Основы информационной безопасности критически важных объектов

Учебная дисциплина ОИБ КВО

Тема 4

Исходная концептуальная схема обеспечения ИБ

Толстой Александр Иванович

к.т.н., доцент

Кафедра «Информационная безопасность банковских систем»

Институт интеллектуальных кибернетических систем

Факультет «Кибернетика и информационная безопасность»

НИЯУ МИФИ

Москва, 2017

4.Исходная концептуальная схема обеспечения ИБ

4.1.Традиционный подход

4.2.Специфика обеспечения ИБ

4.3.Современный подход к обеспечению ИБ

4.4.Система управления ИБ

4.1.Традиционный подход

Информационная безопасность - состояние защищённости информации, которое достигается обеспечением совокупности для нее свойств доступности, целостности, конфиденциальности, аутентичности (подлинности), неотказуемости (неоспоримости) и достоверности (функциональности).

Цель обеспечения ИБ:

Обеспечить сохранность основных свойств информации (свойств ИБ): доступности, целостности, конфиденциальности, …

4.1.Традиционный подход

Информационная безопасность - состояние защищённости информации, которое достигается обеспечением совокупности для нее свойств доступности, целостности, конфиденциальности, аутентичности (подлинности), неотказуемости (неоспоримости) и достоверности (функциональности).

Цель обеспечения ИБ:

Обеспечить сохранность основных свойств информации (свойств ИБ): доступности, целостности, конфиденциальности, …

Определения(ГОСТ Р 50922-2006):

«защита информации» – деятельность, направленная на предотвращение утечки защищаемой информации (конфиденциальность), несанкционированных и непреднамеренных воздействий (доступность, целостность)на защищаемую информацию;

«объект защиты» – информация или носитель информации или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации

4.1. Традиционный подход

Определения(ГОСТ Р 50922-2006):

«защита информации» **– деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию;**

«объект защиты» **– информация или носитель информации или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации;**

«объект информатизации» **–совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией;**

4.1. Традиционный подход

Определения(ГОСТ Р 50922-2006):

«защита информации» **– деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию;**

«объект защиты» **– информация или носитель информации или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации;**

«система защиты информации» **- совокупность органов и/или исполнителей, используемая ими техника защиты информации , а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации;**

4.1. Традиционный подход

Определения(ГОСТ Р 50922-2006):

«система защиты информации» **- совокупность органов и/или исполнителей, используемая ими техника защиты информации , а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации;**

«Комплексная система защиты информации» (КСЗИ)- совокупность мер и средств ЗИ.

«средство защиты информации» - техническое, программное средство, вещество и/или материал, предназначенные или используемые для защиты информации;

4.1. Традиционный подход

Определения(ГОСТ Р 50922-2006):

«система защиты информации» **- совокупность органов и/или исполнителей, используемая ими техника защиты информации , а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации;**

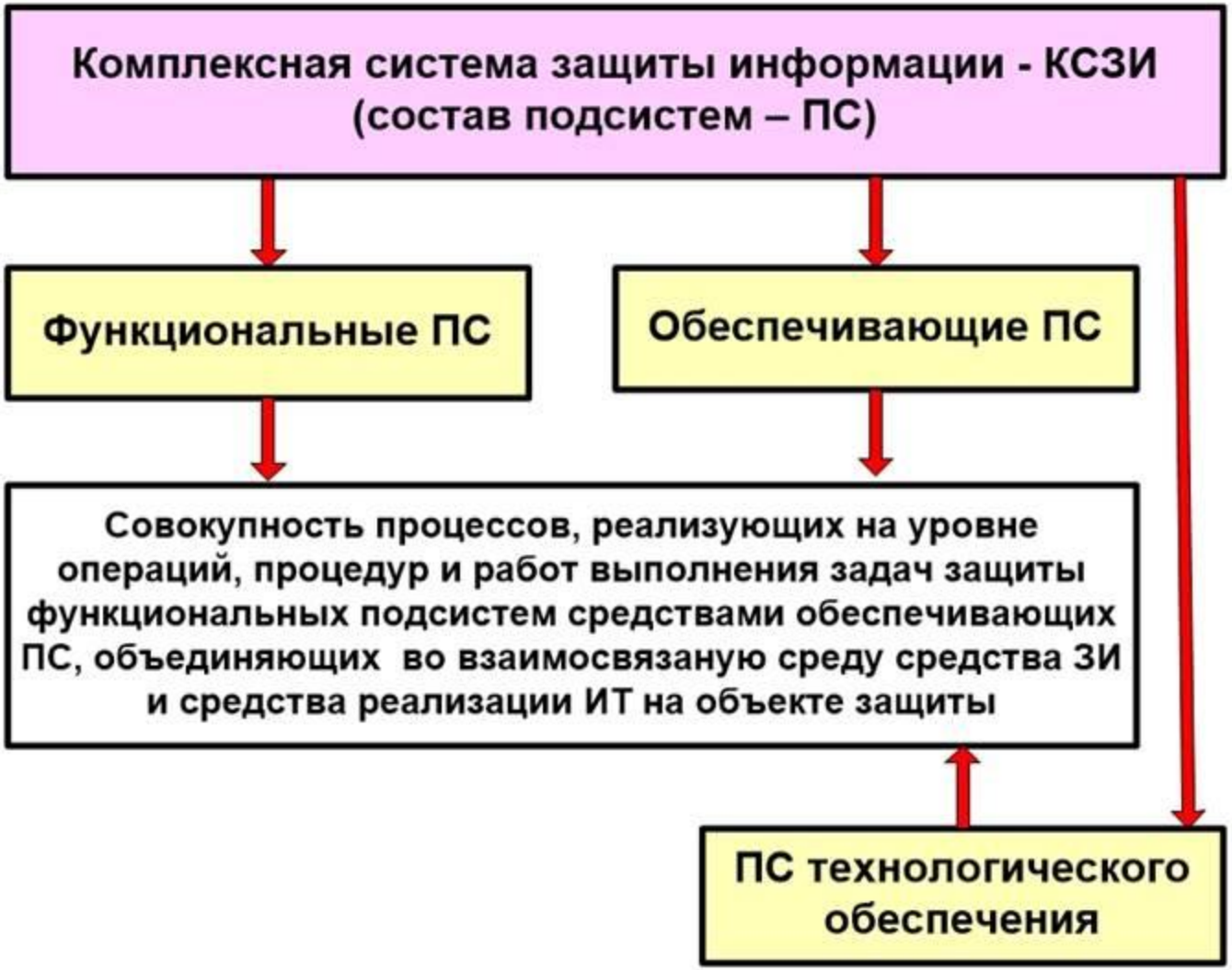
«Комплексная система защиты информации» (КСЗИ)**- совокупность мер и средств ЗИ.**

КСЗИ **- комплексный характер объединения составляющих системы.**

КСЗИ **- совокупность различных подсистем**

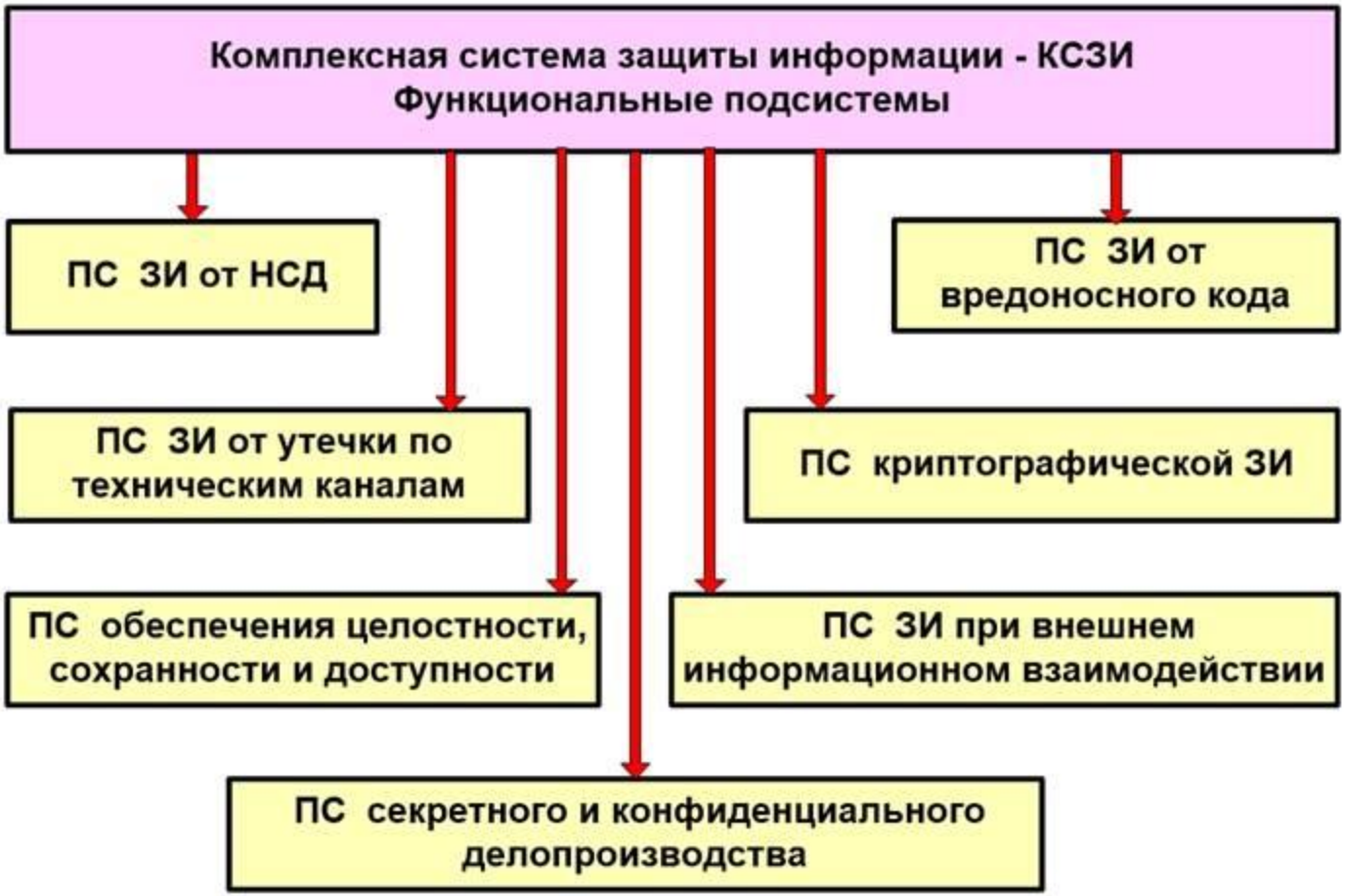
4.1. Традиционный подход

«Комплексная система защиты информации» (КСЗИ) - **совокупность различных подсистем.**



