

Введение в информационную безопасность



Перевозников С.Н.

Базовые понятия информационной безопасности

Информация — это сведения (сообщения, данные),
независимо от формы их представления.

Это закреплено в законодательстве Российской Федерации — в ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
Систему официальных взглядов на обеспечение национальной безопасности РФ в информационной сфере, то есть обеспечение ИБ, представляет Доктрина информационной безопасности Российской Федерации, которая утверждена Указом Президента РФ от 05.12.2016 г. № 646.

Информационная безопасность — это состояние защищённости информационных внешних ресурсов организации от внутренних и внешних угроз.

информационные ресурсы — это данные или сведения и активы компании, на которых обрабатывается информация.

Отдельно в нормативном поле можно встретить термин:
«защита информации». Это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.



Триада

«конфиденциальность, доступность, целостность»

Основная концепция информационной безопасности построена на обеспечении трёх основных свойств:

Конфиденциальность информации

– это состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право.



Целостность информации

– это состояние информации, при котором её изменение осуществляется только субъектами, имеющими на него право.

Доступность информации

– это состояние информации, при котором субъекты, имеющие право доступа (то есть право на чтение, изменение, копирование, уничтожение информации, а также право на изменение, использование, уничтожение ресурсов), могут реализовать его беспрепятственно.

Классификация угроз информационной безопасности

Угроза безопасности информации — совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Угроза ИБ может вызывать негативные последствия (ущерб/вред) для организации. Она характеризуется наличием объекта, источника и проявления угрозы. Форма проявления угрозы ИБ — наступление одного или нескольких взаимосвязанных событий, которые приводят к нарушению свойств информационной безопасности (КЦД). Предпосылкой к этому может быть недостаток или слабое место в информационном ресурсе. Его принято называть *уязвимостью*.



Типы процессов: семантические

Процесс ИБ — это верхнеуровневая единица, в её обеспечение входят несколько базовых типов процессов и подпроцессов. Для выстраивания хорошего контура защиты информации необходимо задействовать организационные, технические и коммуникационные навыки.

Процессы защиты информации — это методы сохранности информации, к которым вы будете прибегать. К ним относятся организационные, технические и коммуникационные типы процессов.

Организационные методы

— включают в себя комплекс законодательных, правовых и локальных актов (норм), устанавливающих правовой статус субъектов информационных отношений, методов, форм и способов защиты.

Также здесь учитывается координация мероприятий и технических мер по защите информации.

Технические методы:

— реализуются при помощи средств физического, программно-аппаратного уровня.

