Учебная дисциплина «Управление информационной безопасностью»

Тема 3

Концептуальные подходы к управлению рисками ИБ

Толстой Александр Иванович

к.т.н., доцент

Доцент кафедры «Информационная безопасность банковских систем»

НИЯУ МИФИ,

Факультет «Кибернетика и информационная безопасность», кафедра

Москва, 2016

3. Концептуальные подходы к управлению рисками ИБ.

1.Почему «управление рисками ИБ»?

2.Нормативная база управления рисками ИБ

3.Термины и определения

4.Составляющие управления рисками ИБ

5.Стадии оценки рисков ИБ для ИС

6.Системный подход к управлению рисками ИБ

3. Концептуальные подходы к управлению рисками ИБ.

1.Почему «управление рисками ИБ»?

Смотри:

Тема 1.
1.Концептуальные основы обеспечения ИБ

1.Почему «управление рисками ИБ»?

Основные идеи современного подхода к обеспечению ИБ:

- ✔ **Эффективность обеспечения ИБ определяется эффективностью управления**
- ✔ **Базовыми процессами УИБ являются:**
  - Управление рисками ИБ.

Фундаментальные особенности безопасности:

1) Безопасность никогда не бывает абсолютной – всегда есть некоторый риск ее нарушения

«риск» – это вероятность причинения вреда с учетом его тяжести (ст.2 Федерального закона № 184-ФЗ «О техническом регулировании»);

2) Наступление рискового события в общем случае предотвратить невозможно, можно лишь понизить вероятность его наступления, т.е. добиться того, чтобы такие события будут наступать реже.

Следствие 1: усилия по обеспечению безопасности реально сводятся к задаче понижения уровня риска до приемлемого уровня, не более.

1.Почему «управление рисками ИБ»?

Основные идеи современного подхода к обеспечению ИБ:

- ✔ Эффективность обеспечения ИБ определяется эффективностью управления
- ✔ Базовыми процессами УИБ являются:
  - ✔ 1.Управление рисками ИБ.
  - ✔ 2.Управление инцидентами ИБ.
  - ✔ 3.Проверка и оценка деятельности по управлению ИБ
  - ✔ 4.Взаимодействие с управлением непрерывностью бизнеса

1.Почему «управление рисками ИБ»?

✔ **Базовыми процессами УИБ являются:**

- ***Управление рисками ИБ*** **– основа деятельности**
- **по обеспечению ИБ.**

«Актив» - все, что имеет ценность для организации **[ГОСТ Р ИСО/МЭК 13335-1-2006];**

«Угроза ИБ» - совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации **[ГОСТ Р 50922-2006];**

«Уязвимость» (брешь) (vulnerability) - слабость одного или нескольких активов, которая может быть использована одной или несколькими угрозами **[ГОСТ Р ИСО/МЭК 13335-1-2006];**

Если уязвимость соответствует угрозе, то существует

1.Почему «управление рисками ИБ»?

Разработки и реализация ПолИБ

Принципы обеспечения ИБ организации

Опыт

Модель угроз ИБ

Модель нарушителя ИБ

Идентификация активов и биз-нес-процессов

Мониторинг

Оценка рисков ИБ

Политика ИБ организации

Аудит

Реализация политики ИБ организации

1.Почему «управление рисками ИБ»?

Разработки и реализация ПолИБ

Принципы обеспечения ИБ организации

Опыт

Модель угроз ИБ

Модель нарушителя ИБ

Идентификация активов и биз-нес-процессов

Мониторинг

Оценка рисков ИБ

Политика ИБ организации

Аудит

Реализация политики ИБ организации

Что защищаем?

1.Почему «управление рисками ИБ»?

Разработки и реализация ПолИБ

Принципы обеспечения ИБ организации

Опыт

От чего защищаем?

Модель угроз ИБ

Идентификация активов и биз-нес-процессов

Модель нарушителя ИБ

Мониторинг

Оценка рисков ИБ

Политика ИБ организации

Аудит

Что защищаем?

Реализация политики ИБ организации

1.Почему «управление рисками ИБ»?

Разработки и реализация ПолИБ

Принципы обеспечения ИБ организации

Опыт

От чего защищаем?

Модель угроз ИБ

Идентификация активов и биз-нес-процессов

Модель нарушителя ИБ

Мониторинг

Оценка рисков ИБ

Политика ИБ организации

Аудит

Что защищаем?

Реализация политики ИБ организации

Как защищаем?

1.Почему «управление рисками ИБ»?

Основные процессы СУИБ

Управление рисками ИБ – один из процессов СУИБ

2.Нормативная база управления рисками ИБ:

стандарты (лучшая практика)

BS 7799–3:2006 «Information security management systems. Guidelines for information security risk management» («Системы менеджмента ИБ. Руководство по управлению рисками ИБ»)

↓

ISO/IEC 27005:2011 «Information technology. Security techniques. Information security risk management» («Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска ИБ»)

↓

ГОСТ Р ИСО/МЭК 27005–2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска ИБ»

↑ ↑ ↑

- *ГОСТ Р ИСО/МЭК ТО 13335–3–2007 «Информационная технология. Методы и средства обеспечения безопасности. Методы менеджмента безопасности информационных технологий»*
- *ГОСТ Р ИСО/МЭК ТО 13335–4–2007 «Информационная технология. Методы и средства обеспечения безопасности. Выбор защитных мер».*
- *ГОСТ Р ИСО/МЭК 13335–1–2006 «Информационная технология. Методы и средства обеспечения безопасности. Концепция и модели менеджмента безопасности информационных и*

2.Нормативная база управления рисками ИБ: стандарты

BS 7799–3:2006 «Information security management systems. Guidelines for information security risk management» **(«Системы менеджмента ИБ. Руководство по управлению рисками ИБ»)**

- ***содержит рекомендации по оценке рисков ИБ, их обработке, непрерывным действиям по управлению рисками ИБ и приложения с примерами активов, угроз ИБ, уязвимостей, методов оценки рисков ИБ;***
- ***описывает взаимосвязи между рисками ИБ и другими рисками организации, содержит требования и рекомендации по выбору методологии и инструментов для оценки рисков, определяет требования, предъявляемые к экспертам по оценке рисков и менеджерам, отвечающим за процессы управления рисками, содержит соображения по выбору законодательных и нормативных требований по ОИБ;***
- ***носит концептуальный характер, что позволяет экспертам по ИБ реализовать любые методы, средства и технологии оценки, отработки и управления рисками ИБ;***
- ***не содержат рекомендаций по выбору какого-либо аппарата оценки риска ИБ, а также по разработке мер, средств и сервисов защиты, используемых для минимизации рисков ИБ.***

2.Нормативная база управления рисками ИБ: стандарты

BS 7799–3:2006 «Information security management systems. Guidelines for information security risk management» («Системы менеджмента ИБ. Руководство по управлению рисками ИБ»)

↓

ISO/IEC 27005:2011 «Information technology. Security techniques. Information security risk management» («Информационная технология. Методы и средства обеспечения безопасности. Управление рисками ИБ»)

↓

- содержит общее руководство по управлению рисками ИБ, которое может быть использовано в различных типах организаций – коммерческих, некоммерческих, государственных;
- предназначен для организации адекватного бизнес-потребностям ОИБ на основе риск-ориентированного подхода.