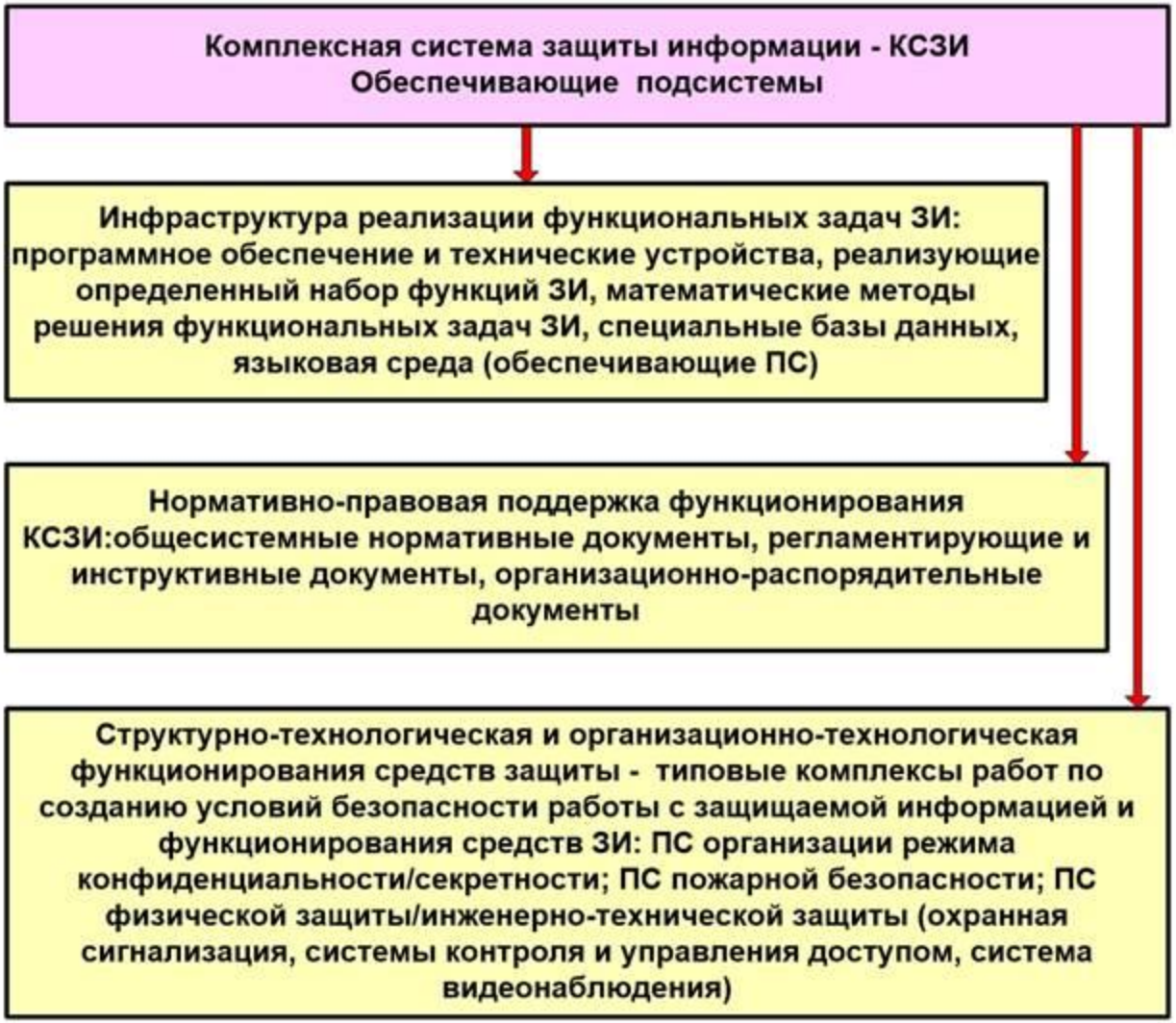
4.1. Традиционный подход

«Комплексная система защиты информации» (КСЗИ) - **совокупность различных подсистем.**



4.1. Традиционный подход

***«Комплексная система защиты информации» (КСЗИ)*- совокупность различных подсистем.**



4.1. Традиционный подход

***«Комплексная система защиты информации» (КСЗИ)*- совокупность мер и средств ЗИ.**

***КСЗИ* - комплексный характер объединения составляющих системы.**

***КСЗИ* - совокупность различных подсистем**

Проблема: снижение эффективность традиционного подхода

***Результат:* организация несет потери, так как на КСЗИ были зря потрачены немалые средств**

Вывод: кризис традиционного подхода

4.2.Специфика обеспечения ИБ

1.Деградация мер и средств защиты информации.

Правильно выстроенные процессы и используемые защитные меры в силу объективных причин имеют тенденцию к постепенному ослаблению своей эффективности.

Причины:

- **угрозы ИБ, их источники через некоторые промежутки времени изменяются под воздействием среды ведения бизнеса организации.**
- **защитные меры всегда тем или иным образом ограничивают сотрудников и сам бизнес (следствие - неправильного распределения ролей и ответственности и плохо отлаженного механизма выделения полномочий всем и все разрешено)**

Результат: организация несет потери, так как на систему ЗИ были зря потрачены немалые средства

4.2.Специфика обеспечения ИБ

2.Изменчивость (стохастичность) бизнеса.

Бизнес ведется в условиях изменчивой среды, то есть при большой неопределенности.

Это естественное свойство среды, которое должно учитываться организацией в ее деятельности.

В условиях неопределенности на бизнес уровне принимается решение о необходимости осуществить то или иное действие, отсрочить его, позаботиться о дополнительных гарантиях или ресурсах, либо вообще отказаться от выполнения действий.

При этом используются естественные для бизнеса механизмы самоконтроля, позволяющие проверить степень достижения заданной цели.

Изменчивость потребует постоянной подстройки обеспечения ИБ под изменение внутренней и внешней среды ведения бизнеса организации.

4.2.Специфика обеспечения ИБ

3.Обеспечение ИБ, в отличие от бизнеса, не имеет механизмов самоконтроля.

4.Эффективность деятельности по обеспечению ИБ реально проявляется только в момент атак.

5.Своевременность обнаружения проблем в области обеспечения ИБ.

6.Рост масштабов и сложности самих задач ОИБ организации.

Выход: целенаправленное управление всеми процессами обеспечения ИБ, основанное на системном методологическом подходе.

4.3.Современный подход к обеспечению ИБ

Основные идеи новой концептуальной схемы обеспечения ИБ:

Информационная безопасность - состояние защищённости информации, которое достигается обеспечением совокупности для нее свойств доступности, целостности, конфиденциальности, аутентичности (подлинности), неотказуемости (неоспоримости) и достоверности (функциональности).

Обеспечение ИБ – это системный процесс, а не состояние.

Процессом надо управлять!

Эффективность обеспечения ИБ определяется эффективностью управления

4.3.Современный подход к обеспечению ИБ

Основные идеи новой концептуальной схемы обеспечения ИБ:

Информационная безопасность - состояние защищённости информации, которое достигается обеспечением совокупности для нее свойств доступности, целостности, конфиденциальности, аутентичности (подлинности), неотказуемости (неоспоримости) и достоверности (функциональности).

Обеспечение ИБ – это системный процесс, а не состояние.

Процессом надо управлять!

✓ ***Эффективность обеспечения ИБ определяется эффективностью управления***

4.3.Современный подход к обеспечению ИБ

Основные идеи новой концептуальной схемы обеспечения ИБ:

- ✓ **Эффективность обеспечения ИБ определяется эффективностью управления**
- ✓ **Основной целью деятельности службы ИБ организации является содействие бизнесу – целям деятельности организации.**

Деятельность организации осуществляется через реализацию трех групп высокоуровневых бизнес-процессов:

- основные процессы (процессы основной деятельности),
- вспомогательные процессы (процессы по видам обеспечения),
- процессы менеджмента (управления) организацией.

Процессы по обеспечению ИБ –

вид вспомогательных процессов, реализующих поддержку (обеспечение) процессов основной деятельности организации в целях достижения ею максимально возможного результата.

4.3. Современный подход к обеспечению ИБ

Основные идеи новой концептуальной схемы обеспечения ИБ:

- ✓ Эффективность обеспечения ИБ определяется эффективностью управления
- ✓ Основной целью деятельности службы ИБ организации является содействие бизнесу – целям деятельности организации.

4.3. Современный подход к обеспечению ИБ

Основные идеи новой концептуальной схемы обеспечения ИБ:

- ✓ Эффективность обеспечения ИБ определяется эффективностью управления
- ✓ Основной целью деятельности службы ИБ организации является содействие бизнесу – целям деятельности организации.
- ✓ **Активы могут рассматриваться только в контексте целей деятельности организации, но не как иначе.**

Причем информационный актив является объектом взаимодействия различных субъектов

Определения:

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

«Собственник» - субъект хозяйственной деятельности, имеющий права владения, распоряжения или пользования активами, который заинтересован или обязан (согласно требованиям законов или иных законодательных или нормативно-правовых актов) обеспечивать защиту активов от угроз, которые могут снизить их ценность или нанести ущерб собственнику.