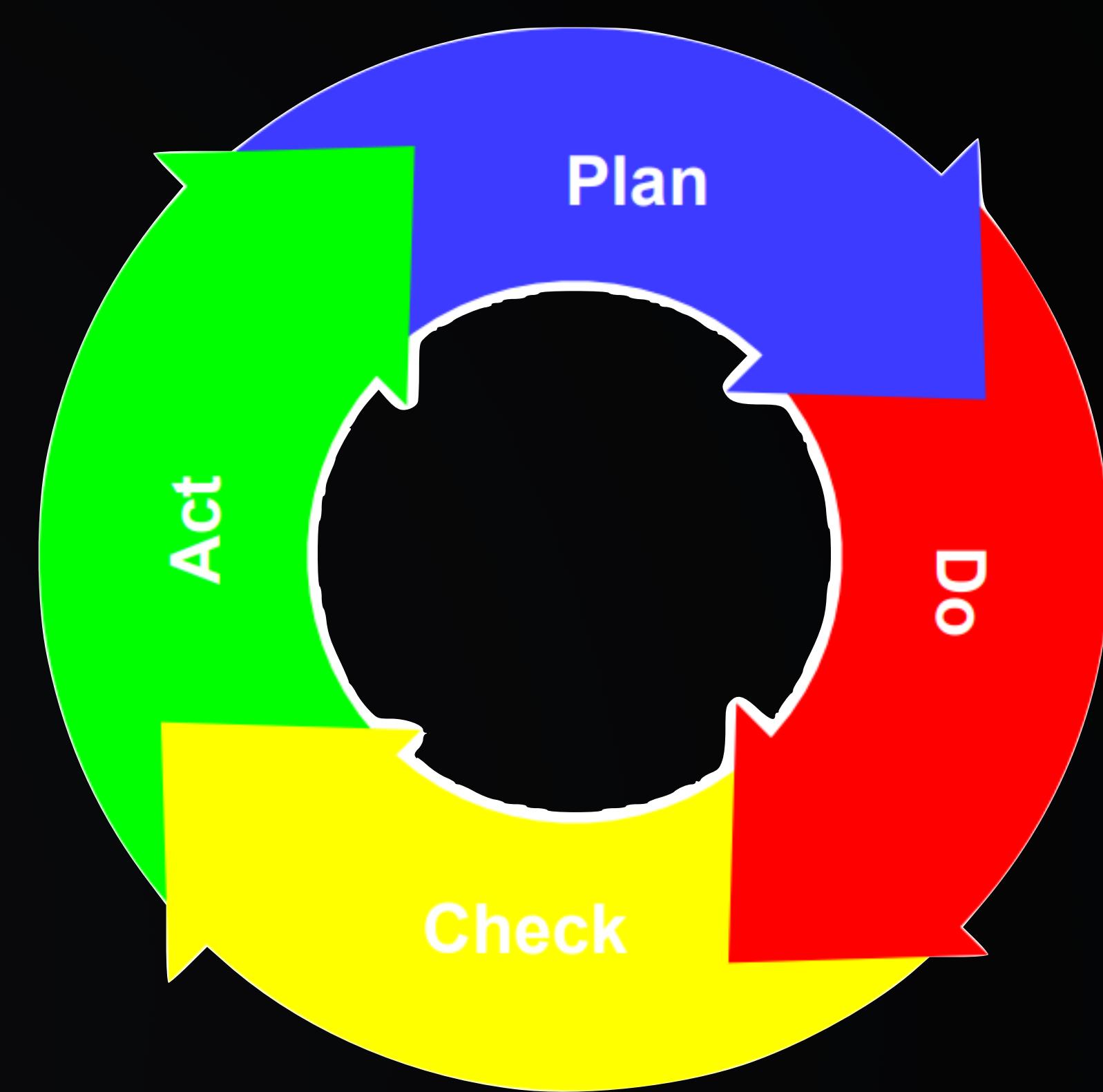
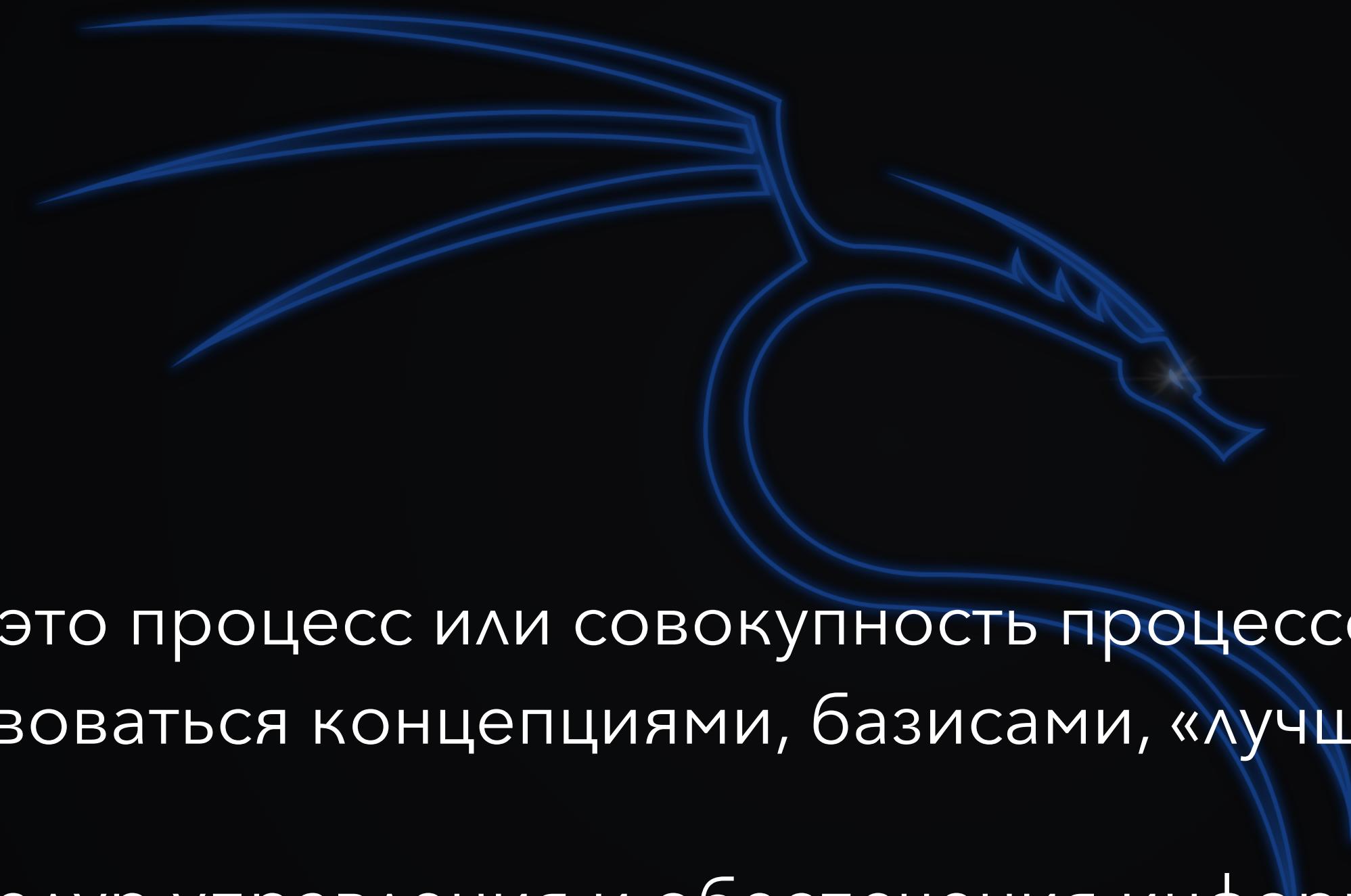
Коммуникационные методы:

— это процессы и способы, в которых вы не добьётесь желаемого результата без коммуникации со сторонними лицами как внутри компании, так и снаружи.

Тип	Перечень подпроцессов
1 Организационные	Координация, планирование и организация информационной безопасности Соблюдение требования законодательства Анализ угроз безопасности информации Аудит и оценка соответствия по требованиям информационной безопасности Информирование и обучение пользователей по вопросам информационной безопасности Управление инцидентами
2 Технические	Управление активами Разработка, внедрение, техническое обслуживание и модернизация информационных систем Контроль (анализ) защищённости информации Управление конфигурацией Управление доступом Регистрация и мониторинг событий безопасности Защита носителей информации Антивирусная защита Обнаружение вторжений Обеспечение целостности информационной системы и информации Обеспечение доступности и непрерывного функционирования Криптографическая защита информации
3 Коммуникационные	Безопасность, связанная с персоналом Анализ угроз безопасности информации Информирование и обучение пользователей по вопросам информационной безопасности Управление инцидентами Управление доступом Обеспечение целостности информационной системы и информации Обеспечение доступности и непрерывного функционирования

Цикл Шухарта-Деминга

Модель PDCA



Обеспечение ИБ – это процесс или совокупность процессов. Чтобы выстроить их, принято руководствоваться концепциями, базисами, «лучшими практиками».

Для описания процедур управления и обеспечения информационной безопасности принято использовать классическую модель непрерывного улучшения процессов – модель PDCA (Планируй – Plan, Выполняй – Do, Проверяй – Check, Действуй – Act). Она получила название от цикла Шухарта-Деминга.

Plan

На стадии «*Планирования*» нужно понять бизнес-контекст организации, чтобы синхронизировать цели обеспечения ИБ со стратегическими целями организации.

Понимание бизнес-процессов компании позволяет корректно проектировать внутреннее устройство процесса ИБ.

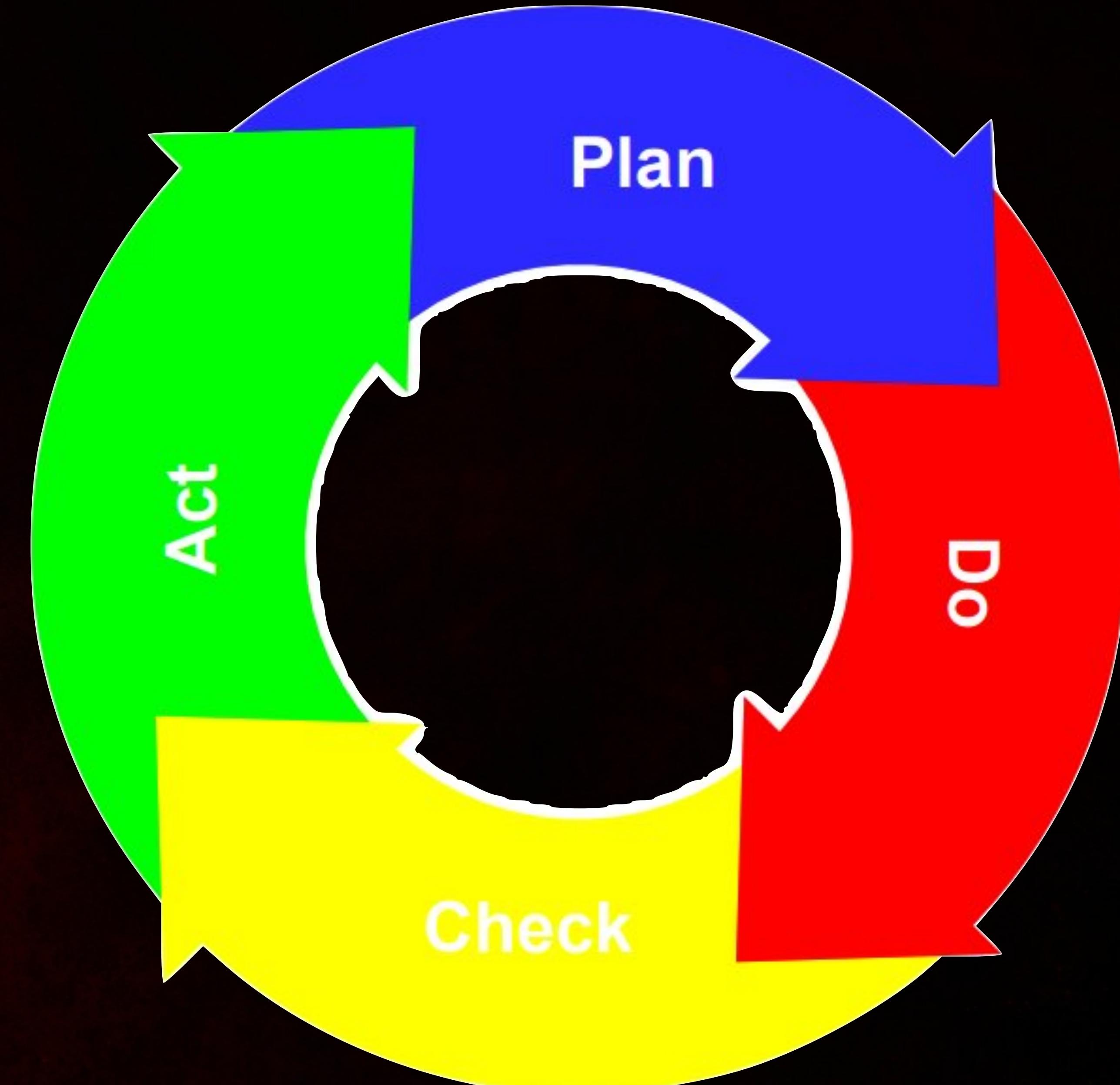
В идеале верхнеуровневые концепции должны быть зафиксированы и отражены в политике информационной безопасности организации.