2.Нормативная база управления рисками ИБ: стандарты

BS 7799–3:2006 «Information security management systems. Guidelines for information security risk management» («Системы менеджмента ИБ. Руководство по управлению рисками ИБ»)

↓

ISO/IEC 27005:2011 «Information technology. Security techniques. Information security risk management» («Информационная технология. Методы и средства обеспечения безопасности. Управление рисками ИБ»)

↓

ГОСТ Р ИСО/МЭК 27005–2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности»

↓

- *носит описательный характер и не содержит какой-либо конкретной методологии и даже не называет конкретные методы управления рисками ИБ*
- *устанавливает структурированный, систематический и строгий порядок анализа рисков ИБ посредством создания плана их обработки*
- *позволяет применяющей его организации самостоятельно учесть различные аспекты СУИБ, идентифицировать уровни своих рисков, определить критерии для принятия риска, идентифицировать приемлемые риски и т. д.*

2.Нормативная база управления рисками ИБ: стандарты

- ISO 31000:2009 «Risk management. Principles and guidelines».
- ISO/IEC 31010:2009 «Risk management. Risk assessment techniques».

- «Risk Management Guide for Information Technology Systems» (NIST Special Publication 800–30). U.S. Government Printing Office. Washington, 2002.
- AS/NZS 4360:2004 «Risk management». Standards Australia International Ltd, GPO Box 5420, Sydney, NSW 2001 and Standards New Zealand, Private Bag 2439, Wellington 6020, 2004.

ISO/IEC Guide 73:2009 «Risk management. Vocabulary. Guidelines for use in standards».

ГОСТ Р ИСО/МЭК 51897–2002 «Менеджмент риска. Термины и определения».

- Стандарт Банка России СТО БР ИББС-1.0 «Обеспечение информационной безопасности организаций банковской системы РФ. Общие положения».
- Рекомендации в области стандартизации Банка России РС БР ИББС-2.2–2009 «Обеспечение информационной безопасности организаций банковской системы РФ. Методика оценки рисков нарушения информационной безопасности».

3.Термины и определения

«риск» – это вероятность причинения вреда с учетом его тяжести

(ст.2 Федерального закона № 184-ФЗ «О техническом регулировании»);

«риск» – это сочетание вероятности события и его последствий (результатов событий, которые могут быть выражены качественно или количественно) (ГОСТ Р 51897–2002 «Менеджмент риска. Термины и определения»

«риск ИБ» → *«риск нарушения ИБ»*

«риск ИБ» - потенциальная возможность использования уязвимостей актива или группы активов конкретной угрозой ИБ для причинения ущерба организации. Измеряется риск ИБ исходя из комбинации вероятности события и его последствия (ГОСТ Р ИСО/МЭК 27005–2010);

«риск нарушения ИБ» - мера, учитывающая вероятность реализации угрозы ИБ и величину потерь (ущерба) от реализации этой угрозы (СТО БР ИББС 1.0–2010)

При этом :

угроза ИБ – это угроза нарушения свойств ИБ (доступности, целостности или конфиденциальности информационных активов организации);

ущерб - это утрата активов, повреждение (утрата свойств) активов и/или инфраструктуры организации или другой вред активам и/или

3.Термины и определения

«информационные риски» *- риски, которым подвергаются информационные активы организации или которые приводят к убыткам или ущербу в результате применения ИТ.*

«РИСК НАРУШЕНИЯ ИБ (РИСК ИБ) *- потенциальная возможность использования уязвимостей активов организации угрозами ИБ для причинения ущерба организации, измеряемая с учетом вероятности реализации угроз ИБ и величины ущерба от реализации угроз ИБ.*

3. Термины и определения

«управления рисками ИБ (information security risk management или IS risk management)» -

согласованные виды деятельности по руководству и управлению организацией в отношении рисков ИБ **[ГОСТ Р ИСО/МЭК 27001–2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»];**

скоординированные непрерывные действия по управлению и контролю рисков ИБ в организации **[BS 7799–3:2006 «Information security management systems. Guidelines for information security risk management»];**

скоординированные действия по руководству и управлению организацией в отношении рисков ИБ, обычно включающие в себя оценку, обработку, принятие и коммуникацию риска ИБ **[ГОСТ Р ИСО/МЭК ТО 13335–3–2007 «Информационная технология. Методы и**

3.Термины и определения

«управления рисками ИБ (information security risk management или IS risk management)» -

процесс выявления, контроля и минимизации или устранения рисков ИБ, оказывающих влияние на ИС, в рамках допустимых затрат [ГОСТ Р ИСО/МЭК 17799–2005 «Информационная технология. Методы и средства обеспечения безопасности. Практические правила управления информационной безопасностью»];

полный процесс идентификации, контроля, устранения или уменьшения последствий опасных событий, которые могут оказать влияние на ресурсы ИТТ [ГОСТ Р ИСО/МЭК 13335–1–2006 «Информационная технология. Методы и средства обеспечения безопасности. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий»];

непрерывный процесс, устанавливающий контекст управления рисками ИБ, оценку и обработку рисков ИБ на основе плана обработки рисков для реализации рекомендаций и принятых решений [ГОСТ Р ИСО/МЭК 27005–2010 «Информационная технология. Методы и средства обеспечения безопасности.

3.Термины и определения

«УПРАВЛЕНИЕ РИСКАМИ ИБ» *- скоординированная непрерывная деятельность по руководству и управлению организацией в отношении рисков ИБ на основе политики управления рисками ИБ и плана обработки рисков ИБ, обычно включающие в себя установление контекста управления рисками ИБ, оценку, обработку, принятие, мониторинг, пересмотр и коммуникацию рисков ИБ*