«Субъект» – сущность, инициирующая выполнение операций (собственник актива, служба ИБ собственника, злоумышленник (нарушитель);

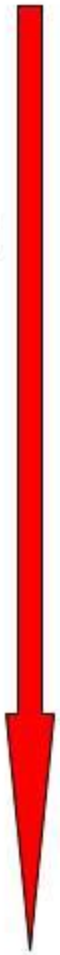
«Злоумышленник (нарушитель)» - лицо, которое совершает или совершило заранее обдуманное действие с осознанием его опасных последствий или не предвидело, но должно было и могло предвидеть возможность наступления этих последствий

4.3. Современный подход к обеспечению ИБ

Основные идеи новой концептуальной схемы обеспечения ИБ:

Примеры злоумышленников:

- ***постороннее лицо***, не имеющее легального доступа к системе и атакующее ее только с использованием общедоступных сетей;
- ***сотрудник*** организации, не имеющий легального доступа к атакуемой системе и сумевший подсмотреть/подобрать пароль легального пользователя;
- ***пользователь*** системы, обладающий минимальными полномочиями и использующий ошибки в ПО и администрировании системы;
- ***администратор*** системы, имеющий легально полученные полномочия, достаточные для успешной атаки на систему;
- ***разработчик системы***, встроивший в код системы “люки” (недокументированные возможности), которые в дальнейшем позволят ему осуществлять НСД к ресурсам системы.



4.3. Современный подход к обеспечению ИБ

Основные идеи новой концептуальной схемы обеспечения ИБ:

Конфликт целей собственника и злоумышленника по установлению контроля над активами

Факторы эффективного Ведения бизнеса

Риски

4.3.Современный подход к обеспечению ИБ

Основные идеи новой концептуальной схемы обеспечения ИБ:

- ✓ Эффективность обеспечения ИБ определяется эффективностью управления
- ✓ Основной целью деятельности службы ИБ организации является содействие бизнесу – целям деятельности организации.
- ✓ Активы могут рассматриваться только в контексте целей деятельности организации, но не как иначе.
- ✓ **Деятельности организации сопутствует значительное число различных рисков – риски ИБ один из видов рисков.**
- ✓ **Менеджмент рисков ИБ – основа деятельности по обеспечению ИБ.**

Определения (ГОСТ Р ИСО/МЭК 13335-1-2006):

«Риск»: потенциальная опасность нанесения ущерба организации в результате реализации некоторой угрозы с использованием уязвимостей актива или группы активов (определяется как сочетание вероятности события и его последствий .

«Менеджмент риска»: скоординированные действия по руководству и управлению в отношении риска с целью его минимизации.

4.3.Современный подход к обеспечению ИБ

Основные идеи новой концептуальной схемы обеспечения ИБ:

- ✓ **Деятельности организации сопутствует значительное число различных рисков – риски ИБ один из видов рисков.**

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.

4.3.Современный подход к обеспечению ИБ

Основные идеи новой концептуальной схемы обеспечения ИБ:

- ✓ **Деятельности организации сопутствует значительное число различных рисков – риски ИБ один из видов рисков.**

Фундаментальные особенности безопасности:

3) Измерить уровень безопасности невозможно, можно лишь косвенно его оценить, измерив соответствующие показатели, характеризующие состояние безопасности объекта.

Следствие 2: можно говорить только о вероятности наступления того или иного события и степени его последствий, т.е. использовать для оценок уровня безопасности рисковый подход.

4.3.Современный подход к обеспечению ИБ

Основные идеи новой концептуальной схемы обеспечения ИБ:

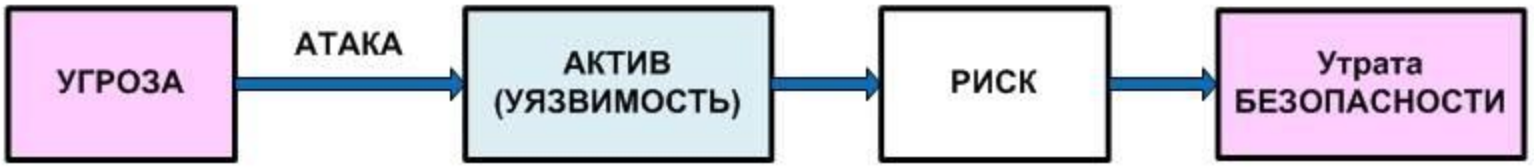
- ✓ **Менеджмент рисков ИБ – основа деятельности по обеспечению ИБ.**

«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];

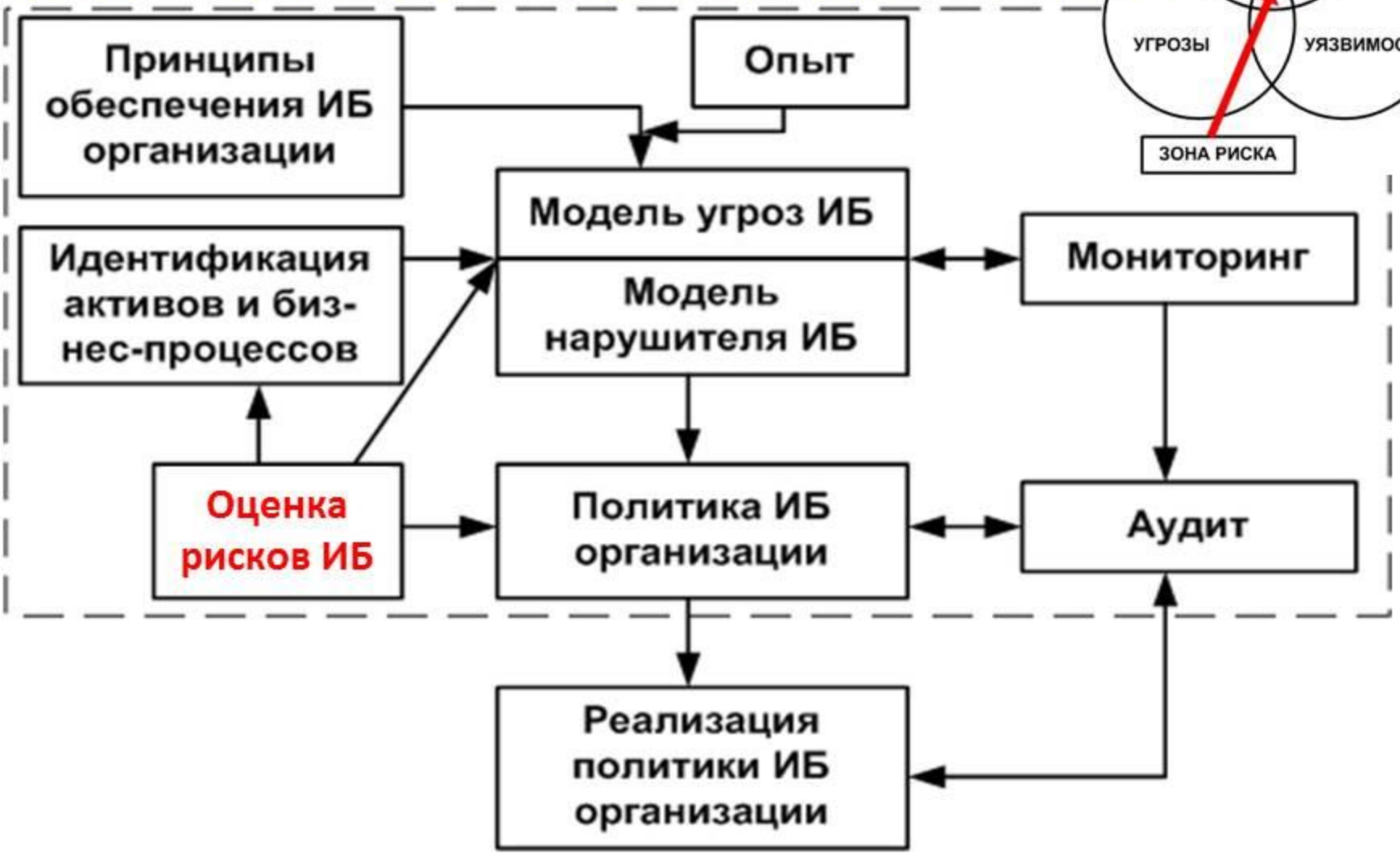
Если уязвимость соответствует угрозе, то существует риск (ИСО 2382-8:1998)



4.3.Современный подход к обеспечению ИБ

Основные идеи новой концептуальной схемы обеспечения ИБ:

- ✓ **Менеджмент рисков ИБ – основа деятельности по обеспечению ИБ**



4.3.Современный подход к обеспечению ИБ

Основные идеи новой концептуальной схемы обеспечения ИБ:

- ✓ **Менеджмент рисков ИБ – основа деятельности по обеспечению ИБ**

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?

4.3.Современный подход к обеспечению ИБ

Основные идеи новой концептуальной схемы обеспечения ИБ:

- ✓ **Менеджмент рисков ИБ – основа деятельности по обеспечению ИБ**

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

4.3.Современный подход к обеспечению ИБ

Основные идеи новой концептуальной схемы обеспечения ИБ:

- ✓ **Менеджмент рисков ИБ – основа деятельности по обеспечению ИБ**

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?

4.3.Современный подход к обеспечению ИБ

Основные идеи новой концептуальной схемы обеспечения ИБ:

- ✓ **Менеджмент рисков ИБ – основа деятельности по обеспечению 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?