Хорошо спроектированная система организации ИБ должна помогать ответить на вопросы:

- Какие роли и функции выделяются в процессе?
- Кто и за что отвечает в процессе?
- Какие действия запускаются разными событиями?
- Что, в какой момент и в каких случаях выполняется?
- Какие результаты даёт каждая активность?
- Какие результаты и где хранятся?
- Какие информационные ресурсы и активы защищаются

KALI LINUX™

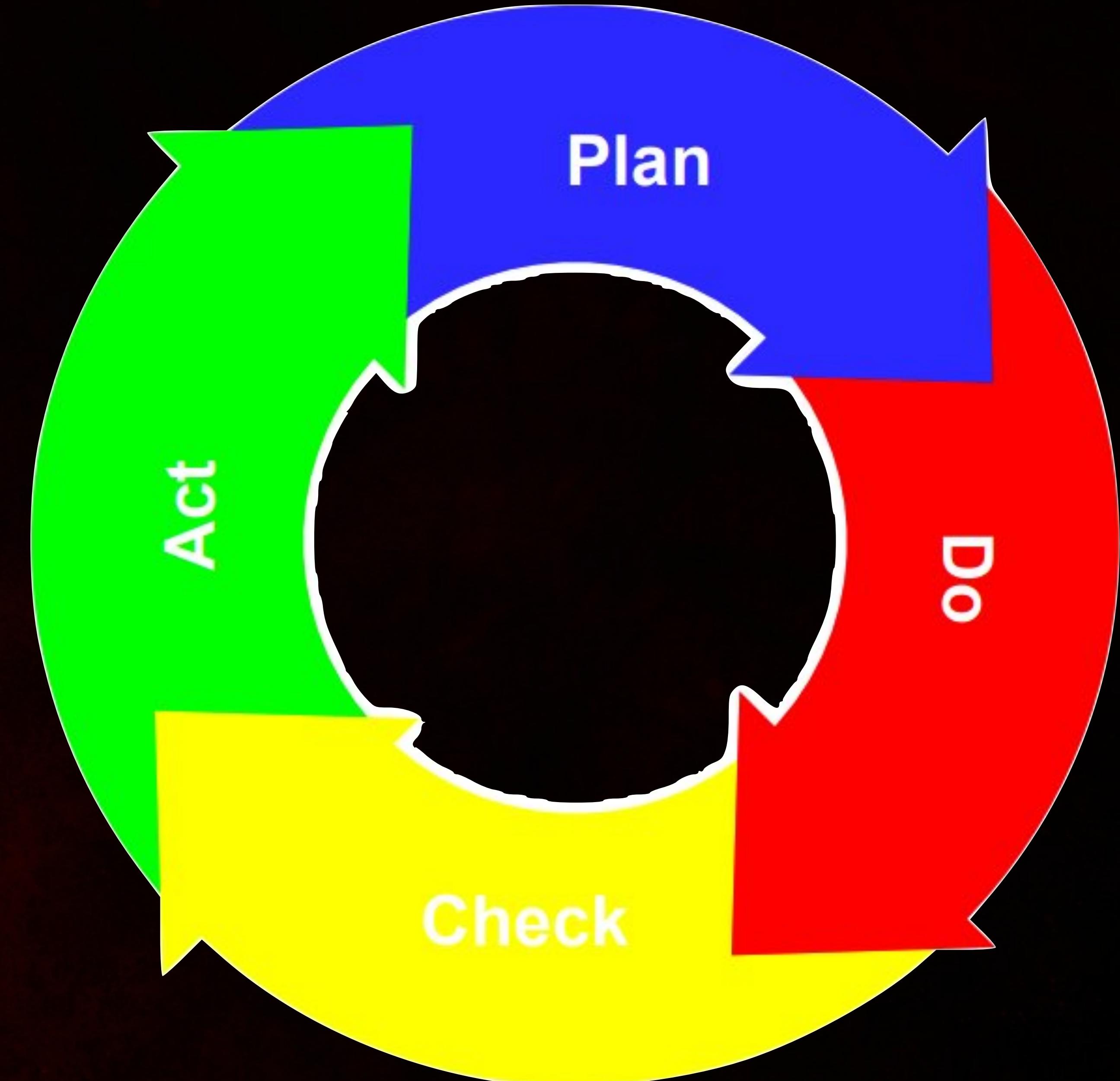
“the quieter you become, the more you are able to hear”



