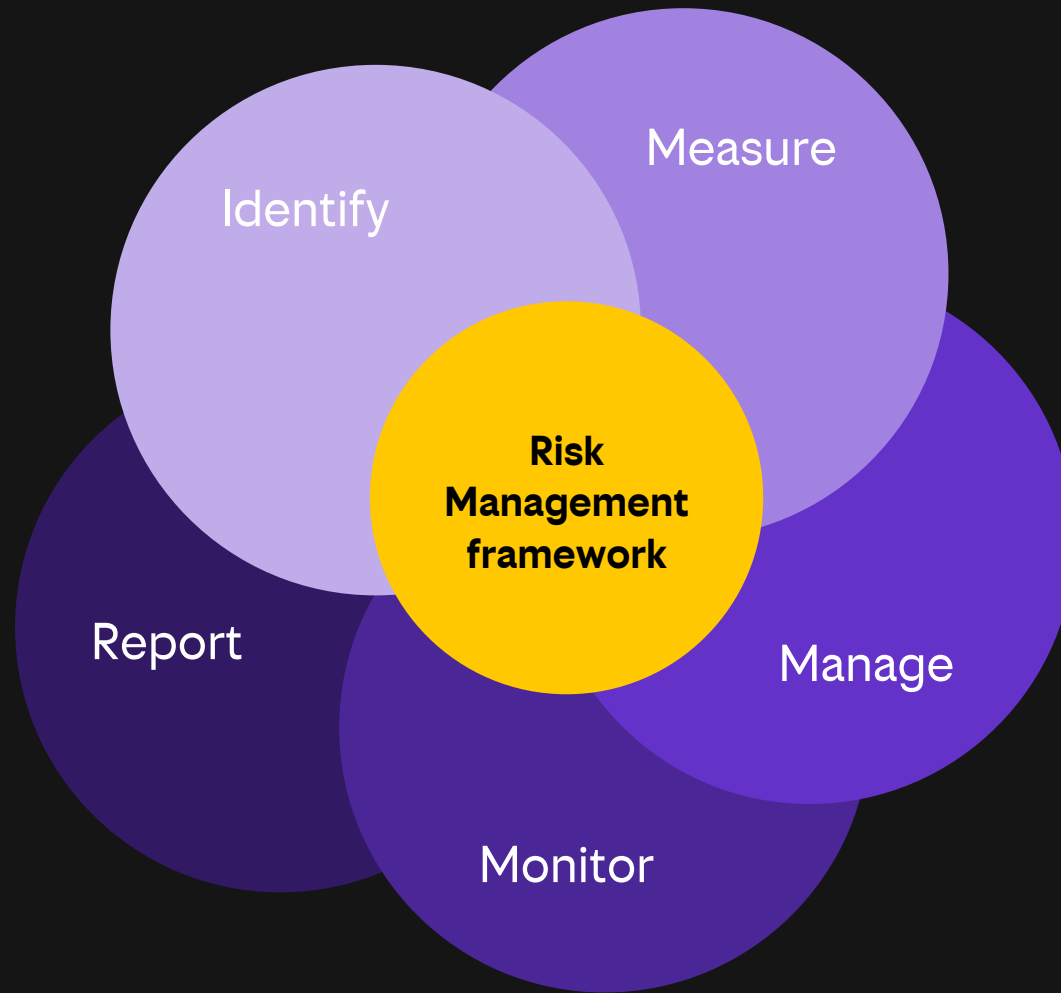
34 management practices

## Service management practices



ITIL 4 34 management practices

# Чем занимается ИБ

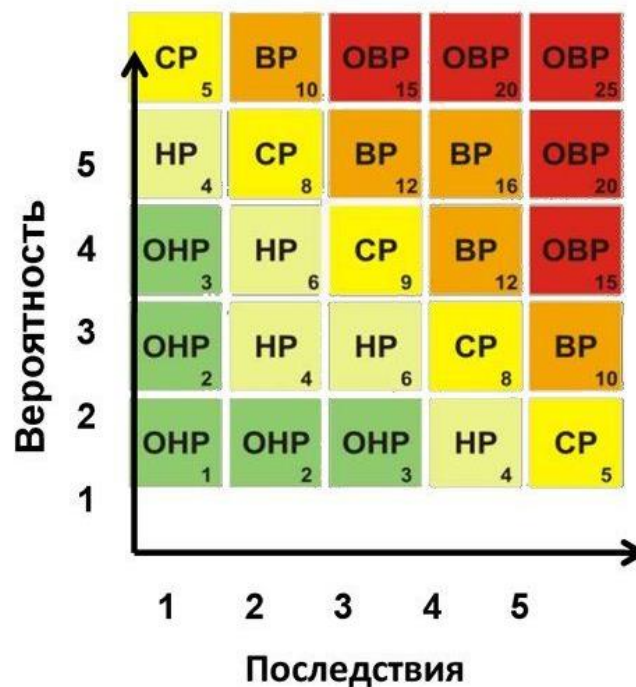




# Риски в ИБ

## Оценка рисков

Величина риска определяется как произведение вероятности события на его последствия