4.3.Современный подход к обеспечению ИБ

Основные идеи новой концептуальной схемы обеспечения ИБ:

- ✓ **Деятельности организации сопутствует значительное число различных рисков – риски ИБ один из видов рисков.**
- ✓ **Менеджмент рисков ИБ – основа деятельности по обеспечению ИБ**

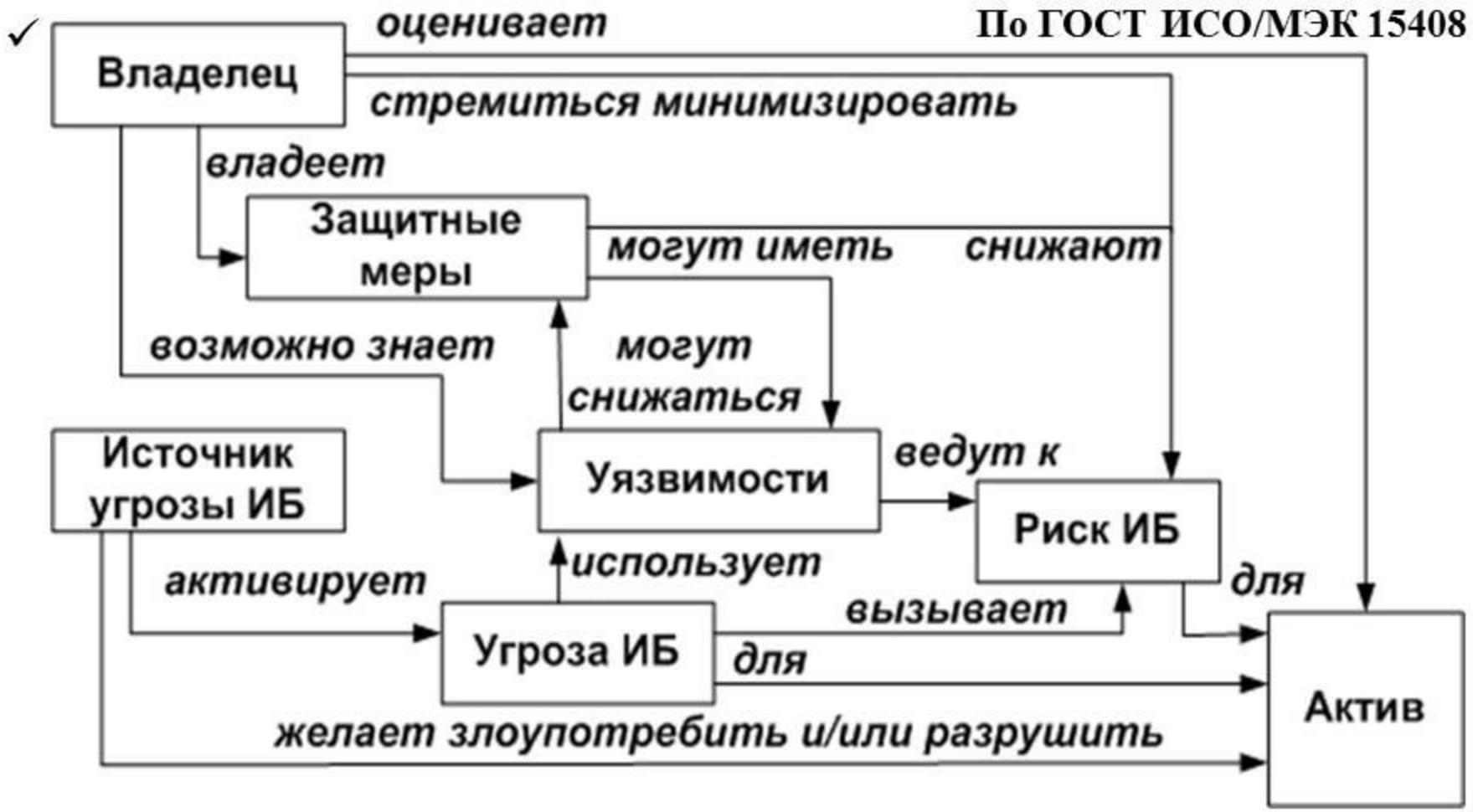
Фундаментальные особенности безопасности:

4) При любом вмешательстве в объект в первую очередь страдает ее безопасность

Следствие 3: при добавлении средства защиты безопасность объекта может не улучшиться, а ухудшится.

4.3.Современный подход к обеспечению ИБ

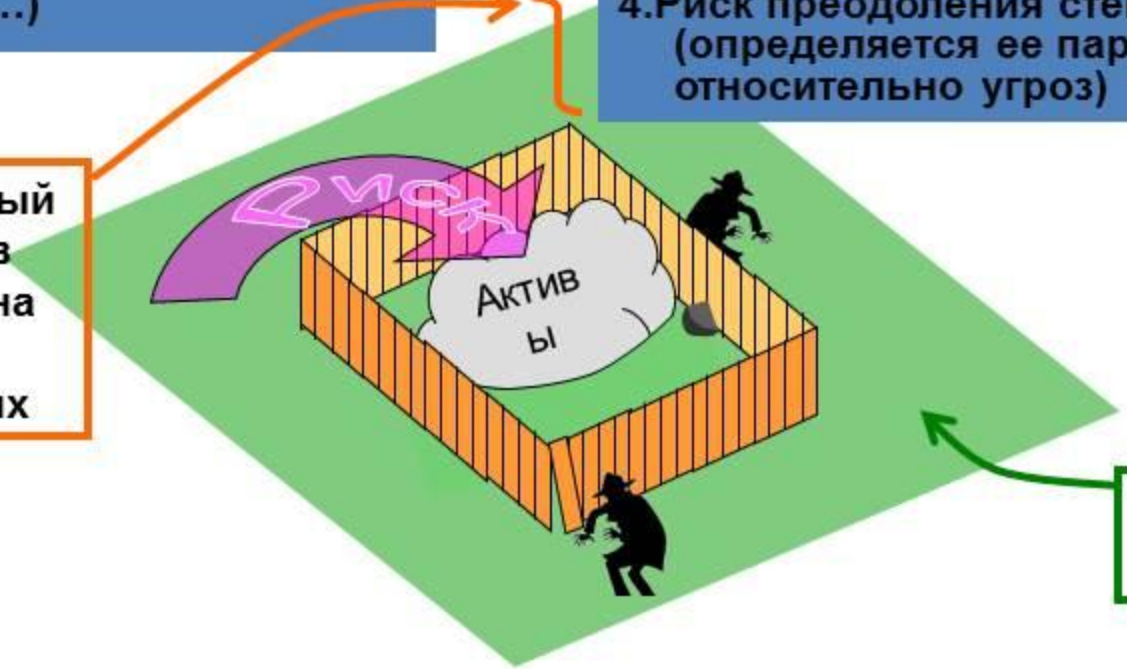
Основные идеи новой концептуальной схемы обеспечения ИБ:



1. Регламентные работы по стене (покраска, проф. ремонт, …)
2. Безопасность стены (мониторинг состояния стены, периодический контроль злоумышленной активности, …)
3. Оценка параметров (толщина, высота, …) стены с точки зрения злоумышленной активности (оснащенность злоумышленника, его мотивация, …)

1.Риск несоблюдения регламента работ по стене (ухудшение характеристик)
2. Риск необнаружения и несвоевременной обработки инцидентов безопасности (дыры и лазейки в стене и их устранение)
3.Риск неверной (несвоевременной) оценки необходимых параметров стены
4.Риск преодоления стены (определяется ее параметрами относительно угроз)

Первоначальный риск активов распадается на четыре составляющих



Агрессивная среда (угрозы)

4.3.Современный подход к обеспечению ИБ

Основные идеи новой концептуальной схемы обеспечения ИБ:

- ✓ Эффективность обеспечения ИБ определяется эффективностью управления
- ✓ Основной целью деятельности службы ИБ организации является содействие бизнесу – целям деятельности организации.
- ✓ Активы могут рассматриваться только в контексте целей деятельности организации, но не как иначе.
- ✓ Деятельности организации сопутствует значительное число различных рисков – риски ИБ один из видов рисков.
- ✓ Менеджмент рисков ИБ – основа деятельности по обеспечению ИБ.
- ✓ **Управление инцидентами ИБ является элементом управления ИБ:**

Фундаментальные особенности безопасности:

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

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 4: событие нарушения безопасности объекта неизбежно!

4.3.Современный подход к обеспечению ИБ

Основные идеи новой концептуальной схемы обеспечения ИБ:

- ✓ **Управление инцидентами ИБ является элементом управления ИБ:**

Фундаментальные особенности безопасности:

1) Безопасность никогда не бывает абсолютной – всегда есть некоторый риск ее нарушения
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 4: событие нарушения безопасности объекта неизбежно!

«Событие нарушения безопасности объекта» - идентифицированное появление определенного состояния объекта, указывающего на возможное нарушение его безопасности или нарушения в работе средств защиты, либо возникновение ранее неизвестной ситуации, которая может иметь отношение к безопасности.

«Инцидент» - ситуация, которая может произойти и привести к нарушению деятельности организации, разрушениям, потерям, чрезвычайной ситуации или кризису в бизнесе.

«Инцидент безопасности» - событие, которое может негативно повлиять на безопасность объекта

4.3.Современный подход к обеспечению ИБ

Основные идеи новой концептуальной схемы обеспечения ИБ:

- ✓ **Управление инцидентами ИБ является элементом управления ИБ:**

Определения:

«Инцидент ИБ» - появление одного или нескольких нежелательных или неожиданных событий ИБ, имеющих значительную вероятность компрометации бизнес-операций и указывающих на свершившуюся, предпринимаемую или вероятную реализацию угрозы ИБ для активов организации ;

«Событие ИБ» - идентифицированное появление определенного состояния актива организации (системы, сервиса или сети), указывающего на возможное нарушение Политики ИБ или нарушения в работе средств защиты, либо возникновение ранее неизвестной ситуации, которая может иметь отношение к ИБ.