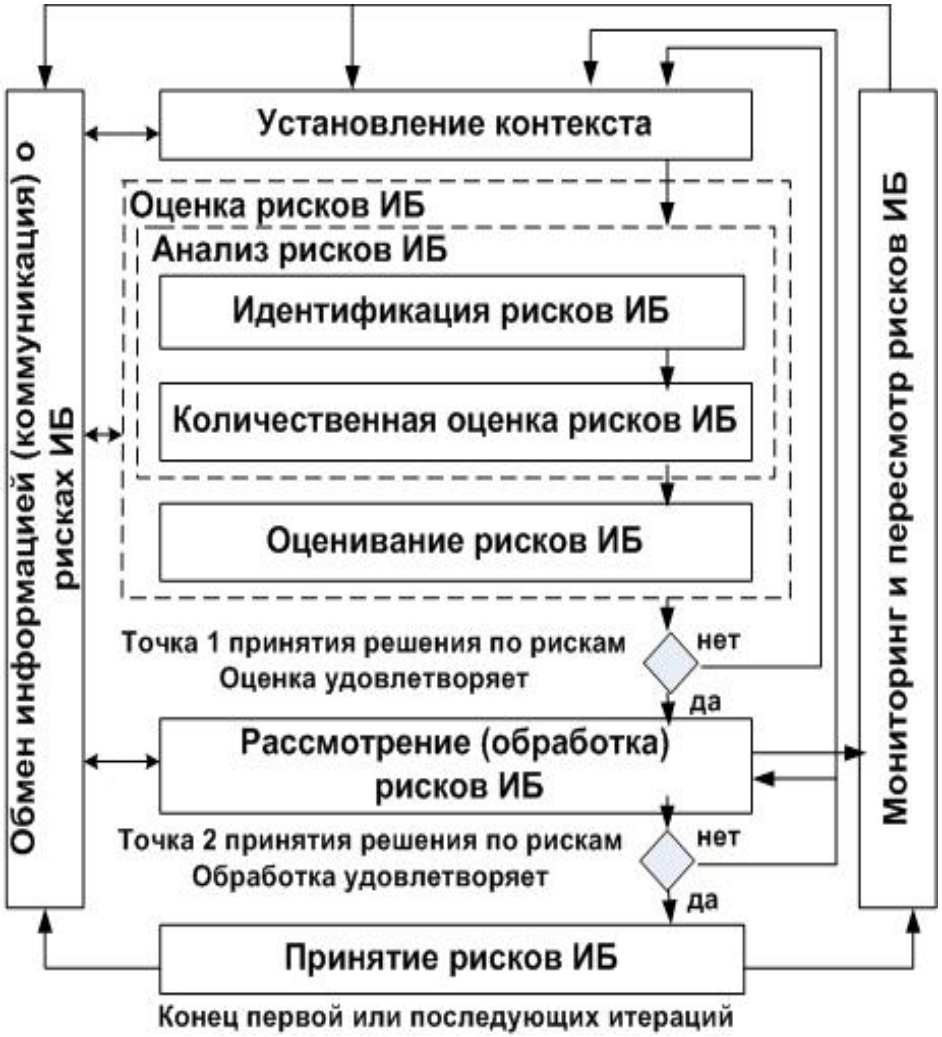
4.Составляющие управления рисками ИБ

«УПРАВЛЕНИЕ РИСКАМИ ИБ» *- скоординированная непрерывная деятельность по руководству и управлению организацией в отношении рисков ИБ на основе политики управления рисками ИБ и плана обработки рисков ИБ, обычно включающие в себя установление контекста управления рисками ИБ, оценку, обработку, принятие, мониторинг, пересмотр и коммуникацию рисков ИБ*

4.Составляющие управления рисками ИБ

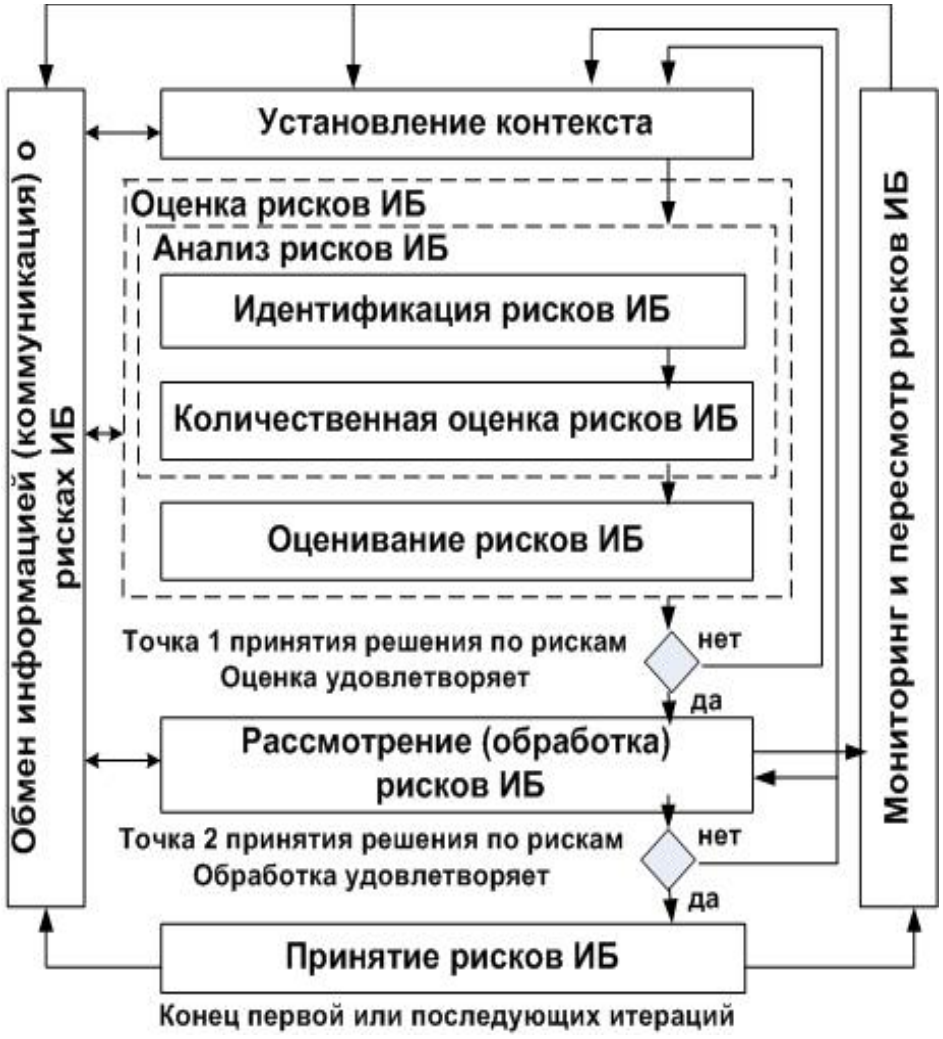
«УПРАВЛЕНИЕ РИСКАМИ ИБ» *- скоординированная непрерывная деятельность по руководству и управлению организацией в отношении рисков ИБ на основе политики управления рисками ИБ и плана обработки рисков ИБ, обычно включающие в себя установление контекста управления рисками ИБ, оценку, обработку, принятие, мониторинг, пересмотр и коммуникацию рисков ИБ*

4.Составляющие управления рисками ИБ



«УПРАВЛЕНИЕ РИСКАМИ ИБ» - ***скоординированная непрерывная деятельность по руководству и управлению организацией в отношении рисков ИБ на основе политики управления рисками ИБ и плана обработки рисков ИБ, обычно включающие в себя установление контекста управления рисками ИБ, оценку, обработку, принятие, мониторинг, пересмотр и коммуникацию рисков ИБ***

4.Составляющие управления рисками ИБ



Установление контекста – это процесс:

На входе:

- *внешний контекст (описание внешних условий функционирования организации),*
- *внутренний контекст (описание организации как объекта)*

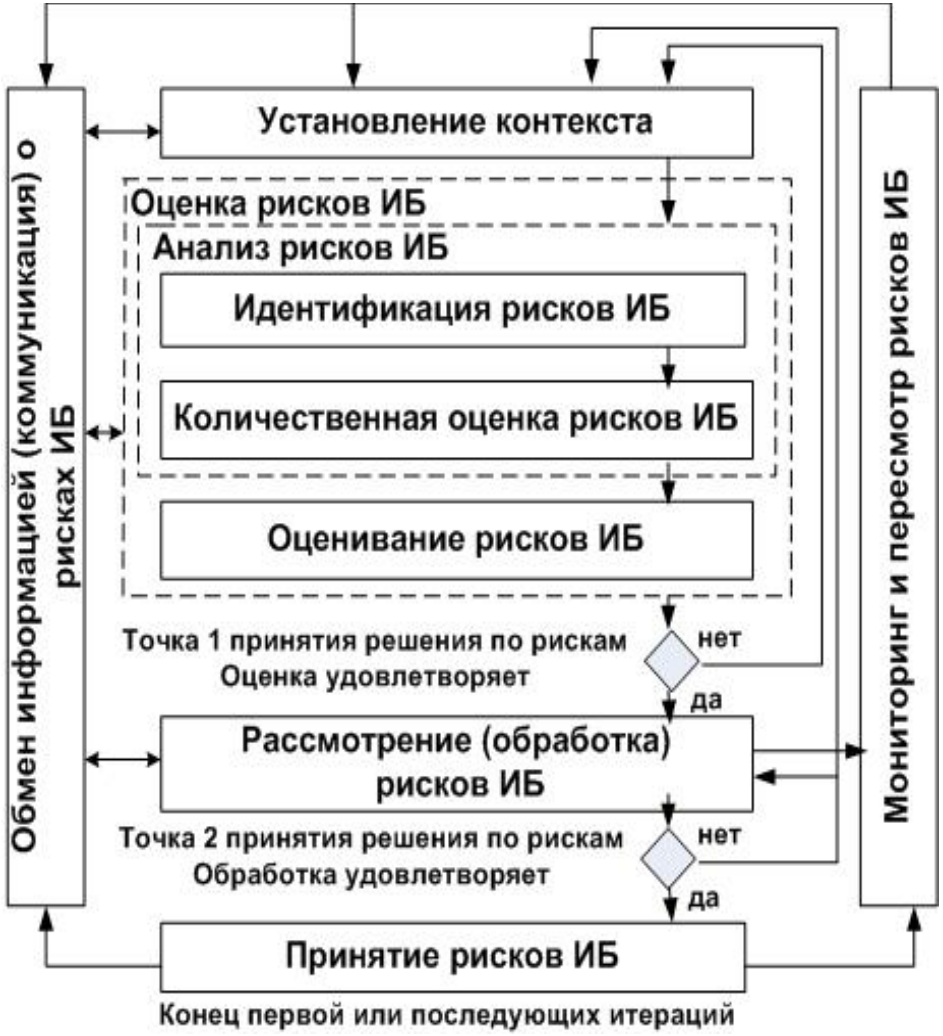
На выходе:

- *базовые критерии принятия решений в области управления рисками ИБ,*
- *определение области действия, ее границ и содержания деятельности организации по процессу управления рисками ИБ ,*
- *описание структуры процесса управления рисками ИБ.*

Цели:

- *Обеспечение функционирования последующих процессов управления рисками ИБ.*
- *Поддержка функционирования системы обеспечения ИБ*
- *Соблюдение соответствующих норм и правил;*
- *Подготовка плана реагирования*

4.Составляющие управления рисками ИБ



Оценка риска ИБ– - это совокупность процессов:

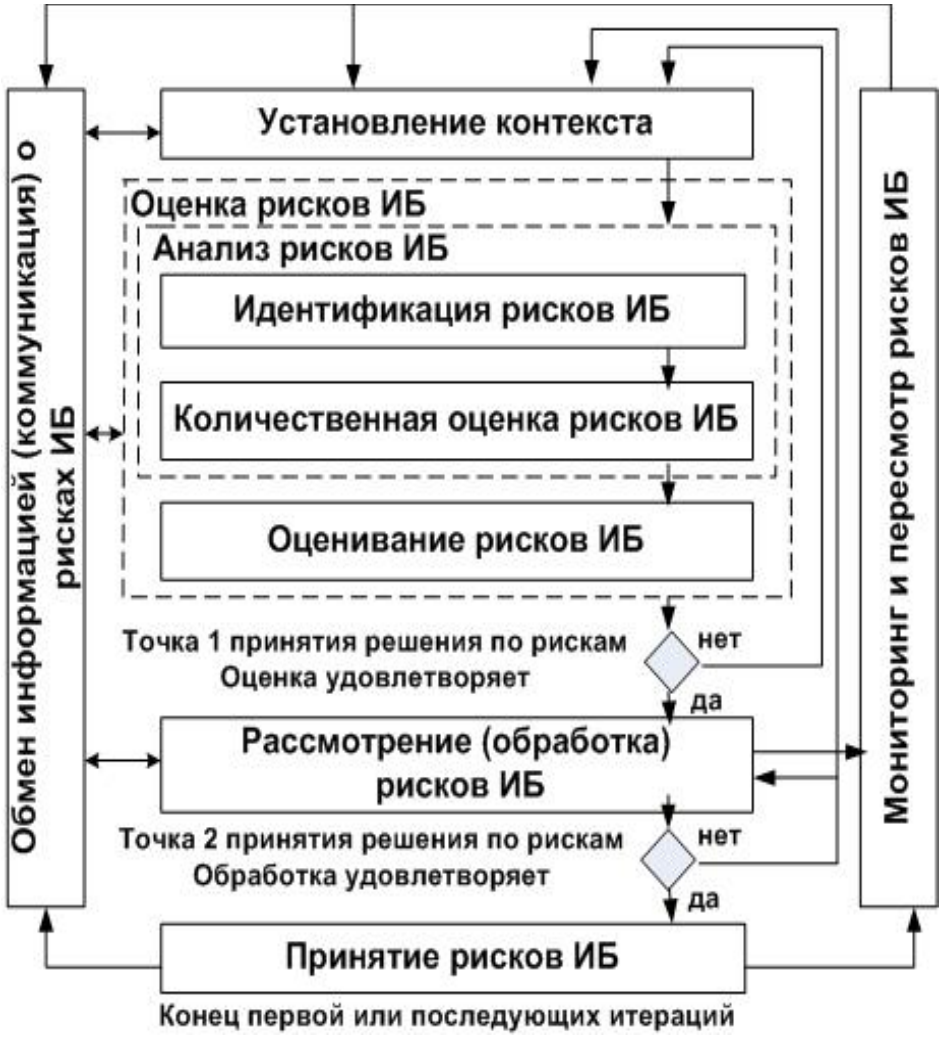
анализа рисков ИБ + оценивания рисков ИБ

Анализ рисков ИБ (IS risk analysis) - систематическое использование информации (исторических данных, результатов теоретического анализа, информированного мнения) для определения источников и количественной оценки рисков ИБ.

Это процесс понимания происхождения риска и определения уровня риска.

Анализ рисков ИБ обеспечивает базу для оценивания рисков ИБ, мероприятий по снижению рисков ИБ и принятия рисков ИБ.

4.Составляющие управления рисками ИБ



Оценка риска ИБ– - это совокупность процессов:

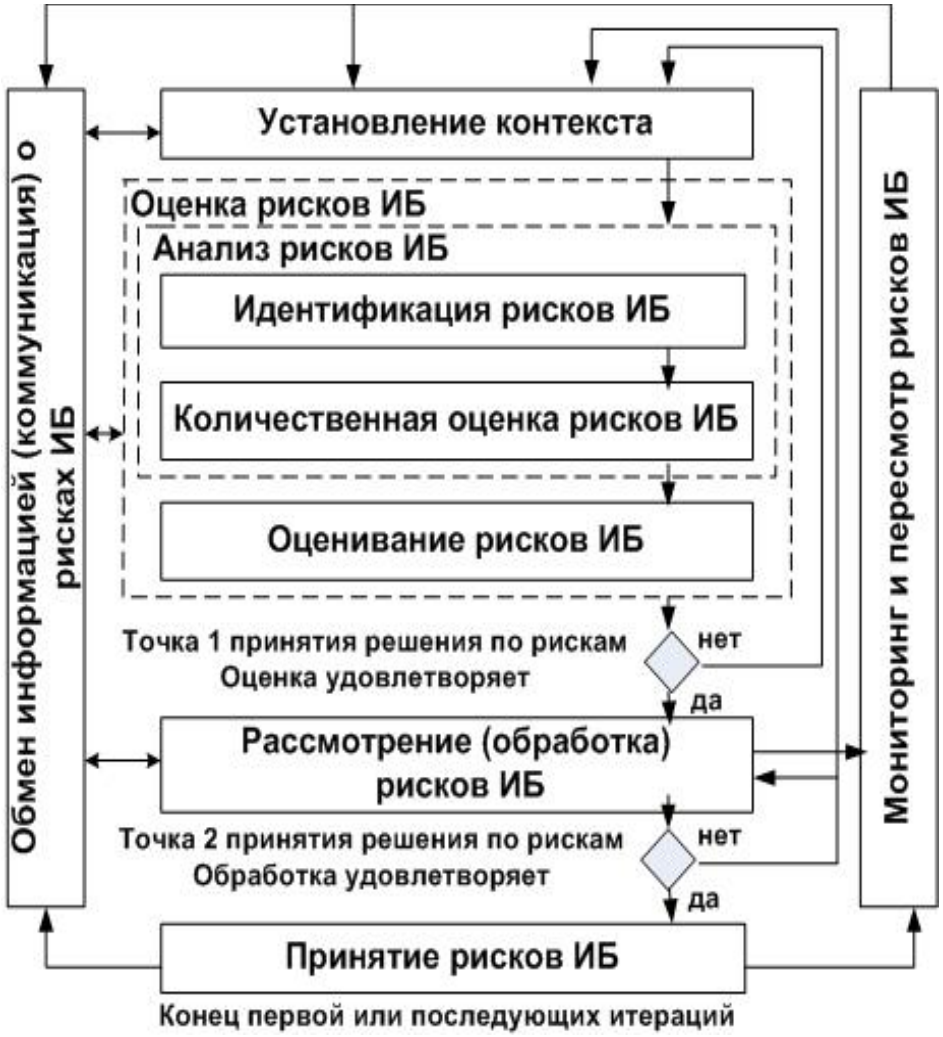
анализа рисков ИБ + оценивания рисков ИБ