Do

Назначение стадии «**Выполнение**» – реализовать процесс в соответствии с концепцией, разработанной на стадии «**Планирование**», и приступить к его эксплуатации.

На стадии внедрения процесса создаются или модифицируются существующие роли для выполнения процесса. Именно здесь проектируются или реструктуризируются существующие функциональные подразделения для создания сил по обеспечению ИБ, а также разрабатываются, внедряются и настраиваются вспомогательных технические или организационные средства для управления ИБ и защиты информации.



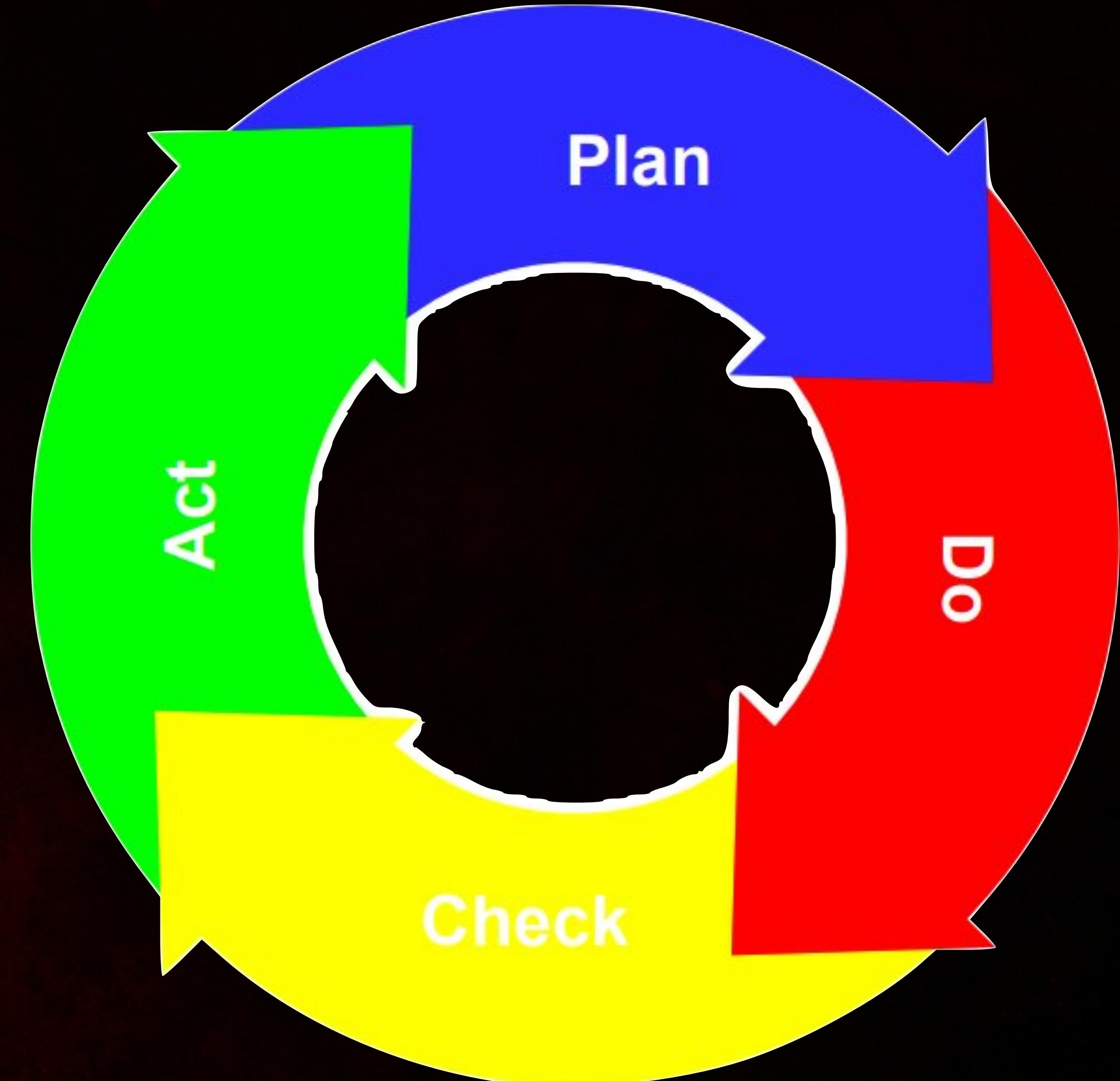
KALI LINUX™

"the quieter you become, the more you are able to hear"

Check

Стадия «**Проверки**» цикла необходима для измерения показателей эффективности внедрённого процесса и сравнения их с ожидаемой эффективностью (целевыми значениями).

Ожидания от процесса должны вытекать из результатов стадии «**Планирование**». Если они не достигнуты, то необходимо прибегнуть к корректирующим мероприятиям.



KALI LINUX™

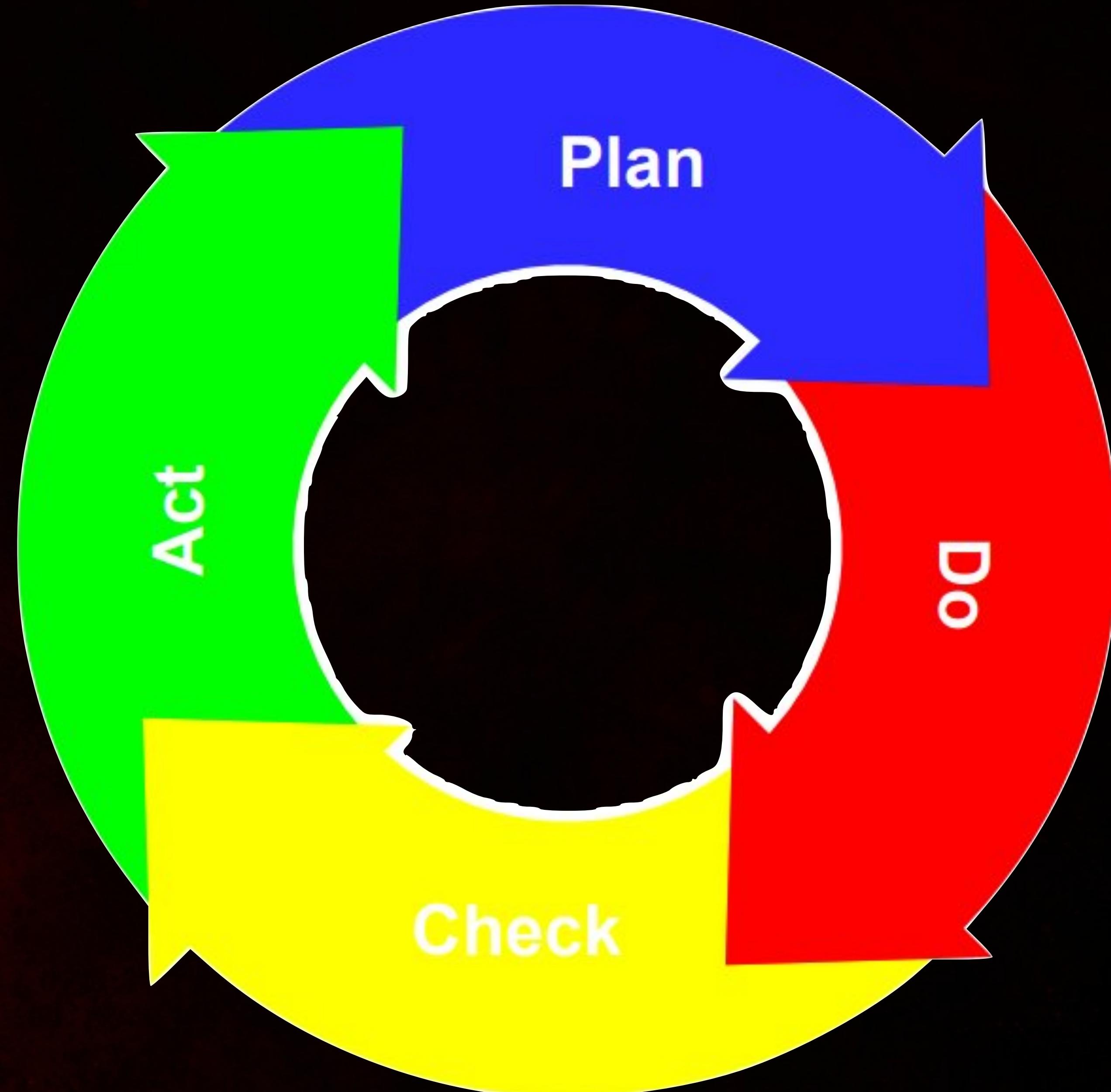
"the quieter you become, the more you are able to hear"

