Управление информационной безопасностью.

Политика ИБ

Толстой Александр Иванович
НИЯУ МИФИ,
факультет «Кибернетика и информационная безопасность»,
кафедра «Информационная безопасность банковских систем»

Москва, 2016

Содержание

1.Почему политика ИБ?
2.Определение термина «политика ИБ»
3. Содержание политик ИБ
4. Жизненный цикл ПолИБ

1.Почему политика ИБ?

ГОСТ Р ИСО/МЭК 27002-2012

ИТ. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности

ISO/IEC 27002:2005

Information technology — Security techniques — Code of practice for information security management.

Политика (policy): Общее намерение и направление, официально выраженное руководством

Мероприятия по управлению ИБ, рассматриваемые как общепринятая практика в области информационной безопасности, включают:

…….

- наличие документа, описывающего политику информационной безопасности;

1.Почему политика ИБ?

ГОСТ Р ИСО/МЭК 27002-2012

Политика ИБ

Цель: Обеспечить управление и поддержку высшим руководством информационной безопасности в соответствии с требованиями бизнеса и соответствующими законами и нормами.

Высшее руководство должно установить четкое направление политики в соответствии с целями бизнеса и демонстрировать поддержку и обязательства в отношении обеспечения информационной безопасности посредством разработки и поддержки политики информационной безопасности в

1.Почему политика ИБ?

ГОСТ Р ИСО/МЭК 27002-2012

Политика ИБ

- **При необходимости следует предусмотреть наличие контактного лица, занимающегося вопросами ИБ внутри организации, к которому могут обращаться заинтересованные сотрудники.**
- **Следует налаживать контакты с внешними специалистами по безопасности или группами специалистов, включая соответствующие органы, чтобы находиться в курсе отраслевых тенденций, осуществлять мониторинг стандартов и методов оценки, и обеспечивать адекватные точки контакта при обработке инцидентов информационной безопасности.**
- **Следует поощрять многопрофильный подход к обеспечению информационной безопасности.**

1.Почему политика ИБ?

ГОСТ Р ИСО/МЭК 27002-2012

Мера и средство контроля и управления ИБ:
Документирование политики ИБ

Политика информационной безопасности должна быть утверждена руководством, издана и доведена до сведения всех сотрудников организации и соответствующих сторонних организаций.

1.Почему политика ИБ?

ГОСТ Р ИСО/МЭК 27002-2012

Документирование политики ИБ: рекомендация по реализации:

Политика ИБ должна устанавливать ответственность руководства, а также излагать подход организации к менеджменту ИБ.

Документ, в котором излагается политика, должен содержать положения относительно:

a) определения ИБ, ее общих целей и сферы действия, а также упоминания значения безопасности как инструмента, обеспечивающего возможность совместного использования информации;

b) изложения намерений руководства, поддерживающих цели и принципы ИБ в соответствии со стратегией и целями бизнеса;

1.Почему политика ИБ?

ГОСТ Р ИСО/МЭК 27002-2012

Документ, в котором излагается политика, должен содержать положения относительно:

d) краткого разъяснения наиболее существенных для организации политик безопасности, принципов, стандартов и требований соответствия, например:

1) соответствие законодательным требованиям и договорным обязательствам;

2) требования по обеспечению осведомленности, обучения и тренинга в отношении безопасности;

3) менеджмент непрерывности бизнеса;

4) ответственность за нарушения политики информационной безопасности;

1.Почему политика ИБ?

ГОСТ Р ИСО/МЭК 27002-2012

Документ, в котором излагается политика, должен содержать положения относительно:

e) определения общих и конкретных обязанностей сотрудников в рамках менеджмента информационной безопасности, включая информирование об инцидентах безопасности;

f) ссылок на документы, дополняющие политику информационной безопасности, например более детальные политики и процедуры безопасности для определенных информационных систем, а также правила безопасности, которым должны следовать пользователи.

1.Концептуальные подходы к управлению ИБ

ГОСТ Р ИСО/МЭК 27002-2012

Документ, в котором излагается политика, должен содержать положения относительно:

e) определения общих и конкретных обязанностей сотрудников в рамках менеджмента информационной безопасности, включая информирование об инцидентах безопасности;

f) ссылок на документы, дополняющие политику информационной безопасности, например более детальные политики и процедуры безопасности для определенных информационных систем, а также правила безопасности, которым должны следовать пользователи.

Политика ИБ должна пересматриваться либо через запланированные интервалы времени, либо, если

1.Почему политика ИБ?

Наиболее правильный и эффективный способ добиться минимизации рисков нарушения ИБ организации еще до того, как появится первая проблема с безопасностью, – разработать Политику ИБ (ПолИБ) и в соответствии с ней реализовать, эксплуатировать и совершенствовать систему обеспечения ИБ (СОИБ) организации

Политика ИБ: Причины выработки политики ИБ:

- ***ПолИБ составляет общую основу для защиты всех влияющих на ОИБ активов организации, в рамках которой определяются правила разграничения доступа к этим активам.***
- ***ПолИБ определяет, какое поведение по отношению к активам разрешено, т. е. является санкционированным, а какое запрещено, является несанкционированным и свидетельствует о незаконном их использовании.***
- ***ПолИБ определяет «правила игры» для всех сотрудников организации и третьих лиц, что позволяет достичь согласия по вопросам ОИБ как внутри самой организации (включая ее руководство), так и вовне.***
- ***ПолИБ часто помогает сделать правильный выбор самой платформы для работы с активами, учитывая, какие***

1.Почему политика ИБ?

Политика ИБ: Причины выработки политики ИБ:

- *Требование руководства, обнаружившего недостаток внимания к проблемам ИБ, которые привели к снижению эффективности бизнеса.*
- *Требования законодательства и отраслевых стандартов.*
- *Требования клиентов и партнеров о подтверждении необходимого уровня ОИБ для гарантии того, что их конфиденциальная информация защищена надлежащим образом.*
- *Необходимость сертификации по стандартам (например, ISO/IEC 9001, 27002, 15408 и т. п.).*
- *Устранение замечаний аудиторов и выполнение их рекомендаций.*
- *Обеспечение конкурентоспособности за счет оптимизации бизнес-процессов и увеличения результативности.*
- *Демонстрация заинтересованности руководства в ОИБ, что значительно увеличивает приоритет безопасности в глазах сотрудников организации.*
- *Создание корпоративной культуры ИБ и широкое вовлечение сотрудников в процесс ОИБ.*
- *Уменьшение стоимости страхования.*

1.Почему политика ИБ?