Анализ рисков ИБ состоит из:

идентификации рисков ИБ и количественной оценки рисков ИБ

Идентификация рисков ИБ (IS risk identification) – деятельность (процесс) по нахождению (выявлению), составлению перечня рисков ИБ, исследования и описания элементов рисков ИБ (источников или опасности, событий, последствий и вероятности). Она включает идентификацию источников риска, событий, их причин и возможных последствий. Идентификация риска может включать статистические данные, теоретический анализ, обоснованную точку зрения и

4.Составляющие управления рисками ИБ



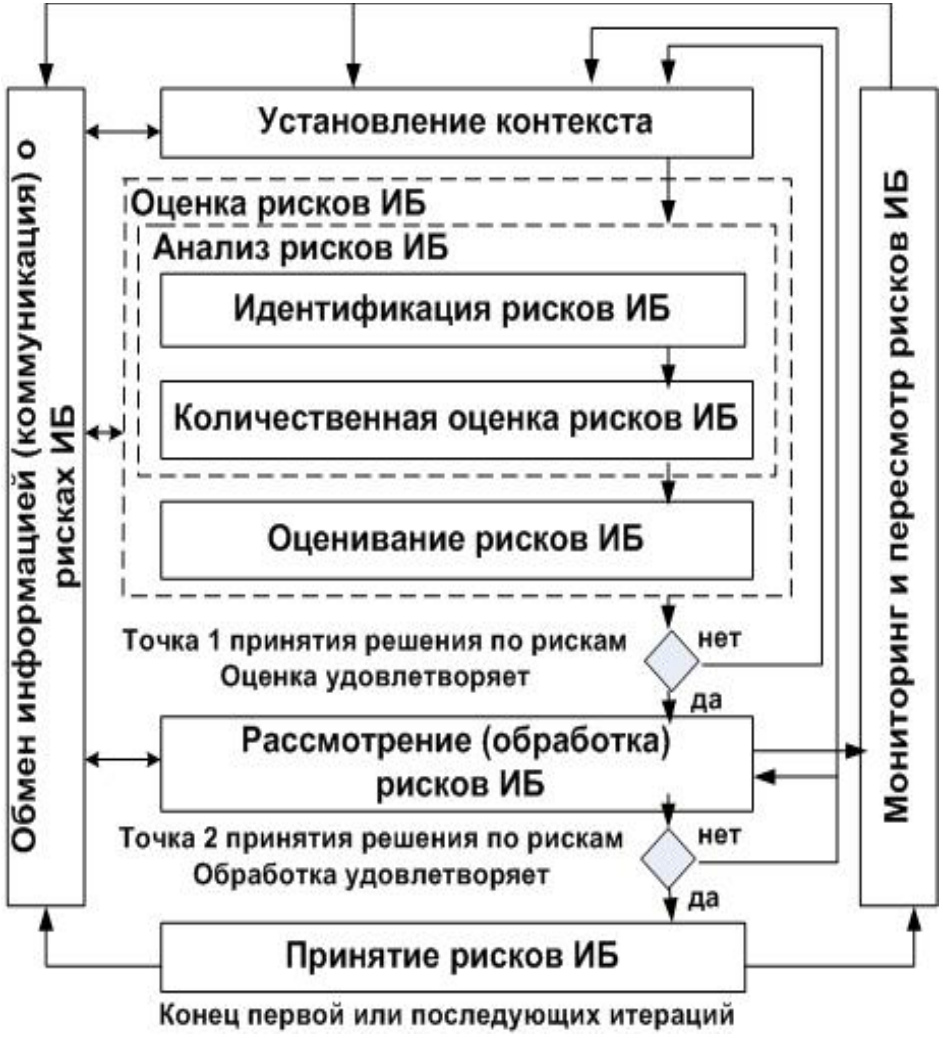
Оценка риска ИБ– - это совокупность процессов:
анализа рисков ИБ + оценивания рисков ИБ

Анализ рисков ИБ состоит из:
идентификации рисков ИБ и количественной оценки рисков ИБ

Количественная оценка или установление значения рисков ИБ (IS risk estimation) – деятельность (процесс) по присвоению значений вероятности и последствий рисков ИБ. Количественная оценка рисков ИБ может учитывать стоимость, прибыль, интересы причастных сторон и другие переменные, рассматриваемые при оценивании рисков ИБ.

Анализ рисков ИБ обеспечивает

4.Составляющие управления рисками ИБ



Оценка риска ИБ– - это совокупность процессов:

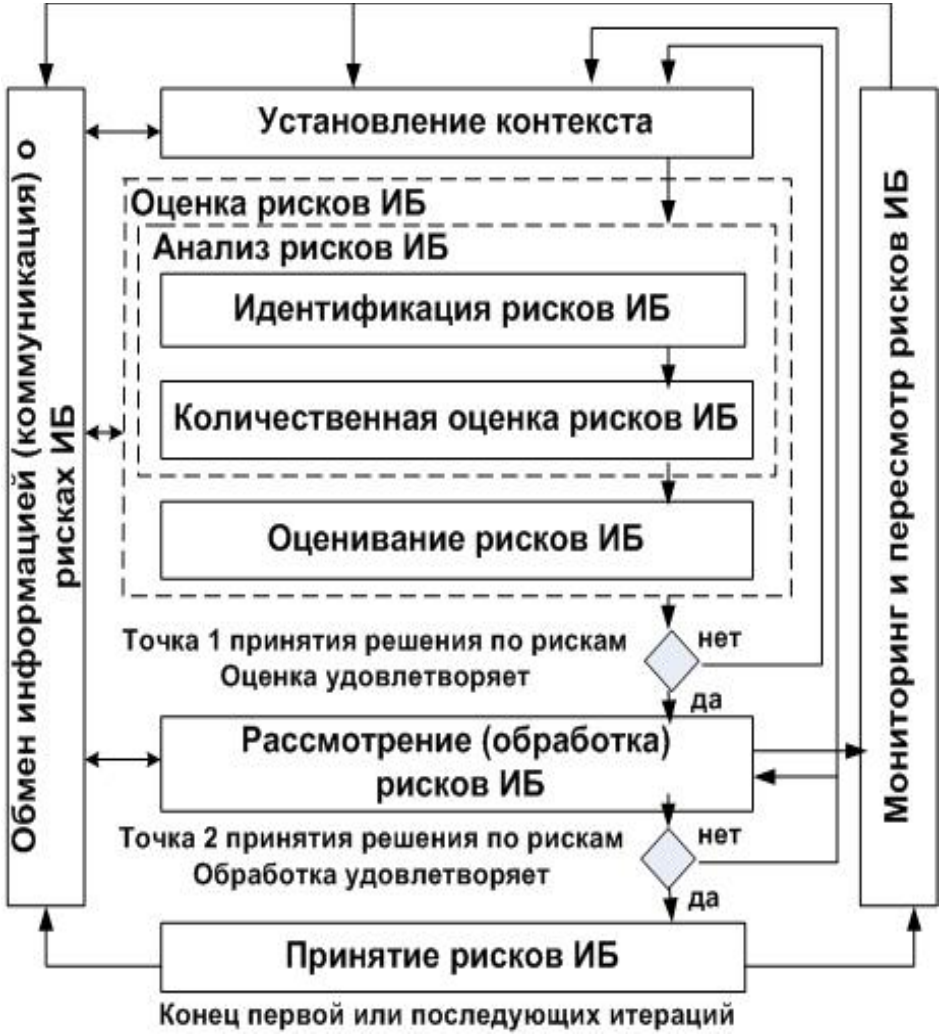
анализа рисков ИБ + оценивания рисков ИБ