4.3.Современный подход к обеспечению ИБ

Основные идеи новой концептуальной схемы обеспечения ИБ:

- ✓ **Управление инцидентами ИБ является элементом управления ИБ:**

Определения:

Управление инцидентами ИБ - это процесс, состоящий из ряда подпроцессов, на вход которого поступают данные, полученные в результате сбора и протоколирования событий ИБ, а на выходе – информация о причинах произошедшего инцидента ИБ, нанесенном организации ущербе и мерах, которые необходимо принять для того, чтобы инцидент ИБ не повторился вновь.

4.3.Современный подход к обеспечению ИБ

Основные идеи новой концептуальной схемы обеспечения ИБ:

✓ **Управление инцидентами ИБ является элементом управления ИБ:**

Цель управления инцидентами ИБ – **обеспечение следующих условий :**

✓ **события ИБ обнаружены и эффективно обработаны, в частности, определены как относящиеся или не относящиеся к категории инцидентов ИБ;**

✓ **идентифицированные инциденты ИБ оценены, и реагирование на них осуществлено наиболее целесообразным и результативным способом;**

✓ **негативные воздействия инцидентов ИБ на организацию и ее бизнес-операции минимизированы соответствующими защитными мерами, являющимися частью процесса реагирования на инцидент, иногда наряду с применением соответствующих элементов из плана(ов) ОНБ;**

✓ **из инцидентов ИБ и их управления быстро извлечены уроки. Это делается с целью повышения шансов предотвращения инцидентов ИБ в будущем, улучшения внедрения и использования защитных мер, улучшения общей системы управления инцидентами ИБ.**

4.3.Современный подход к обеспечению ИБ

Основные идеи новой концептуальной схемы обеспечения ИБ:

- ✓ **Управление инцидентами ИБ является элементом управления ИБ:**

Определение:

Система управления инцидентами ИБ (СУИИБ) –

часть общей системы управления организации, предназначенная для:

обнаружения и регистрации, оценки, классификации и приоритезации, всестороннего исследования, обработки, извлечения уроков и предотвращения инцидентов ИБ в дальнейшем

и включающая организационную структуру, политику, планирование действий, обязанности, установившийся порядок, процедуры, процессы и ресурсы в области реагирования на инциденты ИБ.

Назначение СУИИБ

Структура СУИИБ

4.3.Современный подход к обеспечению ИБ

Основные идеи новой концептуальной схемы обеспечения ИБ:

- ✓ **Эффективность обеспечения ИБ определяется эффективностью управления**
- ✓ **Основной целью деятельности службы ИБ организации является содействие бизнесу – целям деятельности организации.**
- ✓ **Активы могут рассматриваться только в контексте целей деятельности организации, но не как иначе.**
- ✓ **Деятельности организации сопутствует значительное число различных рисков – риски ИБ один из видов рисков.**
- ✓ **Менеджмент рисков ИБ – основа деятельности по обеспечению ИБ.**
- ✓ **Управление инцидентами ИБ является элементом управления ИБ:**
- ✓ **Контроль обеспечения ИБ является элементом управления ИБ:**

4.3.Современный подход к обеспечению ИБ

Основные идеи новой концептуальной схемы обеспечения ИБ:

- ✓ **Контроль обеспечения ИБ является элементом управления ИБ:**

Почему?

Актуальные вопросы, возникающие на объекте, функционирующем в условиях существования угроз в информационной сфере:

- ***Имеются ли в текущей конфигурации систем уязвимости, которые могут быть использованы для несанкционированного доступа (НСД) и взлома системы?***
- ***Насколько адекватны существующим рискам ИБ реализованные защитные меры?***
- ***Какие контрмеры позволят реально повысить существующий уровень защиты?***
- ***Как оценить уровень защищенности объекта и как определить, является ли он достаточным в данной среде функционирования?***
- ***На какие критерии оценки защищенности следует ориентироваться, и какие показатели защищенности использовать?***

Ответы: **в области проверки и оценки деятельности по обеспечению ИБ**

4.3.Современный подход к обеспечению ИБ

Основные идеи новой концептуальной схемы обеспечения ИБ:

- ✓ **Контроль обеспечения ИБ является элементом управления ИБ:**

Почему?

Любые защитные меры в силу ряда объективных причин со временем имеют тенденцию к ослаблению своей эффективности, в результате чего общий уровень ИБ может снижаться. Это неминуемо ведет к возрастанию рисков нарушения ИБ.

Для того, чтобы это не допустить, необходимо:

- ***определить процессы, обеспечивающие контроль (мониторинг и аудит ИБ);***
- ***оценить эффективность обеспечения ИБ, используя «процессный подход»***

Это: основа дальнейшего планирования обеспечения ИБ

4.3.Современный подход к обеспечению ИБ

Основные идеи новой концептуальной схемы обеспечения ИБ:

✓ **Контроль обеспечения ИБ является элементом управления ИБ:**

Для того, чтобы это не допустить, необходимо:

определить процессы, обеспечивающие контроль (мониторинг и аудит ИБ);

оценить эффективность обеспечения ИБ, используя «процессный подход»

Определения:

«мониторинг»: постоянное наблюдение за объектами и субъектами, влияющими на обеспечение ИБ, а также сбор, анализ и обобщение результатов наблюдений;

«аудит»: периодический, независимый и документированный процесс получения свидетельств аудита и объективной их оценки с целью установления степени выполнения установленных требований по обеспечению ИБ (может быть внутренний или внешний аудит);

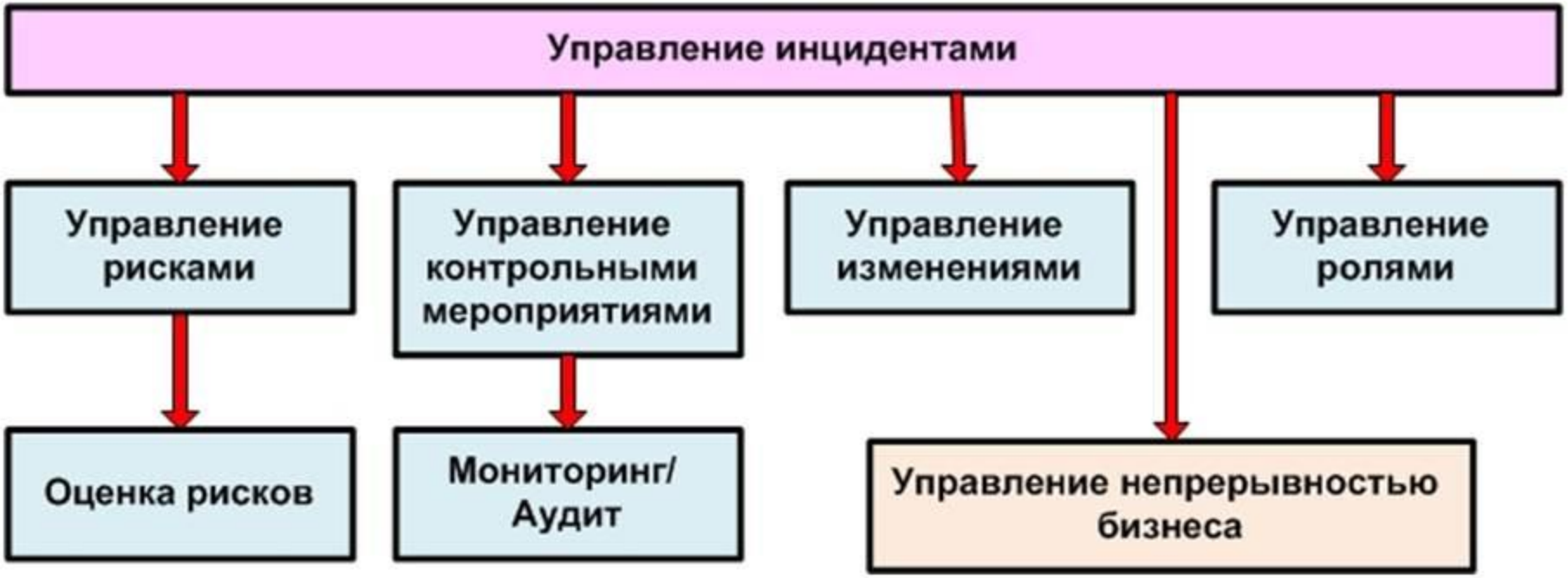
***«процессный подход»:* деятельность по обеспечению ИБ в виде системы процессов в пределах организации;**

***«процесс»:* любое действие, использующее ресурсы и управляемое для обеспечения преобразования неких входных ресурсов в выходные ресурсы.**

4.3.Современный подход к обеспечению ИБ

Основные идеи новой концептуальной схемы обеспечения ИБ:

- ✓ **Управление инцидентами ИБ является элементом управления ИБ.**
- ✓ **Контроль обеспечения ИБ является элементом управления ИБ.**



4.3.Современный подход к обеспечению ИБ

Основные идеи новой концептуальной схемы обеспечения ИБ:

- ✓ *Эффективность обеспечения ИБ определяется эффективностью управления*
- ✓ *Основной целью деятельности службы ИБ организации является содействие бизнесу – целям деятельности организации.*
- ✓ *Активы могут рассматриваться только в контексте целей деятельности организации, но не как иначе.*
- ✓ *Деятельности организации сопутствует значительное число различных рисков – риски ИБ один из видов рисков.*
- ✓ *Менеджмент рисков ИБ – основа деятельности по обеспечению ИБ.*
- ✓ *Управление инцидентами ИБ является элементом управления ИБ.*
- ✓ *Контроль обеспечения ИБ является элементом управления ИБ*
- ✓ *Взаимодействие с управлением непрерывностью бизнеса*

4.3.Современный подход к обеспечению ИБ

Основные идеи новой концептуальной схемы обеспечения ИБ:

Почему «обеспечение НБ»?

Современные проблемы нарушения или прерывания деятельности организации:

- сбои энергетики,
- сбои поставок,
- сбои функционирования информационных и телекоммуникационных систем,
- нарушения информационной безопасности,
- уход ключевого персонала,
- преднамеренные действия персонала,
- ошибки персонала,
- пожары, наводнения, техногенные катастрофы и т. д.