Первостепенной целью разработки ПолИБ организации является обеспечение решения вопросов обеспечения ИБ в пределах организации и вовлечение ее высшего руководства в данный процесс

2. Определение термина «политика ИБ»

Политика ИБ:

- Политика ….. организации
- Политика ИБ
- Политика обеспечения ИБ
- Политика обеспечения ИБ организации
- Политика системы управления ИБ
- Частная политика ИБ

2. Определение термина «политика ИБ»

«Политика ИБ» -

- совокупность требований и правил по ИБ для объекта ИБ, выработанных в соответствии с требованиями руководящих и нормативных документов в целях противодействия заданному множеству угроз ИБ, с учетом ценности защищаемой информационной сферы;
- одно или несколько правил, процедур, практических приемов в области ИБ, которыми руководствуется организация в своей деятельности;
- документированные решения в области обеспечения ИБ;
- совокупность документированных правил, процедур, практических приемов или руководящих принципов в области ИБ, которыми руководствуется организация в своей деятельности;
- система документированных управленческих решений по обеспечению ИБ организации;
- документация, определяющая высокоуровневые цели, содержание и основные направления и устанавливающая правила, процедуры, практические приемы и руководящие принципы обеспечения ИБ активов организации, которыми она руководствуется в своей деятельности.
- локальный нормативный документ, определяющий требования

Роль политики ИБ в управлении ИБ:

Принципы обеспечения ИБ организации

Опыт

От чего защищаем?

Модель угроз ИБ

Идентификация активов и биз-нес-процессов

Модель нарушителя ИБ

Мониторинг

Как контролируем?

Оценка рисков ИБ

Политика ИБ организации

Аудит

Что защищаем?

Реализация политики ИБ организации

Как защищаем?

2. Определение термина «политика ИБ»

ПолИБ (в широком смысле - корпоративная ПолИБ):

- ***документация, определяющая высокоуровневые цели, содержание и основные направления, устанавливающая правила, процедуры, практические приемы и руководящие принципы обеспечения ИБ активов организации, которыми она руководствуется в своей деятельности;***
- ***система документированных управленческих решений по обеспечению ИБ организации.***

ПолИБ (в узком смысле – частная ПолИБ):

- ***локальный нормативный документ, определяющий требования безопасности, систему мер, либо порядок действий, а также ответственность сотрудников организации и механизмы контроля для определенной области обеспечения ИБ;***
- ***документация, детализирующая положения корпоративной ПолИБ применительно к одной или нескольким областям ИБ, видам и технологиям деятельности организации***
- ***ПолИБ по конкретным вопросам или проблемам (issue-specific);***
- ***ПолИБ по конкретным системам (system-specific), ориентированная на отдельную область ОИБ или технологию,***

2. Определение термина «политика ИБ»

ПолИБ (в узком смысле – частная ПолИБ):

- ***локальный нормативный документ, определяющий требования безопасности, систему мер, либо порядок действий, а также ответственность сотрудников организации и механизмы контроля для определенной области обеспечения ИБ;***
- ***документация, детализирующая положения ПолИБ применительно к одной или нескольким областям ИБ, видам и технологиям деятельности организации***
- ***ПолИБ по конкретным вопросам или проблемам (issue-specific);***
- ***ПолИБ по конкретным системам (system-specific), ориентированная на отдельную область ОИБ или технологию, используемую в организации или ее подразделении;***
- ***Примеры частных ПолИБ: «Политика управления паролями», «Политика управления доступом к ресурсам корпоративной сети», «Пол ИБ при взаимодействии с сетью Интернет», «ПолИБ при защите от воздействия вредоносного кода», «Политика использования средств криптографической защиты» и т.п.***

В частной ПолИБ формулируются требования на создание и

2. Определение термина «политика ИБ»

Наиболее часто разрабатываемыми в организациях частыми ПолИБ являются политики для следующих областей и технологий, имеющие аналогичные названия:

1) Физической защиты (включая вопросы организации пропускного режима, регистрации сотрудников и посетителей, использования средств сигнализации и видеонаблюдения и т. п.).
2) Организации режима секретности.
3) Обращения с информацией, составляющей государственную тайну.
4) Опубликования материалов в открытых источниках.
5) Доступа сторонних пользователей (организаций) в ИС организации.
6) Оценки рисков ИБ. 7) Управления паролями.
8. Контроля доступа и защиты от несанкционированного доступа.
9. Назначения и распределения ролей и обеспечение доверия к персоналу.
10. Использования Интернета. 11. Разработки и лицензирования ПО.

2. Определение термина «политика ИБ»

Наиболее часто разрабатываемыми в организациях частыми ПолИБ являются политики для следующих областей и технологий, имеющие аналогичные названия:

14. Использования отдельных универсальных ИТ в масштабе организации:

- **электронной почты;**
- **сетевых сервисов;**
- **программно-технических средств защиты;**
- **МЭ;**
- **технологии ВЧС;**
- **средств антивирусной защиты;**
- **средств криптографической защиты информации;**
- **электронной цифровой подписи (ЭЦП);**
- **Инфраструктуры открытых ключей;**
- **модемов и других коммуникационных средств;**
- **мобильных аппаратных средств и т. д.**

15. Проведения внешних и внутренних аудитов ИБ.

16. Резервирования информации и т. п.

3.1. Общие рекомендации к содержанию ПолИБ

В тексте ПолИБ обязательно в явном виде присутствуют ответы на следующие вопросы:

Что? - **Цель ПолИБ.**

Кто? - **На кого распространяется ПолИБ.**

Где? - **Область действия ПолИБ.**

Как? - **Факторы соблюдения и оценка соблюдения ПолИБ.**

Когда? - **Когда ПолИБ вступает в действие.**

Почему? - **Необходимость внедрения ПолИБ.**

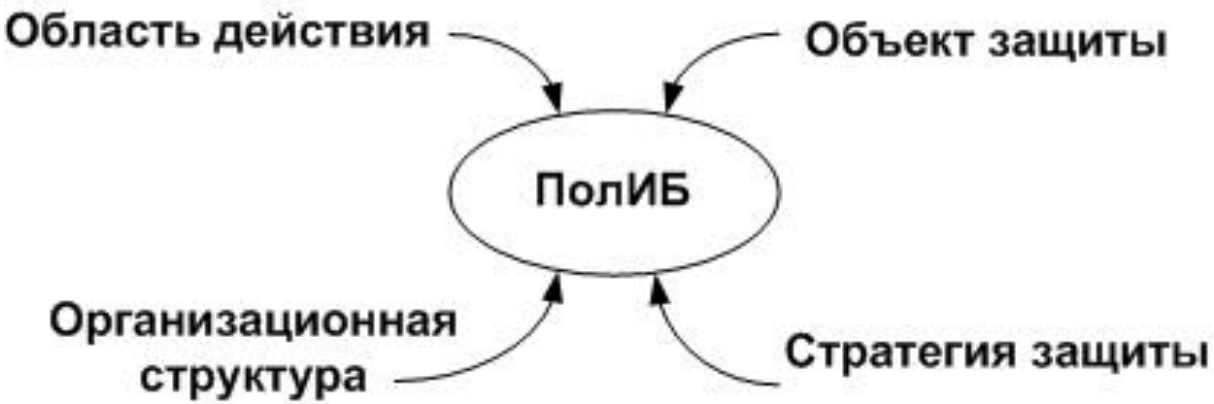
Что защищать? - **Описание активов, их уязвимостей.**

Отчего защищать? - **Перечень актуальных угроз.**

Как защищать? - **Стратегия защиты**

3.1. Общие рекомендации к содержанию ПолИБ

Обобщенная структура ПолИБ:



ПолИБ - должны по возможности носить не рекомендательный, а обязательный характер.

ПолИБ - ответственность за ее нарушение должна быть четко определена.

ПолИБ может быть описана в одном большом или нескольких небольших документах.

3.2. Содержание корпоративной ПолИБ

Информационные источники:

1.Guttman, B.; Roback, E. An Introduction to Computer Security: The NIST Handbook. NIST Special Publication 800–12. 1995.

2.Рекомендации в области стандартизации Банка России РС БР ИББС-2.0 «Обеспечение ИБ организаций банковской системы РФ. Методические рекомендации по документации в области обеспечения ИБ в соответствии с требованиями СТО БР ИББС-1.0».

3.2. Содержание корпоративной ПолИБ

Корпоративная ПолИБ как политика верхнего уровня должна включать в себя следующие разделы:

Введение ***(назначение корпоративной ПолИБ)***

Пример: определить высокоуровневые цели, содержание и основные направления, устанавливающая правила, процедуры, практические приемы и руководящие принципы обеспечения ИБ активов организации, которыми она руководствуется в своей деятельности;

Документ «Корпоративная ПолИБ» - система документированных управленческих решений по обеспечению ИБ организации.

3.2. Содержание корпоративной ПолИБ

Корпоративная ПолИБ как политика верхнего уровня должна включать в себя следующие разделы:

1.Цель обеспечения ИБ объекта

Объект: **организация в целом**

Типовые цели:

- **обеспечение устойчивого функционирования организации за счет предотвращения реализации угроз ИБ ее активам, защиты законных интересов владельца информации от противоправных посягательств;**
- **обеспечение определенного уровня ИБ активов организации, рассчитанного на основе риск ориентированного подхода;**
- **выработка планов восстановления после критических ситуаций и обеспечение непрерывности бизнеса (НБ) организации;**
- **достижение экономической целесообразности в выборе защитных мер.**

3.2. Содержание корпоративной ПолИБ

Корпоративная ПолИБ как политика верхнего уровня должна включать в себя следующие разделы:

2.Задачи обеспечения ИБ (которые необходимо решить для достижения поставленных целей)

Например, анализ и управление рисками ИБ, расследование инцидентов ИБ, разработка и внедрение планов обеспечения НБ, повышение квалификации и осведомленности сотрудников в области ИБ и т. д.

3.Область действия корпоративной Пол ИБ

Рекомендации: необходимо уточнить, где, как, когда, кем и к чему применяется данная ПолИБ.

3.2. Содержание корпоративной ПолИБ

Корпоративная ПолИБ как политика верхнего уровня должна включать в себя следующие разделы:

4.Описание активов объекта, подлежащих защите

Например,

- **классификация активов;**
- **виды активов: персонал, информация, ПО и АО, устройства, технологии;**
- **уязвимости активов;**
- **свойства информационных активов, которые должны быть защищены и т.д.**

5.Угрозы ИБ (на противодействие которым ориентирована корпоративная ПолИБ)

Рекомендации:

1.Необходимо определить актуальные угрозы ИБ с привязкой к определенным видам активов.

2. Необходимо определить роль нарушителей ИБ.

3.2. Содержание корпоративной ПолИБ

Корпоративная ПолИБ как политика верхнего уровня должна включать в себя следующие разделы:

6.Требования и правила корпоративной ПолИБ (содержательная часть ПолИБ, высокоуровневые требования)

Рекомендации (необходимо):

1.Кратко описать:

-позицию организации по обеспечению ИБ;

-процессы системы управления ИБ (СУИБ) (контроль доступа к активам организации, внесение изменений в ее ИС, взаимодействие с третьими лицами, повышение квалификации сотрудников в области ИБ, управление рисками ИБ, управление инцидентами ИБ, мониторинг и аудит ИБ и т.д.);

-конкретные меры, реализующие корпоративную ПолИБ в организации.

2.Дать обоснование выбора именно такого перечня мер и указать, какие угрозы ИБ для активов наиболее эффективно предотвращаются данными защитными мерами.

3.Обосновать создание организационной структуры

3.2. Содержание корпоративной ПолИБ

Корпоративная ПолИБ как политика верхнего уровня должна включать в себя следующие разделы:

7.Субъекты корпоративной ПолИБ (определение субъектов (ролей), на которых распространяется действие политики (как структурных подразделений организации, так и отдельных исполнителей)

Рекомендации:

1.Устанавливается, кто и за что отвечает.

2.Приводится информация о должностных лицах, ответственных за реализацию корпоративной ПолИБ, и их обязанностях.

3.Уместно описание (с краткой детализацией) нарушений, которые неприемлемы, и последствий такого поведения.

4.Могут быть явно перечислены наказания, применяемые к нарушителям корпоративной ПолИБ.

5.Устанавливаются организационные и технические меры реагирования на нарушение корпоративной ПолИБ (инциденты ИБ).

6. Обязанность за общее управление ИБ возлагается на руководство организации.

3.2. Содержание корпоративной ПолИБ

Корпоративная ПолИБ как политика верхнего уровня должна включать в себя следующие разделы:

8.Повышение осведомлённости в области ИБ

Рекомендации:

1.Должно вестись обучение всех сотрудников основным вопросам обеспечения ИБ.