Оценивание риска ИБ (IS risk evaluation) –

- ***процесс сравнения количественно оцененного риска с данными критериями риска для определения значимости риска ИБ. Этот же процесс иногда называется оценка значимости риска ИБ;***
  - ***Правила, по которым оценивают значимость риска ИБ, называются критериями риска ИБ.***
- ***процесс сравнения результатов анализа риска с установленными критериями риска для определения, является ли риск и/или его величина приемлемыми или допустимыми.***

Такое определение может быть

4.Составляющие управления рисками ИБ

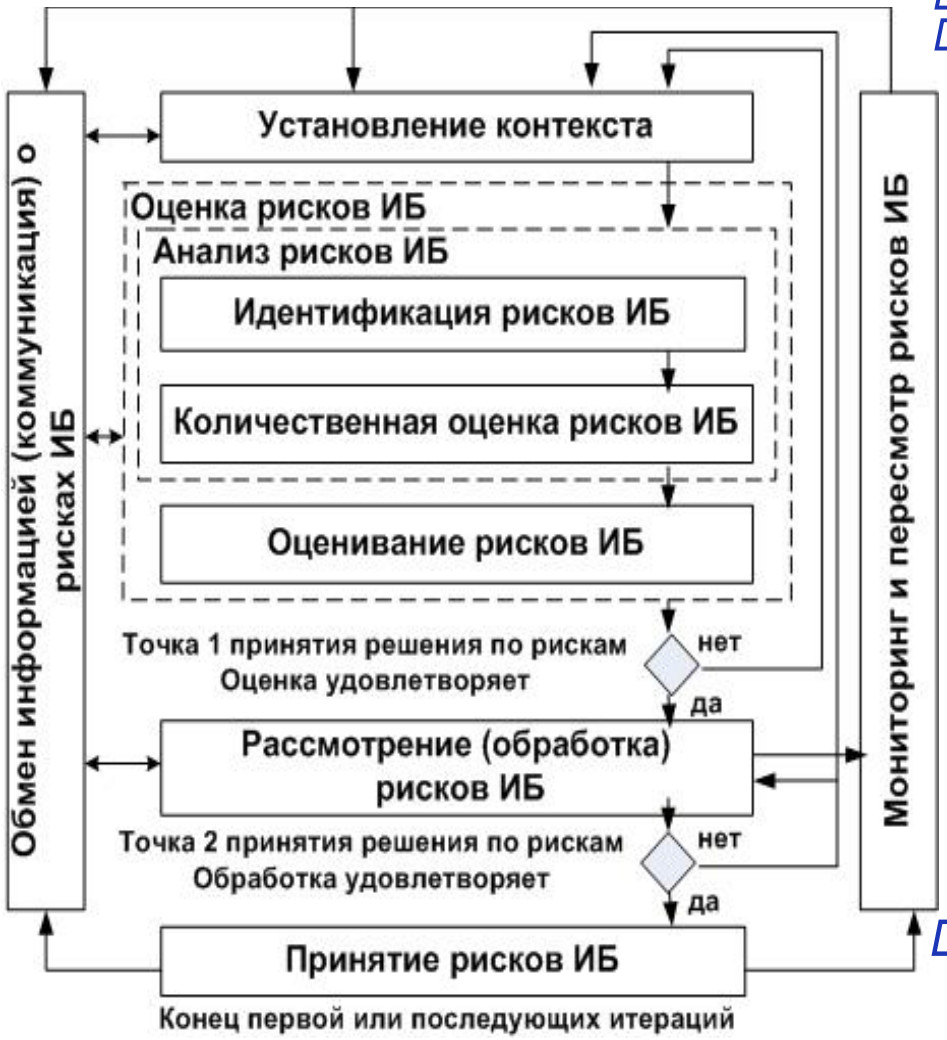


Таким образом, оценка риска ИБ - это

- *целостный процесс анализа и оценки значимости риска;*
- *целостный процесс анализа и оценивания риска ИБ;*
- *систематический и документированный процесс выявления, сбора, использования и анализа информации, позволяющей провести оценивание рисков ИБ, связанных с использованием информационных активов организации на всех стадиях их жизненного цикла.*

Точка 1

4.Составляющие управления рисками ИБ



Обработка рисков ИБ (IS risk treatment) – это процесс:

- ***изменения риска ИБ;***
- ***выбора и реализации мер по снижению (уменьшению, модификации), переносу или уходу от риска ИБ;***

Снижение/уменьшение риска ИБ (IS risk reduction) – действия, предпринятые для уменьшения вероятности, негативных последствий или того и другого вместе, связанных с риском ИБ.