Ключевая задача, стоящая перед руководством любой организации: непрерывное функционирования всех видов деятельности

4.3.Современный подход к обеспечению ИБ

Основные идеи новой концептуальной схемы обеспечения ИБ:

Почему «обеспечение НБ»?

В ряде высокотехнологичных отраслей, таких как, например, телекоммуникации, непрерывность деятельности является не просто потребностью бизнеса, но и требованием законодательства.

Временное непредоставление услуг вне зависимости от причин, вызвавших этот перерыв, может привести к отзыву лицензии и, следовательно, полному прекращению деятельности.

4.3.Современный подход к обеспечению ИБ

Основные идеи новой концептуальной схемы обеспечения ИБ:

Почему «обеспечение НБ»?

Перед каждой организацией рано или поздно встают следующие вопросы:

- ***насколько применим и критичен для нее тот или иной риск прерывания бизнеса;***
- ***как избежать данного риска или минимизировать его негативные последствия;***
- ***что нужно сделать заранее;***
- ***как найти «золотую середину» между приемлемыми инвестициями в превентивные меры (по предотвращению прерываний и минимизации их последствий) и возможными потерями.***

Ответ: внедрение процессов управления обеспечением НБ (УНБ)

УНБ - важный элемент надлежащего управления всей деятельностью организации, предоставления ее услуг и производства продукции, а также предпринимательской дальновидности и конкурентоспособности.

4.3.Современный подход к обеспечению ИБ

Основные идеи новой концептуальной схемы обеспечения ИБ:

Почему «обеспечение НБ»?

Перед каждой организацией рано или поздно встают следующие вопросы:

- *насколько применим и критичен для нее тот или иной риск прерывания бизнеса;*
- *как избежать данного риска или минимизировать его негативные последствия;*
- *что нужно сделать заранее;*
- *как найти «золотую середину» между приемлемыми инвестициями в превентивные меры (по предотвращению прерываний и минимизации их последствий) и возможными потерями.*

Ответ: внедрение процессов управления обеспечением НБ (УНБ)

УНБ - важный элемент надлежащего управления всей деятельностью организации, предоставления ее услуг и производства продукции, а также предпринимательской дальновидности и конкурентоспособности.

4.3.Современный подход к обеспечению ИБ

Основные идеи новой концептуальной схемы обеспечения ИБ:

Почему «обеспечение НБ»?

Тактика УНБ:

- *анализ рисков ИБ, связанных с чрезвычайными ситуациями (ЧС);*
- *установление критерии оценки возможности перерастания инцидента ИБ в ЧС и планирование действий в данном случае;*
- *определение сценариев реализации ЧС, связанные с ИБ, для которых будут разработаны соответствующие планы;*
- *выбор стратегии ОИБ в процессе ЧС;*
- *разработка, тестирование и обновление плана обеспечения непрерывности функционирования процессов ОИБ и соответствующих защитных мер и средств (или включение соответствующих разделов в уже имеющиеся планы в организации);*
- *разработка, тестирование и обновление плана восстановления работы защитных мер после ЧС (или включение соответствующих разделов в уже имеющиеся планы в организации).*

4.3.Современный подход к обеспечению ИБ

Основные идеи новой концептуальной схемы обеспечения ИБ:

Почему «обеспечение НБ»?

Перед каждой организацией рано или поздно встают следующие вопросы:

- ***насколько применим и критичен для нее тот или иной риск прерывания бизнеса;***
- ***как избежать данного риска или минимизировать его негативные последствия;***
- ***что нужно сделать заранее;***
- ***как найти «золотую середину» между приемлемыми инвестициями в превентивные меры (по предотвращению прерываний и минимизации их последствий) и возможными потерями.***

Ответ: внедрение процессов управления обеспечением НБ (УНБ)

УНБ - важный элемент надлежащего управления всей деятельностью организации, предоставления ее услуг и производства продукции, а также предпринимательской дальновидности и конкурентоспособности.

4.1. Исходная концептуальная схема (парадигма) обеспечения ИБ

5. Концептуальные подходы к обеспечению НБ

Почему «обеспечение НБ»?

Современный подход: *новая парадигма*

Основные идеи парадигмы (модели) обеспечения ИБ:

«флаги» новой парадигмы:

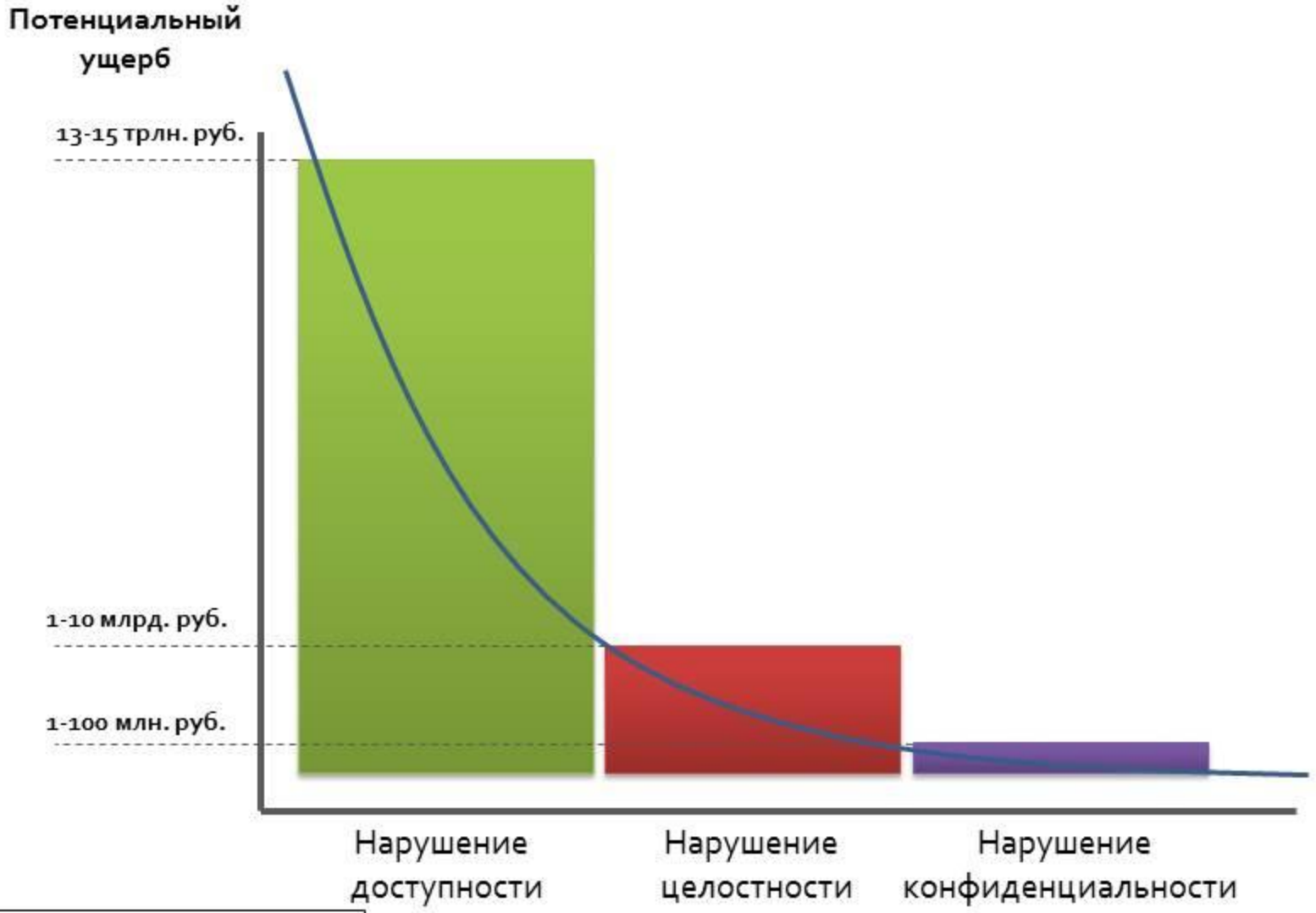
Главный «флаг»: Управление информационной безопасности

Составляющие «флага»:

1. *Управление рисками ИБ.*
2. *Управление инцидентами ИБ.*
3. *Проверка и оценка деятельности по управлению ИБ*
4. *Взаимодействие с управлением непрерывностью бизнеса*

Перечень основных рисков ИТС Банка России

Соотношение рисков ИТС Банка России



Сенаторов М.Ю. (13.09.2012)

4.4.Система управления ИБ

Основные идеи новой концептуальной схемы обеспечения ИБ:

- ✓ Эффективность обеспечения ИБ определяется эффективностью управления
- ✓ Основной целью деятельности службы ИБ организации является содействие бизнесу – целям деятельности организации.
- ✓ Активы могут рассматриваться только в контексте целей деятельности организации, но не как иначе.
- ✓ Деятельности организации сопутствует значительное число различных рисков – риски ИБ один из видов рисков.
- ✓ Менеджмент рисков ИБ – основа деятельности по обеспечению ИБ.
- ✓ Управление инцидентами ИБ является элементом управления ИБ.
- ✓ Контроль обеспечения ИБ является элементом управления ИБ.
- ✓ Взаимодействие с управлением непрерывностью бизнеса

4.4.Система управления ИБ

Основные идеи новой концептуальной схемы обеспечения ИБ:

- ✓ Эффективность обеспечения ИБ определяется эффективностью управления
- ✓ Основной целью деятельности службы ИБ организации является содействие бизнесу – целям деятельности организации.
- ✓ Активы могут рассматриваться только в контексте целей деятельности организации, но не как иначе.
- ✓ Деятельности организации сопутствует значительное число различных рисков – риски ИБ один из видов рисков.
- ✓ Менеджмент рисков ИБ – основа деятельности по обеспечению ИБ.
- ✓ Управление инцидентами ИБ является элементом управления ИБ.
- ✓ Контроль обеспечения ИБ является элементом управления ИБ.
- ✓ Взаимодействие с управлением непрерывностью бизнеса