9.Контроль реализации корпоративной ПолИБ

Рекомендации:

1.Определить меры контроля реализации корпоративной ПолИБ.

2.Поставить задачу конкретному подразделению организации следить за соблюдением ПолИБ.

3.Отдельно описать ответственность за контроль соблюдения ПолИБ.

3.2. Содержание корпоративной ПолИБ

Корпоративная ПолИБ как политика верхнего уровня должна включать в себя следующие разделы:

10.Пересмотр корпоративной ПолИБ

Рекомендации :

1.Необходимо предусмотреть порядок и период пересмотра корпоративной ПолИБ.

2.Внеплановый пересмотр ПолИБ проводится в случаях:

-существенных изменений в национальной законодательной базе в области ИБ;

-внесения существенных изменений в интранет организации;

-возникновения инцидентов ИБ.

3.При внесении изменений в положения ПолИБ организации учитываются:

-результаты анализа функционирования СУИБ со стороны руководства организации;

-результаты аудита ИБ (внешнего и внутреннего);

3.2. Содержание корпоративной ПолИБ

Корпоративная ПолИБ как политика верхнего уровня должна включать в себя следующие разделы:

11.Состав ссылочных документов (документы, ознакомление с которыми обязательно для адекватного понимания текста корпоративной ПолИБ)

12.Перечень используемых терминов, определений и сокращений

13. Перечень частных ПолИБ

Рекомендации:

1.Определить перечень частных ПолИБ, развивающих и детализирующих положения корпоративной Пол ИБ.

2.Указать подразделения организации, ответственные за соблюдение и/или реализацию

3.2. Содержание корпоративной ПолИБ

К разработке и согласованию корпоративной ПолИБ рекомендуется привлекать представителей следующих служб организации, связанных с ее информационной сферой:

- **руководство организации;**
- **профильные подразделения;**
- **служба информатизации;**
- **служба безопасности (ИБ)**

3.3. Содержание частной ПолИБ

Содержания частных ПолИБ по перечню разделов не отличаются от таковых для корпоративной ПолИБ.

Положения частной ПолИБ:

ни в коем случае не должны вступать в противоречия с положениями корпоративной ПолИБ

формируются на основании принципов, требований и задач, определенных в корпоративной ПолИБ.

Положения частной ПолИБ формируются на основе :

- **детализации, уточнения и дополнительной классификации активов и угроз ИБ;**
- **определения владельцев защищаемых активов;**
- **анализа, оценки рисков ИБ и возможных последствий реализаций угроз ИБ в границах области действия частной ПолИБ и т. п.**

Не рекомендуется повторение одинаковых правил в различных частных ПолИБ.

Включение в частную ПолИБ правила, содержащегося в другой существующей политике, целесообразно осуществлять посредством соответствующей ссылки

3.3. Содержание частной ПолИБ

Перечень разделов частной ПолИБ:

Введение ***(назначение частной ПолИБ)***

Пример: **определить требования, систему мер, либо порядок действий, а также ответственность сотрудников организации и механизмы контроля для определенной области обеспечения ИБ, видам и технологиям деятельности организации.**

Документ «Частная ПолИБ» **- детализирует положения корпоративной ПолИБ применительно к одной или нескольким**

3.3. Содержание частной ПолИБ

Перечень разделов частной ПолИБ:

1.Цель обеспечения ИБ объекта

Объект: одна или несколько областей ИБ, отдельные виды и технологии деятельности организации

Типовые цели:

- **обеспечение устойчивого функционирования отдельных видов и технологий деятельности организации за счет предотвращения реализации угроз ИБ ее активам, защиты законных интересов владельца информации от противоправных посягательств;**
- **обеспечение определенного уровня ИБ активов, относящихся к отдельным видам и технологиям деятельности организации, рассчитанного на основе риск ориентированного подхода;**
- **выработка планов восстановления отдельных видов и технологий деятельности организации после критических ситуаций;**
- **достижение экономической целесообразности в**

3.3. Содержание частной ПолИБ

Перечень разделов частной ПолИБ:

2.Задачи обеспечения ИБ ***(которые необходимо решить для достижения поставленных целей)***

Например, анализ и управление рисками ИБ, расследование инцидентов ИБ, разработка и внедрение планов обеспечения НБ, повышение квалификации и осведомленности сотрудников в области ИБ и т. д.

3.Область действия частной Пол ИБ

Рекомендации:

необходимо уточнить, где, как, когда, кем и к чему применяется данная ПолИБ

3.3. Содержание частной ПолИБ

Перечень разделов частной ПолИБ:

4.Описание активов объекта, подлежащих защите

Например,

-классификация активов;

-виды активов: персонал, информация, ПО и АО, устройства, технологии;

-уязвимости активов;

-свойства информационных активов, которые должны быть защищены и т.д.

5.Угрозы ИБ (на противодействие которым ориентирована частная ПолИБ)

Рекомендации (необходимо определить):

1.Актуальные угрозы ИБ с привязкой к определенным видам активов.

2. Роль нарушителей ИБ.

3.3. Содержание частной ПолИБ

Перечень разделов частной ПолИБ:

6.Требования и правила частной ПолИБ

(содержательная часть частной ПолИБ)

Рекомендации (необходимо):

1.Кратко описать:

-требования к процессам обеспечения ИБ объекта;

-конкретные меры, реализующие частную ПолИБ.

2.Дать обоснование выбора именно такого перечня мер и указать, какие угрозы ИБ для активов наиболее эффективно

3.3. Содержание частной ПолИБ

Перечень разделов частной ПолИБ:

7.Субъекты частной ПолИБ (определение субъектов (ролей), на которых распространяется действие политики (как структурных подразделений организации, так и отдельных исполнителей).

Рекомендации:

1.Устанавливается, кто и за что отвечает.

2.Приводится информация о должностных лицах, ответственных за реализацию частной ПолИБ, и их обязанностях.

3.Уместно описание (с краткой детализацией) нарушений, которые неприемлемы, и последствий такого поведения.

4.Могут быть явно перечислены наказания, применяемые к нарушителям корпоративной ПолИБ.

5.Устанавливаются организационные и технические меры реагирования на нарушение корпоративной ПолИБ (инциденты ИБ).

3.3. Содержание частной ПолИБ

Перечень разделов частной ПолИБ:

8.Повышение осведомлённости в области ИБ.

Рекомендации:

1.Должно вестись обучение всех сотрудников основным вопросам обеспечения ИБ.