Act

Этап «**Действуй**» можно назвать стадией корректировок. Его назначение – проанализировать и отреагировать в соответствии с собранными на стадии «**Проверка**» данными по эффективности процесса. Эта стадия обеспечивает качественное функционирование процесса, несмотря на изменения окружающей среды, и в ходе таких измерений гарантирует, что процесс можно непрерывно совершенствовать, добиваясь соответствия целевым показателям эффективности, которые тоже со временем меняются.

Выполнение цикла PDCA не единоразово, а процессам требуется **поддержка**. При изменениях или нововведениях цикл запускается заново.

В видео разберём, как применить цикл PDCA к процессам обеспечения и управления ИБ.



KALI LINUX™

"the quieter you become, the more you are able to hear"

Памятка

ИБ – информационная безопасность

СИБ – Система информационной безопасности

СОИБ – Система обеспечения информационной безопасности

СУИБ – Система управления информационной безопасностью

СМИБ – Система менеджмента информационной безопасностью

СМИБ – это набор политик, целей и процессов, которые использует организация.

СОИБ

Система обеспечения информационной безопасности
совокупность организационно-
технической структуры и/или
исполнителей, задействованных в
обеспечении ИБ и используемых ими
механизмов обеспечения безопасности
(средств защиты), взаимодействующая с
органами управления организации.

СОИБ включает в себя общие методы защиты информации:

- управление доступом;
- антивирусы;
- средства шифрования.

Их относят к системе информационной безопасности (СИБ).

Есть и организационные мероприятия:

- распределение ролей;
- планирование;
- документирование;
- управление инцидентами ИБ.

Их относят к (СУИБ).

СОИБ = СИБ + СУИБ



Система информационной безопасности

Система управления информационной
безопасности

СУИБ или СМИБ

Система управления/менеджмента информационной безопасностью

В системе управления реализуются функции управления, то есть она объединяет управляющую систему и систему связи.

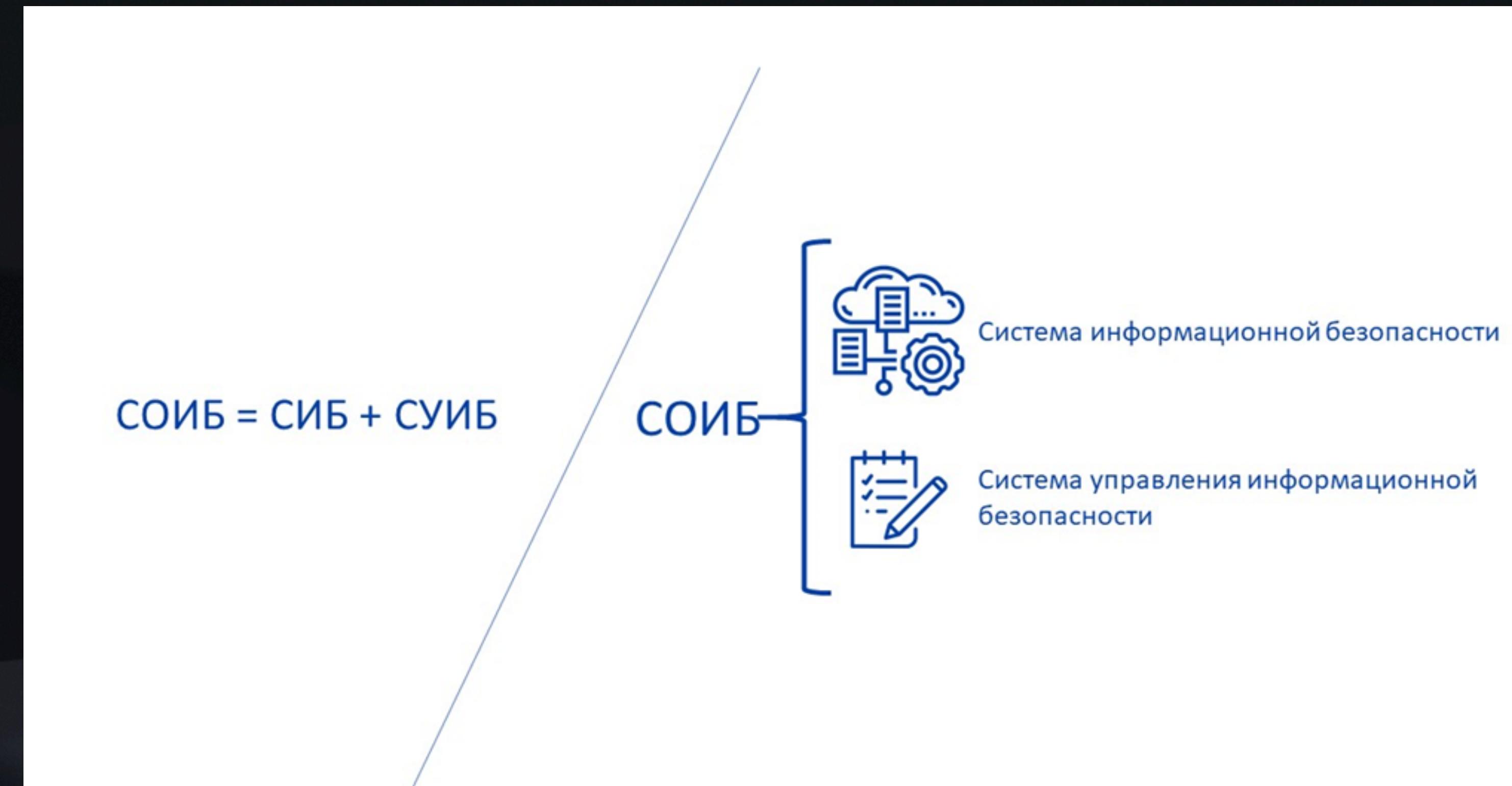
Система менеджмента это набор политик, целей и процессов, которые использует организация.