Основные процессы УИБ:

1. *Управление рисками ИБ.*
2. *Управление инцидентами ИБ.*
3. *Проверка и оценка деятельности по управлению ИБ*
4. *Взаимодействие с управлением непрерывностью бизнеса*

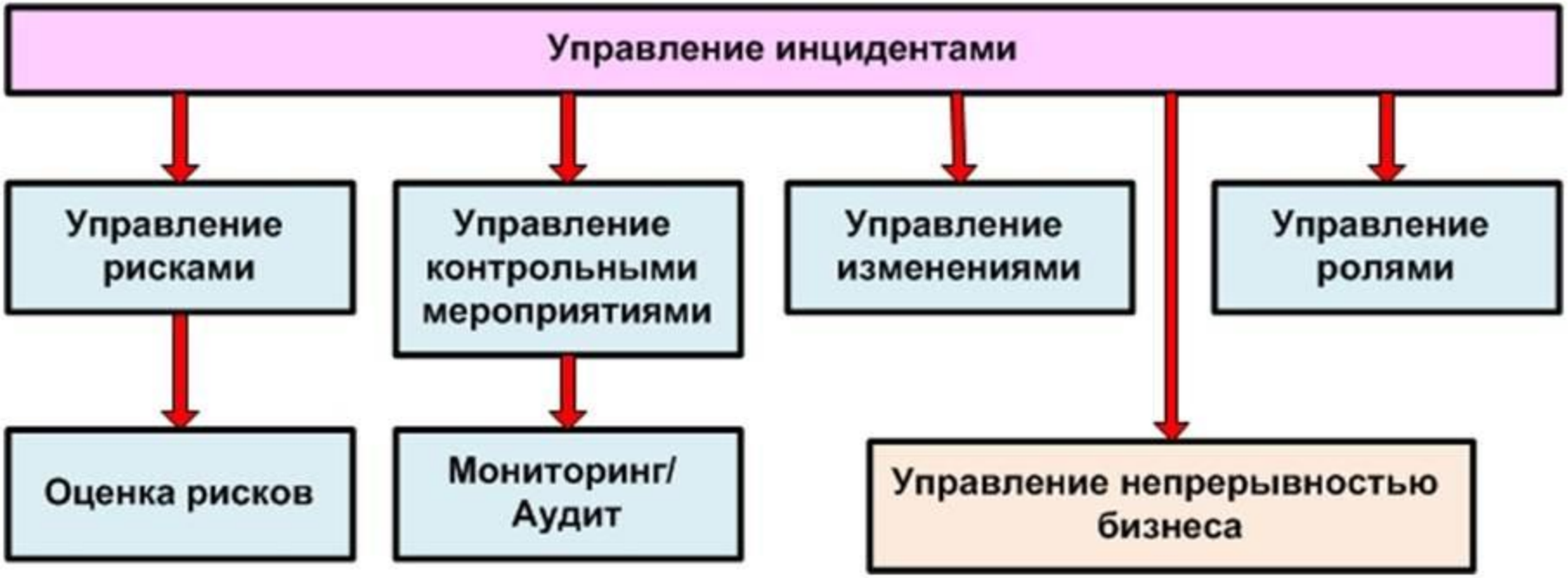
4.4.Система управления ИБ

Работа с процессами СУИБ: ***Основные процессы СУИБ***

4.3.Современный подход к обеспечению ИБ

Основные идеи новой концептуальной схемы обеспечения ИБ:

- ✓ **Управление инцидентами ИБ является элементом управления ИБ.**
- ✓ **Контроль обеспечения ИБ является элементом управления ИБ.**



4.4.Система управления ИБ

Обеспечение ИБ – это системный процесс, а не состояние.

Процессом надо управлять!

«управление» *- осуществление совокупности непрерывных взаимосвязанных воздействий на объект (управляемую систему), выбранных из множества возможных воздействий на основании информации о поведении объекта и состоянии внешней среды для достижения заданной цели;*

Пояснения

- ***Control*** *– исторически первый из применяемых в информационных технологиях (ИТ) терминов, отражающий самые простейшие операции в области управления, в большей степени с точки зрения технического аспекта деятельности.*
- ***Management*** *– термин, который первоначально употреблялся в отношении управления человеческими ресурсами; в настоящее время встречается в сочетании с множеством понятий из области ИТ и имеет смысл организации и регулирования какой-либо деятельности, т. е. ее администрирования.*
- ***Governance*** *– термин, который стал активно использоваться применительно к ИТ только в последнем десятилетии; под ним обычно понимается руководство по организации и контролю за какой-либо деятельностью. Это слово переводится на русский как «власть, руководство, управление».*

4.4.Система управления ИБ

Обеспечение ИБ – это системный процесс, а не состояние.

Процессом надо управлять!

«управление» *- осуществление совокупности непрерывных взаимосвязанных воздействий на объект (управляемую систему), выбранных из множества возможных воздействий на основании информации о поведении объекта и состоянии внешней среды для достижения заданной цели;*

«менеджмент» *- скоординированная деятельность по руководству и управлению организацией* [ГОСТ Р ИСО 9000-2001].

Выводы:

1.Иногда делают вывод, что понятие менеджмента шире, чем просто управление.

2.Для ИБ более подходит термин «менеджмент ИБ»

4.4.Система управления ИБ

Обеспечение ИБ – это системный процесс, а не состояние.

Процессом надо управлять!

Определения:

«процесс» *– это совокупность взаимосвязанных или взаимодействующих видов деятельности, преобразующая входы в выходы и требующая для этого определенных ресурсов и управляющих воздействий (управления);*

«бизнес процесс» *- множество из одной или нескольких упорядоченных во времени, логически связанных и завершенных видов деятельности, в совокупности поддерживающих деятельность организации и реализующих ее политику, направленную на достижение поставленных целей;*

4.4.Система управления ИБ

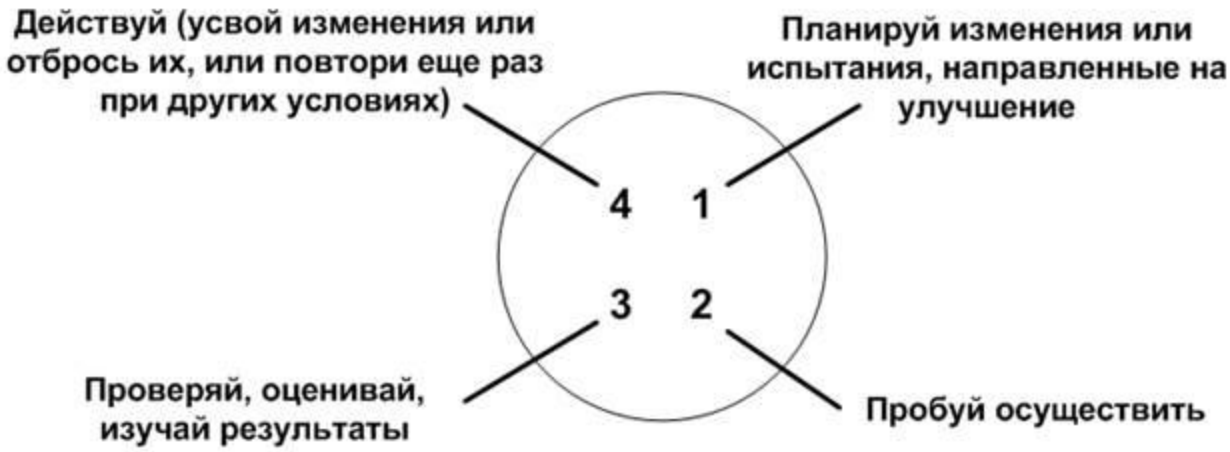
Управление: процессный подход (улучшение процессов)

Процессный подход: *циклическая модель (для структурирования всех процессов управления и для обеспечения учета всех значимых элементов процессного подхода)* ***PDCA (от англ. Plan-Do-Check-Act – планируй – выполняй – проверяй – действуй»)***

Циклическая модель:

Предложена и развита двумя американскими учеными и специалистами в теории управления качеством. Шухарт (Walter A. Shewhart) (1939 г. «Статистические методы с точки зрения управления качеством»)

Пропагандировалась: *Деминг (William Edwards Deming) в качестве основного способа достижения непрерывного улучшения процессов (цикл PDSA).*



4.4.Система управления ИБ

Эталонная модель Деминга (-Шухарта) – Цикл Деминга

PDCA – «планируй – сделай – проверь – действуй»

ISO/TC 176/SC 2/N 544R2, ISO 9000 Introduction and Support Package: Guidance on Concept and Use of the Process Approach for management systems, 13 may 2004»

4.4. Система управления 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 совершенствования функционирования процесса.

4.4.Система управления ИБ

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

ШИРОКОЕ применение («волшебный цикл»):

Национальные стандарты: ГОСТ Р ИСО/МЭК 27001-2012;
ГОСТ Р ИСО 90000 (качество);
ГОСТ Р ИСО 14000 (экология).
Отраслевые стандарты: СБР ИББС-1.0-2010 (Банк России);
автомобилестроение;
поставка и безопасность продуктов питания
Направления деятельности: безопасность (экономическая, физическая, информационная и пр.)

В основе практики реализации модели Деминга лежит процессный подход

4.4.Система управления ИБ

Управление ИБ – Управление обеспечением ИБ

Управление ИБ:

совокупность целенаправленных действий, осуществляемых для обеспечения нормального функционирования основных процессов и, в конечном счете, достижения бизнес целей организации посредством обеспечения защищенности ее информационной сферы.

Определение:

«информационная сфера» - представляет собой совокупность информации, информационной инфраструктуры (состоит из баз данных и знаний, систем связи и т. п.), субъектов, осуществляющих сбор, формирование, распространение, хранение и использование информации, а также системы регулирования возникающих при этом отношений.