9.Контроль реализации частной ПолИБ.

Рекомендации:

1.Определить меры контроля реализации частной ПолИБ.

2.Поставить задачу конкретным исполнителям (подразделению) организации следить за соблюдением частной ПолИБ.

3.Отдельно описать ответственность за контроль соблюдения частной ПолИБ.

3.3. Содержание частной ПолИБ

Перечень разделов частной ПолИБ:

10.Пересмотр частной ПолИБ

Рекомендации :

1.Необходимо предусмотреть порядок и период пересмотра частной ПолИБ.

2.При внесении изменений в положения частной ПолИБ учитываются:

-результаты анализа функционирования системы обеспечения ИБ;

-результатов мониторинга;

-рекомендации независимых экспертов по ИБ.

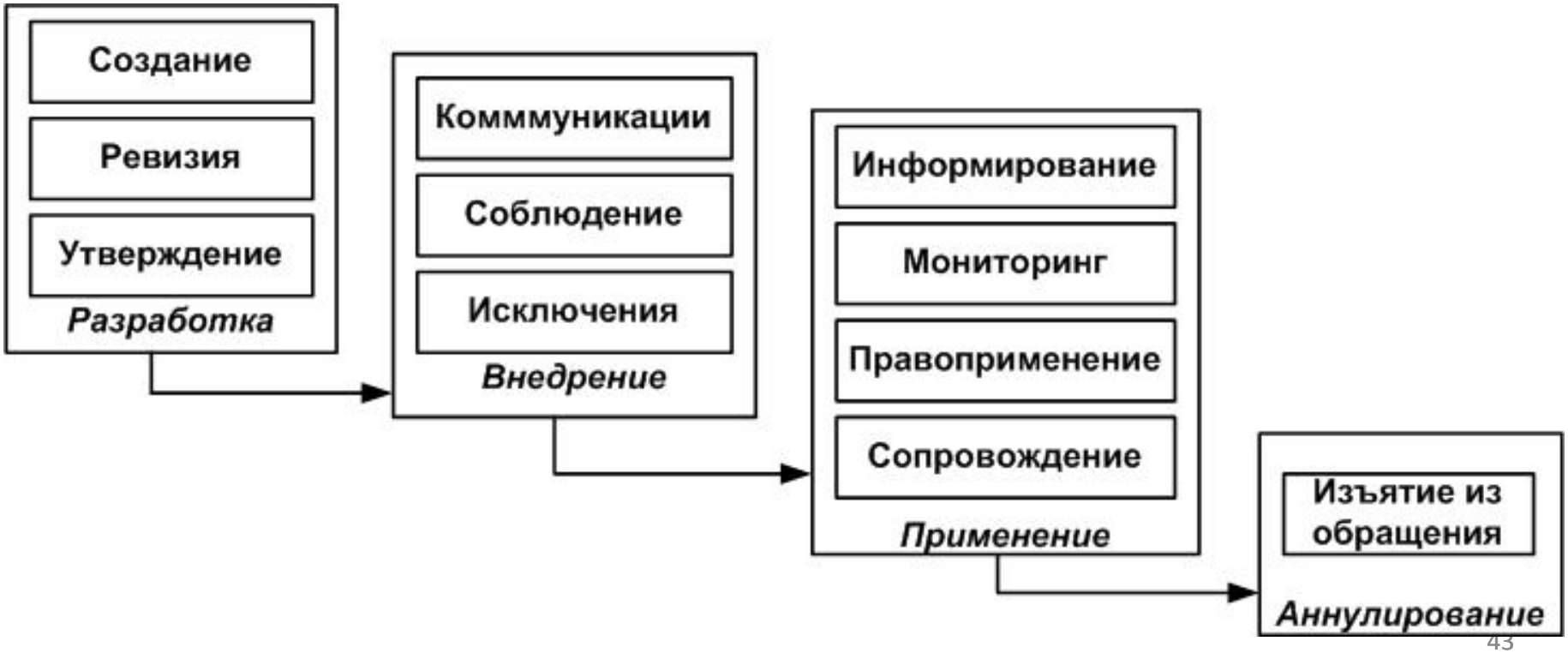
11.Состав ссылочных документов (документы, ознакомление с которыми обязательно для адекватного понимания текста частной ПолИБ)

12.Перечень используемых терминов, определений и сокращений

4. Жизненный цикл политики ИБ

8.1. Этапы жизненного цикла ПолИБ:

1. Разработка ПолИБ.
2. Внедрение ПолИБ.
3. Применение ПолИБ.
4. Анулирование ПолИБ.



4.1.Этапы жизненного цикла ПолИБ:

1.Разработка ПолИБ; 2.Внедрение ПолИБ;
3.Применение ПолИБ; 4.Анулирование ПолИБ.

Циклическая модель Деминга-Шухарта

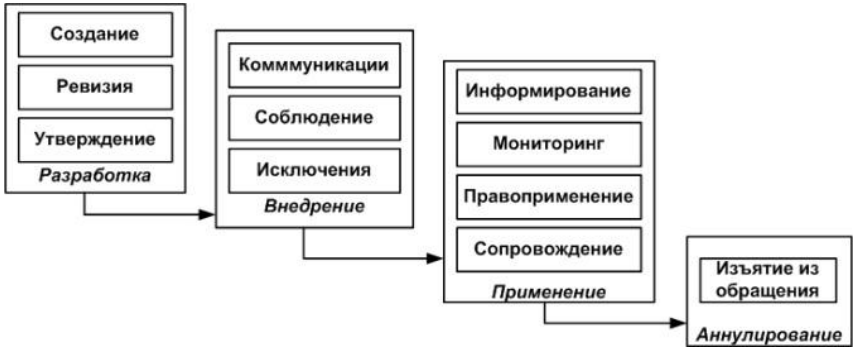
«ПЛАНИРОВАНИЕ»: установление целей и процессов, необходимых для выработки результатов в соответствии с требованиями клиентов и политики организации;