**ОНР**

очень низкий риск 1 – 3

**НР**

низкий риск 4 - 6

**СР**

средний риск 5 – 9

**ВР**

высокий риск 10 - 16

**ОВР**

очень высокий риск 15 - 25

# Митигация рисков

**Методы реагирования на риск могут включать в себя:**

- ✓ Избегание риска
- ✓ Передача риска
- ✓ Управление риском

- ✓ Разделение риска
- ✓ Принятие риска

# Проблемы ИБ

**Человеческий  
фактор**

**Нет  
процессов**

# Как решается сейчас?



# Как повысить уровень ИБ в компании?



# Оценка



# План

№	Мероприятие	Q1-3 2021	Q4-2021	Q1-2022	Q2-2022	Q3-2022	Q4-2022	Q1-2023	Q2-2023	Q3-2023	Q4-2023
<b>1.</b>	<b>Целеполагание и контроль</b>										
1.1.	Сделать "нулевой замер". Провести тестирование на проникновение										
1.2.	Провести анализ рисков и приоритизировать направления развития ИБ и ГИСы, подлежащие защите		Кач. оценка, неприемлемые риски	Количественный анализ							
1.3.	Разработать концепцию развития ИБ до 2024 год		Согласование подхода	Написание и утверждение концепции							
1.4.	Запустить периодическое тестирование защищенности	пен-тест					пен-тест				пен-тест
<b>2.</b>	<b>Управление программой развития ИБ</b>										
2.1.	Создать управляющий комитет программы проектов		Приказ о создании и 1ая встреча	Ежемесячные встречи УК	Ежеквартальные встречи УК				Подведение итогов реализации программы		
2.2.	Запустить офиса управления программой проектов			Офис запущен							
2.3.	Разработать дорожную карту развития ИБ до 2024 года			Утвердить ДК и план на 2022 год			Утвердить план на 2023 год				Утвердить план на 2024 год
2.4.	Бюджетное планирование		Бюджет программы развития ИБ		Бюджетирование 2023 года					Бюджетирование 2024 года	
2.5.	Обеспечить финансирование и контрактование программы		Конкурсы и договора на работы 2022 года			Конкурсы и договора на работы 2023 года					Конкурсы и договора на работы 2024 года
<b>3.</b>	<b>Разработка нормативной базы и оргструктуры обеспечения ИБ</b>										
3.1.	Разработать меморандум, определяющий зоны ответственности при обеспечении ИБ		Согласование и утверждение меморандума на уровне Губернатора								
3.2.	Разработать политику обеспечения ИБ и нижестоящий пакет ОРД			Политика согласована и утверждена							
3.3.	Разработать положение о SOC				Положение утверждено						
3.4.	Разработать типовой пакет ОРД, регламентирующий обеспечение ИБ в ДЗО				ОРД разработаны и утверждены						
3.5.	Определить целевую организационную модель обеспечения ИБ и обеспечить наполнение ресурсами		Целевая модель определена	Согласованы и утверждены положения о подразделениях		Обеспечено кадровое наполнение					

# Безопасность, которую не отнять







# Александр Митусов

Руководитель по сопровождению  
продуктов кибербезопасности,  
beeline cloud

02

# beeline cloud в цифрах

**100+**

Облачных сервисов  
и решений

**3000+**

Клиентов из разных  
отраслей бизнеса

**99,95%**

Облачный SLA

**6**

ЦОДов в РФ  
уровня Tier III

**5**

Независимых интернет-  
провайдеров

## Secure by design

**УЗ-1 152-ФЗ**

Публичное  
облако

**ГИС К1, ИСПДн УЗ-1**

Изолированный  
сегмент

**PCI DSS 4.0**

Соответствие  
стандарту

**ГОСТ Р 57580.1-2017**

Первый уровень  
защиты информации

**ФСБ, ФСТЭК**

Лицензии

## Партнеры

kaspersky



MULTIFACTOR

positive technologies

radware

UserGate

COMMUNIGATE  
SYSTEMS

ARENADATA



ФЛАНТ

# Задачи и возможности

## Задачи

1. Повышение уровня осведомленности сотрудников
2. Уменьшение количества инцидентов информационной безопасности
3. Снижение количества повторных инцидентов

## Возможности

1. Отправка фишинговых писем сотрудникам и сбор данных из внешних систем
2. Определение компетенций сотрудников, формирование индивидуального учебного плана
3. Сбор статистики о ходе обучения, тестирование сотрудников по пройденному материалу
4. Автоматизация процесса обучения сотрудников на основе правил и сценариев

## Соответствие требованиям регуляторов

1. ГОСТ Р 57580.1-2017
2. Положение Банка России от 20 апреля 2021 г. № 757-П
3. PCI-DSS
4. ФЗ № 152
5. и другие



# Что из себя представляет платформа

## Модуль «Обучение»

- Создание учебных программ
- Запись сотрудников на обучение
- Рассылки напоминаний о предстоящем обучении
- Создание отчетов по итогам обучения
- Назначение учебных программ сотрудникам, учебной группе, отделу или подразделению

## Модуль «Атаки»

- Отвечает за управление и настройку рассылки учебных фишинговых писем сотрудникам
- Платформа поддерживает несколько типов учебных атак

## Модуль «Сотрудники»

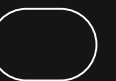
- Позволяет создавать древовидную структуру подразделений компании в соответствии со штатным расписанием

## Модуль «Правила»

- Позволяет создавать сценарии, которые помогут автоматизировать процесс осведомленности в организации

## Модуль «Отчеты»

- Позволяет получать аналитическую информацию в виде отчетов





beeline **cloud**

# Вопросы и ответы