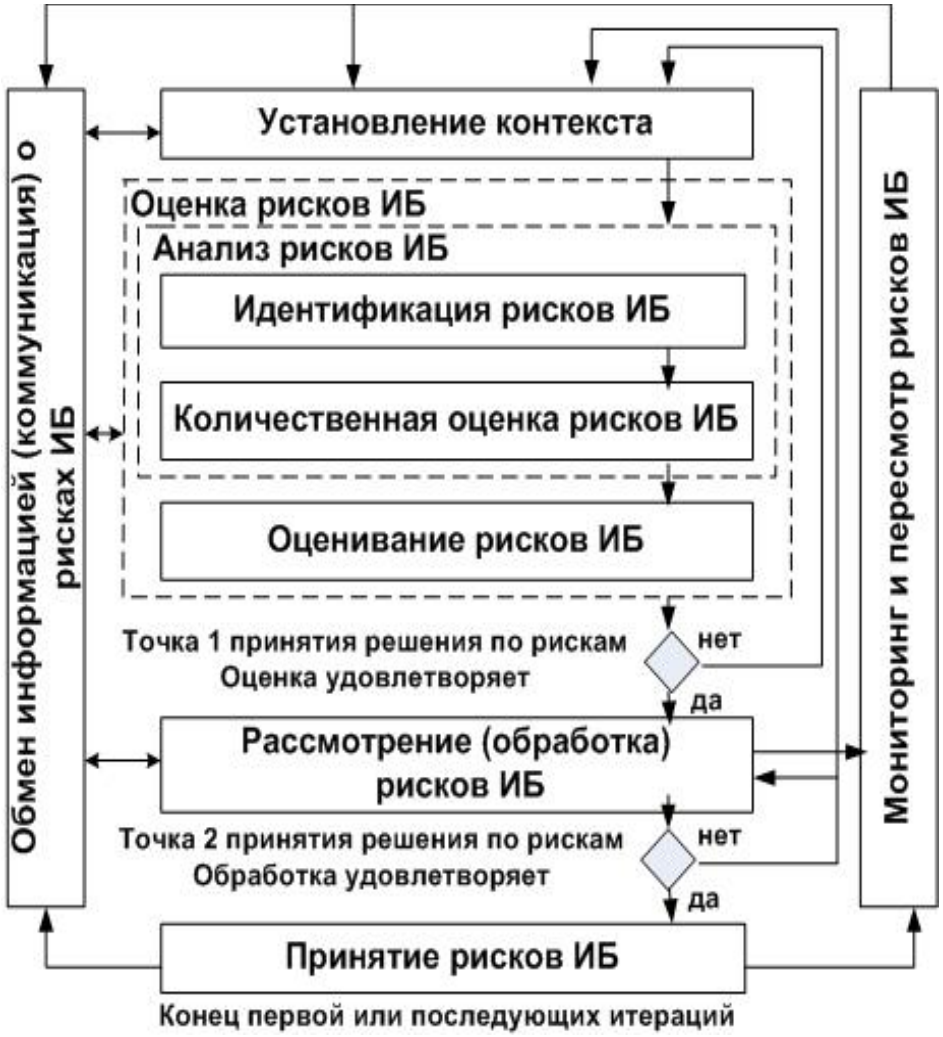
Перенос риска ИБ (IS risk transfer) – разделение с другой стороной бремени потерь от риска ИБ. Перенос риска ИБ может быть осуществлен страхованием или другими соглашениями

Уход от риска ИБ/избежание риска ИБ (IS risk avoidance) – решение не быть вовлеченным в рискованную ситуацию или действие, предупреждающее вовлечение в нее. Решение может быть принято на основе результатов оценивания риска ИБ.

- ***выбора и осуществления защитных мер, снижающих риски ИБ;***

Меры по обработке рисков ИБ могут

4. Составляющие управления рисками ИБ



Обработка рисков ИБ (IS risk treatment):

Меры по обработке рисков ИБ могут включать в себя их оптимизацию или сохранение.

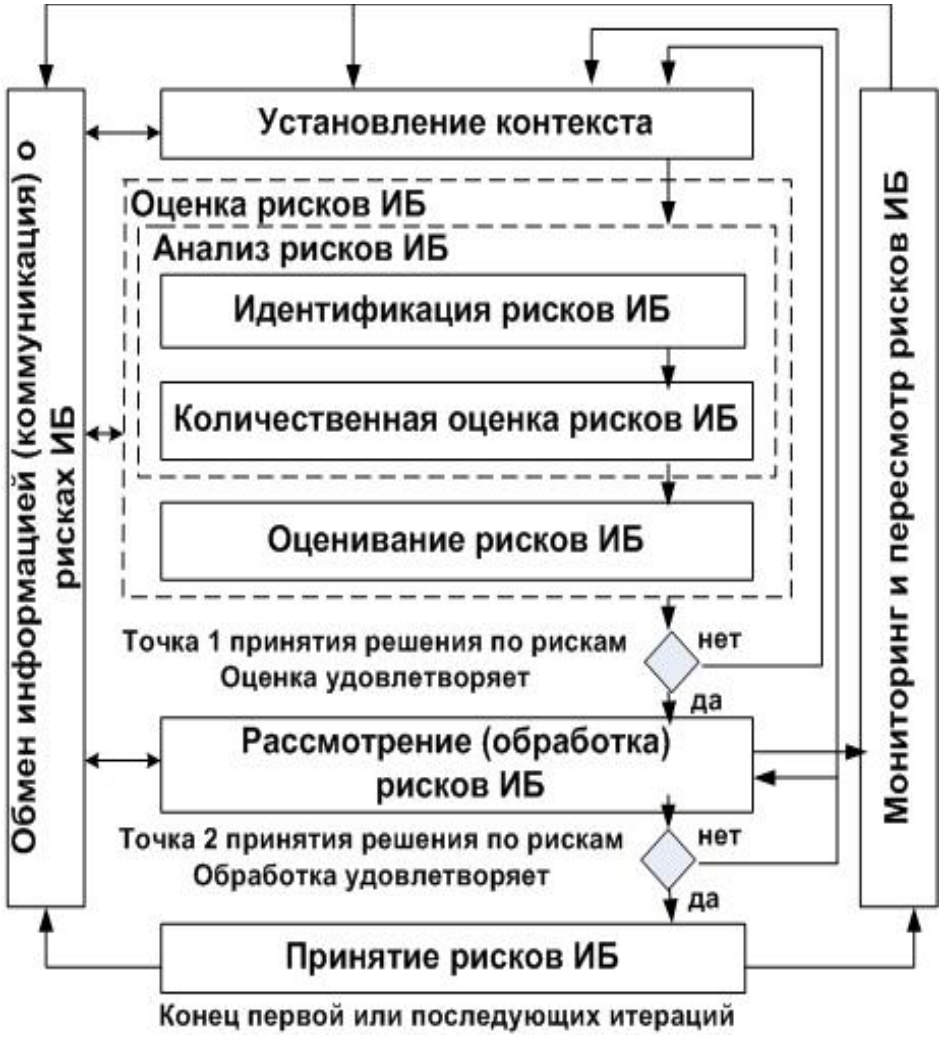
Оптимизация риска ИБ (risk optimization) – процесс, связанный с риском ИБ, направленный на минимизацию негативных последствий и их вероятности. Оптимизация риска ИБ зависит от критериев риска ИБ с учетом стоимости и законодательных требований.

Сохранение/удержание риска ИБ (IS risk retention) – принятие бремени потерь от конкретного риска ИБ. Сохранение риска ИБ не включает в себя обработку риска ИБ в результате страхования или перенос риска ИБ другими средствами.

Остаточный риск ИБ (IS residual risk) – риск ИБ, остающийся после обработки риска ИБ.