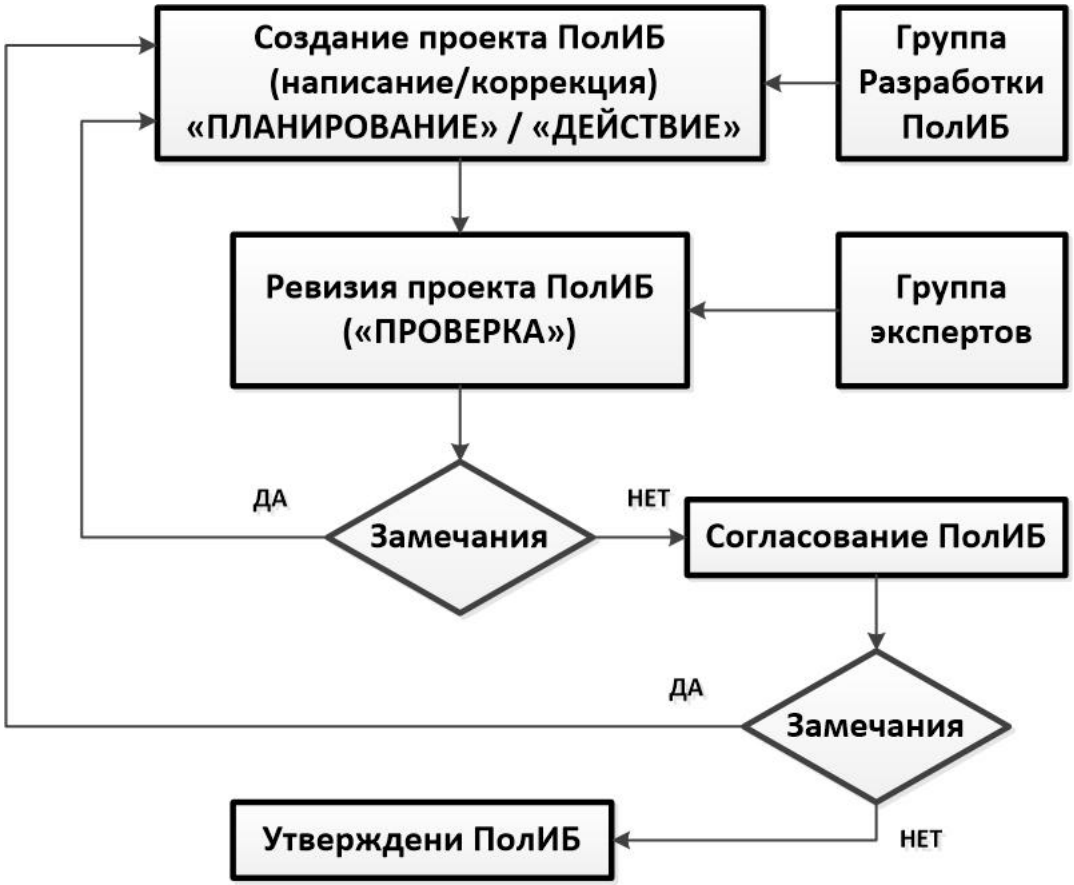
«ВЫПОЛНЕНИЕ» («реализация»): реализация запланированных процессов и решений;

«ПРОВЕРКА»: контроль и измерение процессов и производимых продуктов относительно политик, целей и требований к продукции и отчетность о результатах;

«ДЕЙСТВИЕ» («совершенствование»): принятие корректирующих и превентивных мер для постоянного совершенствования

4.2.Разработка ПолИБ («ПЛАНИРОВАНИЕ» - «ПРОВЕРКА» - «ДЕЙСТВИЕ»)

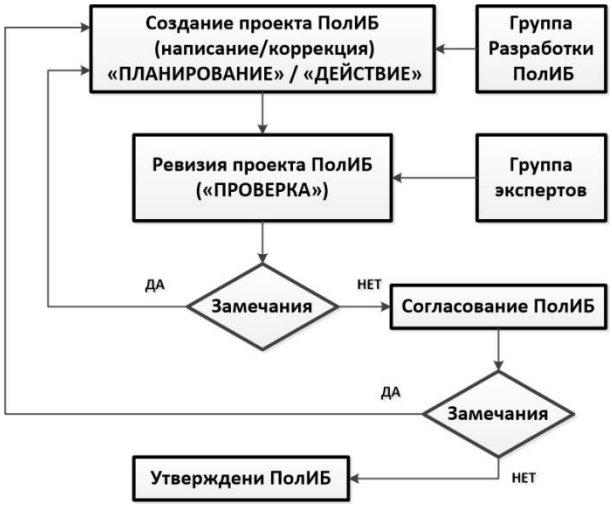




4.2.Разработка ПолИБ

Процессный подход: «ПЛАНИРОВАНИЕ» - «ПРОВЕРКА» - «ДЕЙСТВИЕ»

«Создание проекта ПолИБ» - формализованный шаг жизненного цикла ПолИБ, который включает в себя деятельность по планированию, проведению различных исследований, документированию необходимой информации и написанию самой ПолИБ.

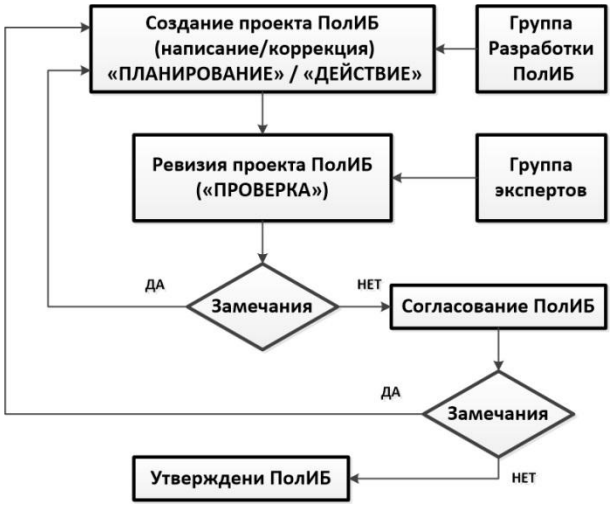


Мероприятия:

- **определяется, зачем ПолИБ нужна в организации (например, в соответствии с правовыми требованиями или требованиями регулирующих органов);**
- **устанавливаются границы и область действия;**
- **выделяются роли и ответственность, связанные с реализацией и внедрением ПолИБ;**
- **назначается группа конкретных людей, которые будут участвовать во всех процессах создания политики;**
- **оценивается осуществимость реализации ПолИБ.**

4.2.Разработка ПолИБ

Процессный подход: «ПЛАНИРОВАНИЕ» - «ПРОВЕРКА» - «ДЕЙСТВИЕ»