Цель построения – выбор соответствующих мер управления ИБ, предназначенных для защиты информационных активов и гарантирующих доверие заинтересованных сторон.

К элементам СУИБ можно отнести организационную структуру, роли и обязанности, процессы планирования и функционирования. Сфера действия СУИБ может охватывать организацию в целом, конкретные выявленные функции или сегменты организации, а также одну функцию (или несколько функций) в рамках группы организаций

При построении СУИБ нужно учитывать основные вехи (цикл PDCA):

- понимание требований по обеспечению ИБ организации и необходимости установления политики и целей ИБ;
- внедрение и использование мер для управления угрозами (рисками) ИБ наряду с общими бизнес-рискаами организации;
- мониторинг и проверка производительности и эффективности СУИБ;
- непрерывное улучшение СУИБ, основанное на результатах объективных измерений.



Стандарты

Выстраивание процессов ИБ обычно базируется на стандартах. Для полного понимания вы прочитаете несколько основных популярных стандартов российской и международной практики.

Дословное знание стандартов не обязательно, достаточно понимать общую концепцию подхода. Тем более некоторые частности стандартов применимы не ко всем сферам деятельности компаний.

При использовании «лучшей практики» необходима адаптация к особенностям деятельности организации, информационной инфраструктуры и так далее. В следующих материалах поговорим о том, какие критерии стоит при этом учитывать.

|ГОСТ Р ИСО/МЭК 27001-2021 | ГОСТ Р ИСО/МЭК 27002-2021|ГОСТ Р ИСО/МЭК 27002-2021|

|Стандарт Банка России СТО БР ИББС|Payment Card Industry Data Security Standard (PCI DSS)|

|ITIL (Information Technology Infrastructure Library)|

Процессы управления ИБ

- **Документальное обеспечение:**

Формализация процессов ИБ,
моделирование процессов

- **Учёт и классификация объектов**

защиты:

На основе общей CMDB с учётом
дополнительных параметров

- **Управление рисками:**

Формирование модели угроз,
обработка и принятие рисков

- **Контроль соответствие
требованиям ИБ:**

Проведение проверок, контроль
устранения несоответствий

- **Управление инцидентами ИБ:**

реализация процесса управления
инцидентами ИБ

- **Повышение осведомлённости:**

Доведения от состояния signed к
состоянию approve

Процессы обеспечения ИБ

- **Мониторинг событий и инцидентов ИБ:**

Управление событиями ИБ,
принципы эскалации инцидентов ИБ

- **Управление уязвимостями:**

Управление уязвимостями в ИТ -инфраструктуре

- **Управление доступом:**

Контроль и управление доступом к информации и ИТ - активам

- **Безопасное хранение данных:**

Разграничение доступа к классифицируемым данным, правовые механизмы защиты

- **Обеспечение безопасной разработки ПО:**

Контроль разработки ПО, отсутствие уязвимости и закладок

- **Аутентификация, антивирусная защита, криптография:**

Инструментальное повышение защищённости