Точка 2

4. Составляющие управления рисками ИБ



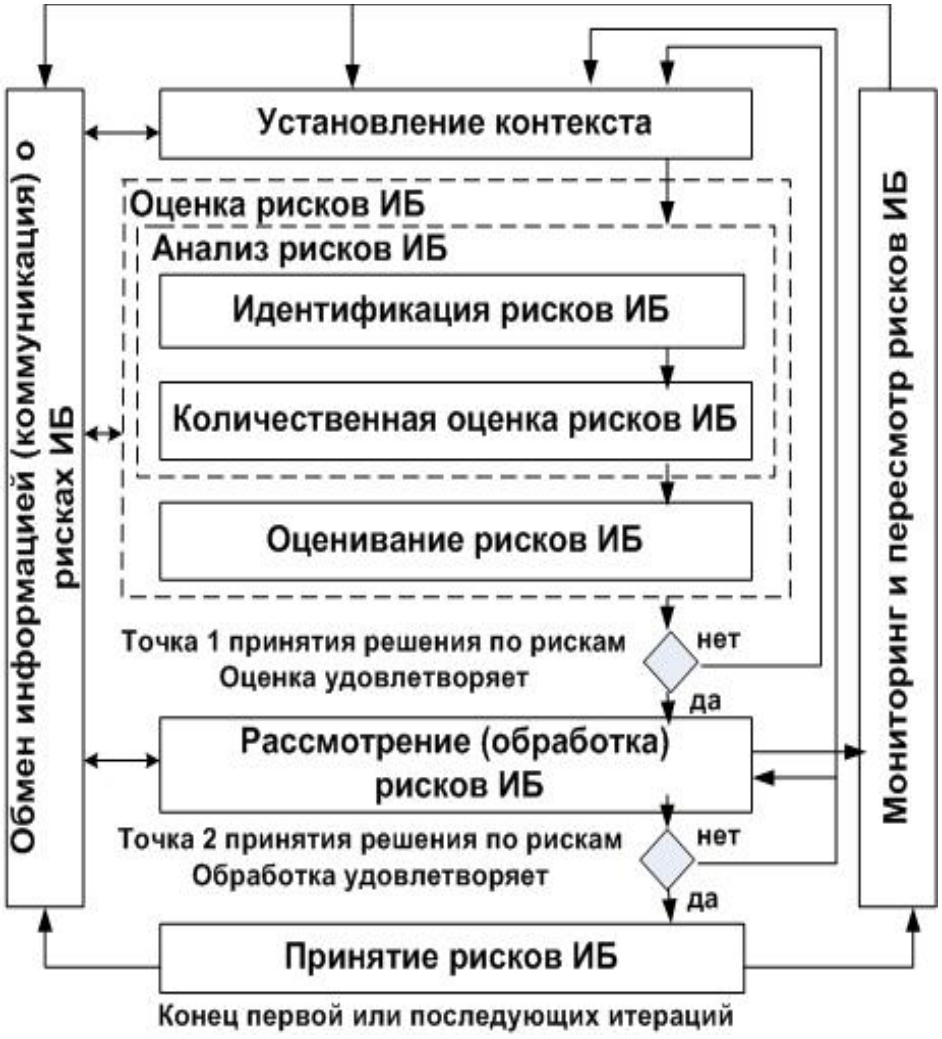
***Принятие рисков ИБ** (IS risk acceptance) – решение принять (взять на себя) риски ИБ, зависящее от критериев рисков ИБ*

***Допустимый риск ИБ** – риск ИБ, предполагаемый ущерб от которого организация в данное время и в данной ситуации готова принять.*

***Контроль риска ИБ** (IS risk control) – действия, осуществляемые для выполнения решений в рамках управления рисками ИБ, включая мониторинг, переоценивание и действия, направленные на обеспечение соответствия принятым решениям.*

***Коммуникация рисков ИБ** (IS risk communication) – обмен информацией о рисках ИБ или совместное использование этой информации между лицом, принимающим решение, и другими причастными сторонами .*

4.Составляющие управления рисками ИБ



ВАЖНО:

Осознание риска ИБ (IS risk perception) – набор ценностей и озабоченностей, в соответствии с которыми причастная сторона рассматривает конкретный риск ИБ.
Осознание риска ИБ зависит от потребностей, результатов и знаний причастных сторон.

Финансирование риска ИБ (IS risk financing) – предусмотрение финансовых средств на расходы по обработке риска ИБ и сопутствующие затраты.

6.Системный подход к управлению рисками ИБ

«Процесс управления рисками ИБ» ***- систематическое применение политик, процедур и практик управления рисками ИБ к задачам коммуникации, установления контекста, идентификации, анализу, оцениванию, обработке, мониторинга и пересмотра (переоценки) риска ИБ.***

К управлению рисками ИБ, в соответствии со стандартами, применим системный подход.

Он основывается на том, что все процессы и явления, связанные с рисками ИБ, рассматриваются в их системной связи, учитывается влияние отдельных решений и элементов на систему в целом.

К управлению рисками ИБ применима модель PDCA .

6. Системный подход к управлению рисками ИБ

Модель Деминга (-Шухарта) – Цикл Деминга (PDCA)

«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

6.Системный подход к управлению рисками ИБ

Система управления рисками ИБ (СУРИБ) (IS risk management system) - ***набор элементов системы управления организации в отношении средств управления рисками ИБ на всех уровнях, включая стратегическое планирование, принятие решений и другие процессы, затрагивающие риски ИБ .***

Это часть общей системы управления организацией.

Внедрение такой системы основано на комплексном подходе к решению проблемы контроля над рисками ИБ, возникающими в ходе деятельности организации.

6.Системный подход к управлению рисками ИБ

СУРИБ объединяет в себе три составляющие:

1) совокупность формализованных взаимосвязанных процессов, обеспечивающих все этапы управления рисками ИБ – от анализа и планирования, до проверки и совершенствования;

2) международные, национальные, ведомственные и иные стандарты, технологии, методики управления рисками ИБ, представленные в виде документального обеспечения, обязательно включающего политику управления рисками ИБ, методологию оценки рисков ИБ, план обработки рисков ИБ, декларация о применимости и т. д.;

3) организационную структуру управления рисками ИБ и квалифицированные кадры, состоящую из нескольких уровней (минимально трех).

6.Системный подход к управлению рисками ИБ

СУРИБ организации предусматривает работу в следующих режимах:

- **обычный, действующий по умолчанию в обычных условиях ведения бизнеса;**
- **контроля, применяемый к отдельному подразделению, при накоплении сигналов о концентрации рисков ИБ, по особым решениям руководства и т. д.;**
- **чрезвычайный, реализуемый по отношению ко всей организации при сигнале о превышении допустимого уровня концентрации рисков;**
- **отладки – режим испытания СУРИБ, внедрения новых продуктов и процедур, устанавливаемый по решению руководства.**

6.Системный подход к управлению рисками ИБ

Наличие СУРИБ в организации способствует следующему:

- ***риски ИБ идентифицированы;***
- ***риски ИБ оценены с точки зрения их последствий для бизнеса и вероятности их осуществления;***
- ***информация о вероятности и последствиях этих рисков ИБ доведена до сведения и понята всеми причастными и заинтересованными сторонами;***
- ***приоритетный порядок обработки рисков ИБ установлен;***
- ***приоритетность действия по снижению рисков ИБ выполняется;***
- ***заинтересованные стороны участвуют в принятии решений по рискам ИБ и информируются о положении дел в области управления рисками ИБ;***
- ***осуществляется мониторинг эффективности обработки рисков ИБ;***
- ***риски ИБ и процесс управления рисками ИБ регулярно контролируются и пересматриваются;***
- ***собирается информация для усовершенствования подходов к управлению рисками ИБ;***

Учебная дисциплина «Управление рисками ИБ» ***- только для Б02-44М***

Направление подготовки: 10.04.01 «ИБ» (магистратура)

Семестр: 2

Перечень тем:

1. ***Базовая терминология***
2. ***Нормативное обеспечение управления рисками ИБ.***
3. ***Оценка рисков ИБ.***
4. ***Обработка рисков ИБ.***
5. ***Принятие, коммуникация, мониторинг и пересмотр рисков ИБ. Обеспечение управления рисками ИБ***

Практические занятия и выполнение домашнего задания: ***Оценка и обработка рисков ИБ***

Рекомендованная литература:

Серия «Вопросы управление информационной безопасностью». Книга 2: Управление рисками информационной безопасности. Учебное пособие. для вузов /Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия–Телеком, 2012. – 130 с.

ЭОК-2 «УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ» (199)

Благодарю за внимание!

Толстой Александр Иванович

AITolstoj@mephi.ru

8(499)324-97-35