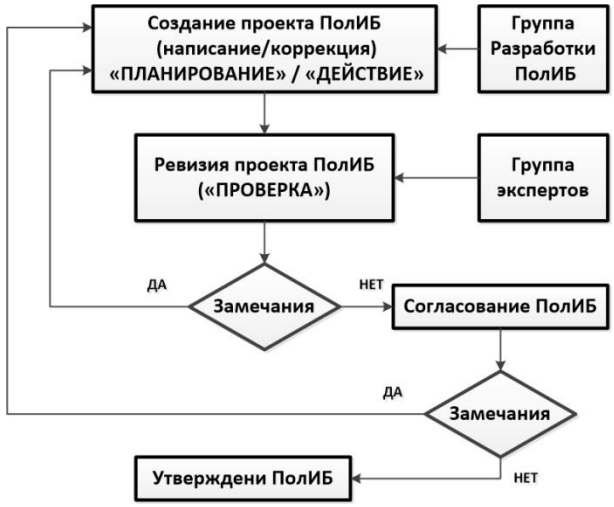


Группа разработки ПолИБ:

- *Представитель руководства организации (уровень принятия решений);*
- *Руководитель подразделения информатизации;*
- *Руководитель подразделения ИБ;*
- *Представитель юридического отдела;*
- *Аналитик из подразделения информатизации;*
- *Аналитик из подразделения ИБ;*
- *Представители подразделений, реализующих ПолИБ;*
- *Технический специалист для подготовки проекта ПолИБ.*

4.2.Разработка ПолИБ

Процессный подход: «ПЛАНИРОВАНИЕ» - «ПРОВЕРКА» - «ДЕЙСТВИЕ»



Группы экспертов ПолИБ:

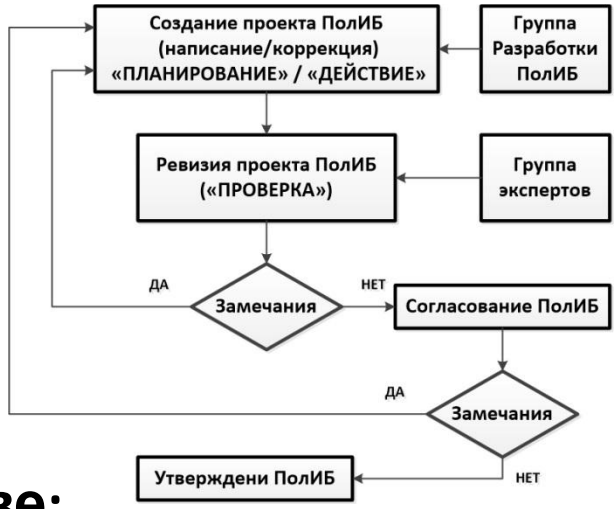
1. *Сотрудники организации, которые несут ответственность за то, что ПолИБ хорошо написана и понятна и выполнима*
2. *Представители руководства организации*

Цель группы 1: независимая оценка отдельными лицами (группами лиц) ПолИБ, предшествующая этапу согласования и окончательному ее утверждению.

В процессе оценки должны рассматриваться не только технические, но и юридические аспекты обеспечения ИБ, поскольку ПолИБ имеет непосредственное отношение к практической деятельности организации и напрямую затрагивают работу ее персонала.

4.2.Разработка ПолИБ

Процессный подход: «ПЛАНИРОВАНИЕ» - «ПРОВЕРКА» - «ДЕЙСТВИЕ»



Группы экспертов ПолИБ:

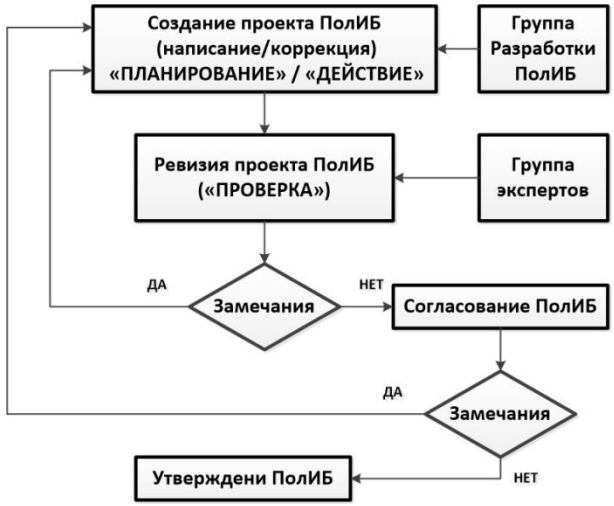
2.Представители руководства организации

Цель группы 2: оценить ПолИБ на основе:

1) **Результатов работы группы 1;**
2) **Реакции группы разработчиков;**
3) **Статуса предупреждающих и корректирующих действий;**
4) **Результатов предыдущего анализа со стороны руководства;**
5) **Особенностей последующей реализации ПолИБ;**
6) **Изменений в деятельности организации в случае реализации данной ПолИБ;**
7) **Тенденций, связанных с угрозами ИБ и уязвимостями;**
8) **Инцидентов ИБ, которые были ранее;**
9) **Рекомендаций, предоставленных соответствующими**

4.2.Разработка ПолИБ

Процессный подход: «ПЛАНИРОВАНИЕ» - «ПРОВЕРКА» - «ДЕЙСТВИЕ»



Согласование и утверждение ПолИБ:

Процесс согласования ПолИБ.

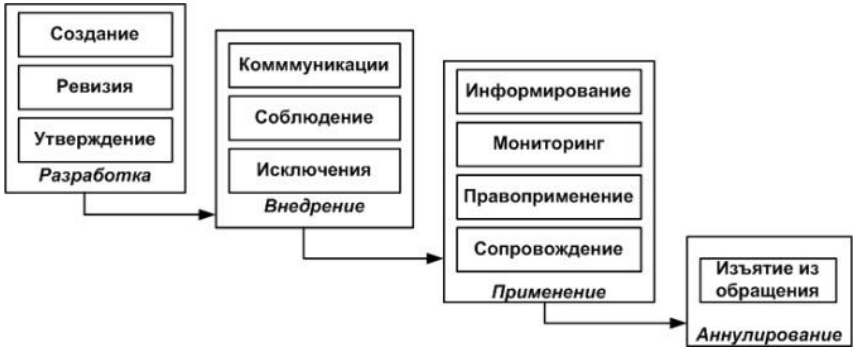
Роль разработчиков ПолИБ:

- **дать обоснованные разъяснения официальным лицам, имеющему полномочия согласовывать ПолИБ;**
- **координировать все действия по согласованию ПолИБ с этими официальным лицом;**
- **представить комментарии по рекомендациям группы экспертов;**
- **предпринимать должные усилия по расширению поддержки ПолИБ со стороны руководства организации.**

Процесс утверждения ПолИБ представляет собой простое одобрение руководством окончательной редакции документа. На бумажном документе с ПолИБ ставится подпись соответствующего уполномоченного должностного лица организации, после чего ПолИБ готова к

4.3.Внедрение ПолИБ

Процессный подход: «ПЛАНИРОВАНИЕ» - «ВЫПОЛНЕНИЕ» - «ПРОВЕРКА» - «ДЕЙСТВИЕ»



Мероприятия по внедрению ПолИБ: технические и организационные

«ПЛАНИРОВАНИЕ»:

- ***Выбор мер по обеспечению ИБ в соответствии с ПолИБ («соблюдение»);***
- **Распространение ПолИБ внутри организации и среди тех, на кого она распространяется – партнеров, клиентов и т. д. («коммуникации»);**
- ***Коррекция применимости ПолИБ («исключение»).***

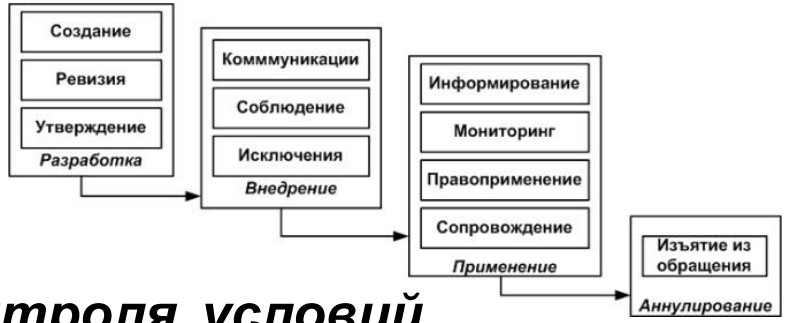
«ВЫПОЛНЕНИЕ»: внедрение мер по обеспечению ИБ.

«ПРОВЕРКА»: корректности внедрения мер по обеспечению ИБ.

«ДЕЙСТВИЕ»: принятие решения и коррекция внедрения

4.4.Применение ПолИБ

Процессный подход: «ПЛАНИРОВАНИЕ» - «ВЫПОЛНЕНИЕ» - «ПРОВЕРКА» - «ДЕЙСТВИЕ»



«ПЛАНИРОВАНИЕ»: *разработка мер контроля условий, результатов и уровня выполнения ПолИБ («сопровождение»);*

«ВЫПОЛНЕНИЕ»:

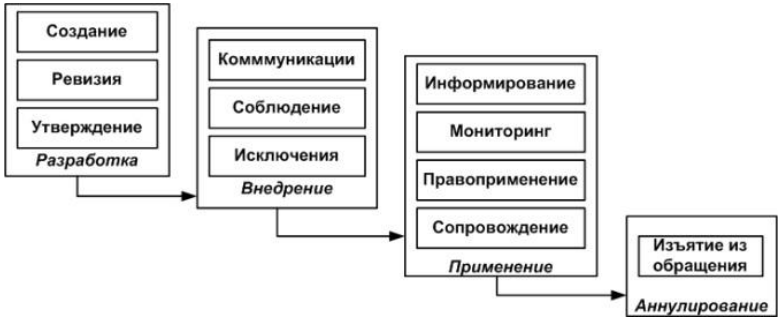
- *реализация мер контроля условий, результатов и уровня выполнения ПолИБ («мониторинг», аудит);*
- *реализация мер контроля правоприменимости ПолИБ («правоприменимость»);*

«ПРОВЕРКА»:

- *анализ результатов реализации мер контроля условий, результатов и уровня выполнения ПолИБ («мониторинг», «правоприменимость», аудит);*
- *информирование всех заинтересованных лиц о результатах контроля («информирование»);*
- *отслеживаются основные побудительные мотивы и события для внесения изменений в нее (например, изменения в технологиях, процессах, людях, самой организации, направленности бизнеса и т. д.), которые могут влиять на политику;*

4.4.Применение ПолИБ

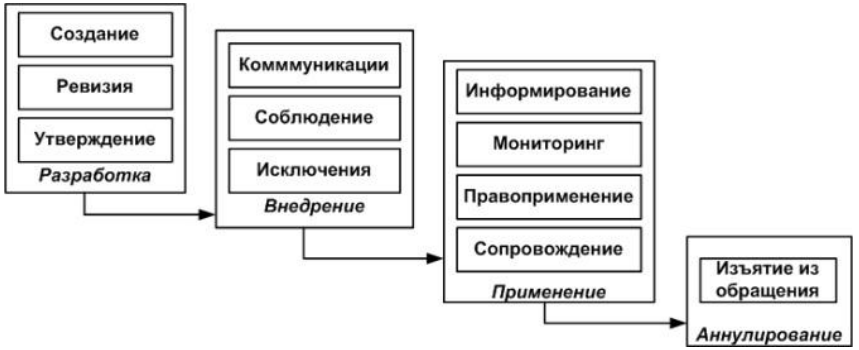
Процессный подход: «ПЛАНИРОВАНИЕ» - «ВЫПОЛНЕНИЕ» - «ПРОВЕРКА» - «ДЕЙСТВИЕ»



«ДЕЙСТВИЕ»: ***вырабатываются рекомендации и согласуются коррективы на:***

- ***внесение изменений методы контроля (внутренний цикл процессного подхода);***
- ***внесение изменений в ПолИБ в выбор мер по обеспечению ИБ (внешний цикл процессного подхода);***
- ***прекращение действия ПолИБ и изъятие ее из использования («изъятие из обращения») и разработку новой ПолИБ (внешний цикл процессного подхода).***

4.4.Анулирование ПолИБ



***Аннулирование** является заключительной стадией жизненного цикла ПолИБ, а изъятие из обращения – последним его шагом.*

Отслужившая свой срок ПолИБ удаляется из перечня действующих документов, архивируется для дальнейших ссылок на нее, а решение об отмене ПолИБ (включая обоснование, дату и т. д.) документируется.

Ответственностью за аннулирование ПолИБ наделяется соответствующее официальное лицо в организации.

Благодарю за внимание!

Толстой Александр Иванович

Национальный исследовательский ядерный университет «МИФИ» (НИЯУ МИФИ)
факультет «Кибернетика и информационная безопасность»
кафедра «Информационная безопасность банковских систем»
AITolstoj@mephi.ru