4.4.Система управления ИБ

Управление ИБ – Управление обеспечением ИБ

Различают:
Управление ИБ организации ***Управление ИБ технологии (ИТТ)***

Определение:
«Управление ИБ организации» ***- управление ИБ организации как циклический процесс, состоящий из совокупности целенаправленных действий, осуществляемых для достижения заявленных бизнес целей организации посредством обеспечения защищенности ее информационной сферы, и включающий :***

- ***осознание необходимости ОИБ,***
- ***постановку задачи по ОИБ,***
- ***оценку текущей ситуации и состояния объекта управления,***
- ***планирование мер по обработке рисков ИБ,***
- ***реализацию, внедрение и оценку эффективности соответствующих защитных мероприятий и средств управления,***
- ***распределение ролей и ответственности в области ОИБ,***
- ***обучение и мотивацию сотрудников, выбор управляющих и корректирующих воздействий и их реализацию.***

4.4.Система управления ИБ

Управление ИБ организации

Управление (обеспечением) ИБ организации

– *это не разовое мероприятие. Его следует рассматривать как непрерывную деятельность по постоянному поддержанию требуемого организацией уровня ИБ, так как правильно управляемая ИБ – инструмент успешного ведения бизнеса.*

Основным предметом управления ИБ в организации являются следующие области деятельности:

- *планирование работ по ОИБ, включая разработку и продвижение соответствующей документации;*
- *поддержка и участие в эксплуатации защитных мер;*
- *осуществление контроля за ОИБ и уровнем ИБ;*
- *совершенствование работ по ОИБ на основе собственного опыта и лучших практик.*

4.4. Система управления ИБ

Управление ИБ организации

В целом процесс управления ИБ организации, носящий циклический характер, заключается в следующем:

- *описание объектов управления и защищаемых активов организации и сбор данных об их состоянии;*
- *выявление и формализация возможных угроз ИБ и анализ рисков ИБ;*
- *оценка защищенности объектов управления (с выявлением уязвимостей) и ее сравнение с требованиями по ОИБ организации, сформулированными в Политике ИБ организации (ПолИБ);*
- *формирование управляющих воздействий;*
- *оценка результирующей деятельности по управлению ИБ.*

Определение:

«Политика 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.*

4.2.Концептуальные подходы к управлению ИБ

✓ ***Политика ИБ:*** **Разработка и реализация политики 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?

4.4. Система управления ИБ

Управление ИБ организации

Цель управления ИБ в организации:

заключается в гарантировании того, что соответствующие мероприятия по обеспечению ИБ осуществляются таким образом, что в текущий момент надлежащим образом:

1) снижены риски ИБ;

2) осуществляются инвестиции в обеспечение ИБ;

3) руководство ознакомлено со всеми осуществляемыми мероприятиями;

4) верно сформулированы критерии оценки эффективности обеспечения ИБ.

4.4.Система управления ИБ

Управление ИБ организации - **Уровни управления ИБ организации:**

Уровни управления ИБ	*Назначение*	*Основные задачи*
Стратегическое управление ИБ	Обеспечение интересов организации в области ИБ	Определение стратегии и разработка концепции ИБ. Основные направления ОИБ. Нормативно-правовое ОИБ.
Тактическое управление ИБ	Формирование и контроль выполнения ПолИБ	Планирование и обеспечение выполнения ПолИБ. Разработка положений, регламентов, правил, инструкций. Проведение расследований и анализ инцидентов ИБ.
Оперативное управление ИБ	Реализация выполнения требований ПолИБ	Определение механизмов и способов ОИБ. Реализация защитных функций и процедур. Эксплуатация средств защиты и контроля.

4.4.Система управления ИБ

Система управления ИБ

Управление ИБ в организации включает в себя две важнейшие составляющие:

- *собственно сам процесс управления ИБ объекта;*
- *систему управления ИБ (СУИБ) объекта.*

Определение:

«Система управления ИБ объекта - часть общей системы управления объекта, основанная на подходе оценки и анализа рисков, предназначена для разработки, внедрения, эксплуатации, постоянного контроля, анализа, поддержания и улучшения системы обеспечения ИБ (СОИБ), и включающая организационную структуру, политику, планирование действий, обязанности, установившийся порядок, процедуры, процессы и ресурсы в области ИБ

4.4.Система управления ИБ

Система управления ИБ

Определение:

«**Система управления ИБ объекта** - часть общей системы управления объекта, основанная на подходе оценки и анализа рисков, предназначена (назначение СУИБ) для разработки, внедрения, эксплуатации, постоянного контроля, анализа, поддержания и улучшения системы обеспечения ИБ (СОИБ), и включающая (структура СУИБ) организационную структуру, политику, планирование действий, обязанности, установившийся порядок, процедуры, процессы и ресурсы в области ИБ

4.4.Система управления ИБ

СУИБ: выполняет следующие функции:

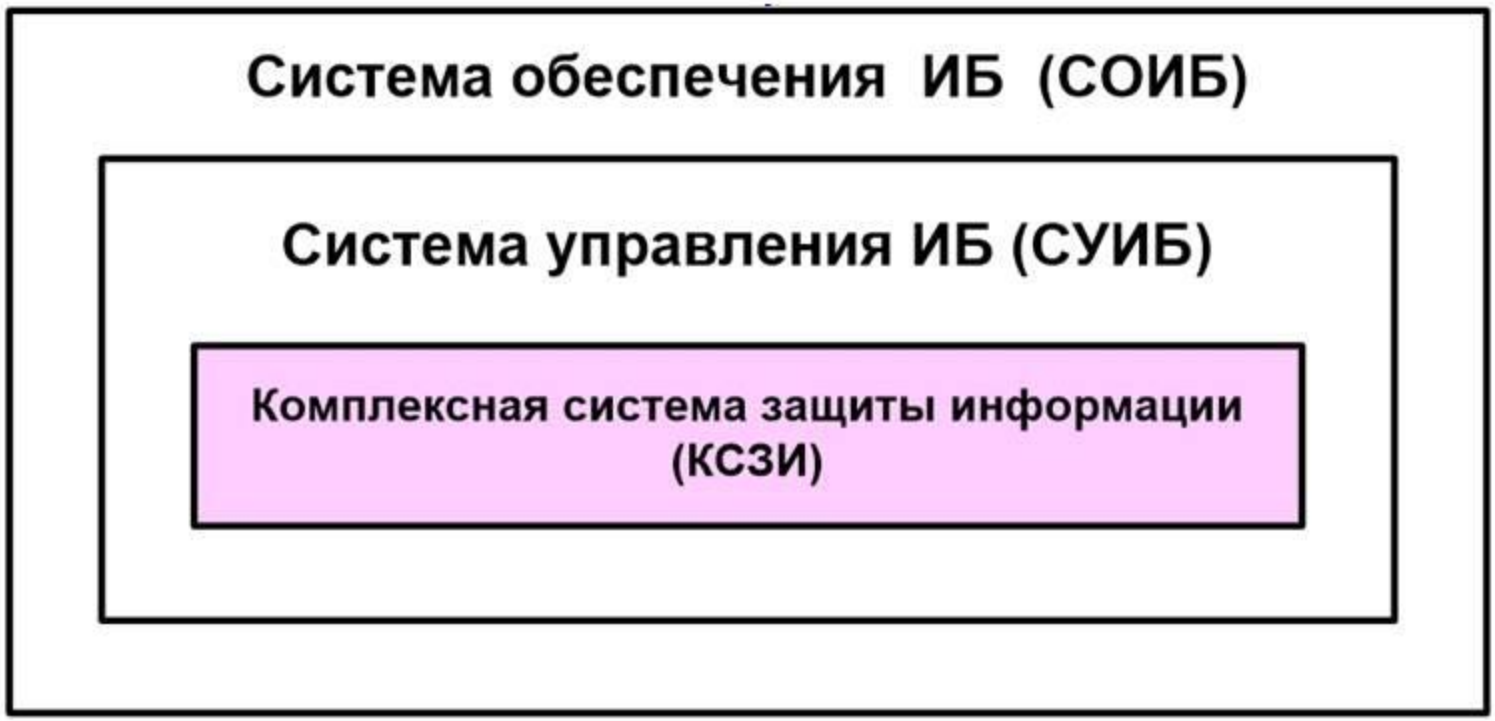
- реализует целенаправленный, систематический и комплексный подход к управлению ИБ защищаемых активов, что приводит к повышению текущего уровня их защищенности;
- объединяет все применяемые в организации защитные и организационные меры в (КСЗИ), позволяющий достигать цели обеспечения ИБ на уровне всей организации;
- позволяет четко установить, как взаимосвязаны процессы и подсистемы обеспечения ИБ (КСЗИ), кто за них отвечает, какие финансовые и трудовые ресурсы необходимы для их эффективного функционирования и т. д.;
- проводит процесс выполнения ПолИБ и позволяет находить и устранять слабые места в обеспечении ИБ;
- охватывает людей, процессы и ИТ-структуру организации.

4.4.Система управления ИБ

Система обеспечения ИБ (СОИБ) =

Система управления ИБ (СУИБ) +

+ Комплексная система защиты информации (КСЗИ)



СОИБ = СУИБ + КСЗИ

4.4.Система управления ИБ

СУИБ - Выгоды от использования СУИБ (начало):

- обеспечение соответствия уровня ИБ законодательным, отраслевым, контрактным, внутрикорпоративным требованиям и целям бизнеса;
- доказательство стремления высшего руководства к ОИБ в необходимом объеме для всей организации в соответствии с установленными требованиями;
- повышение доверия партнеров, клиентов, заказчиков за счет демонстрации высокого уровня ОИБ всем заинтересованным сторонам;
- управляемое ОИБ и контролируемое управление ИБ (особенно в критичных ситуациях);
- систематизация процессов ОИБ;
- расстановка приоритетов в области обеспечения ИБ;
- достижение «прозрачности» в ОИБ;
- обеспечение понятности защищаемых активов для руководства;

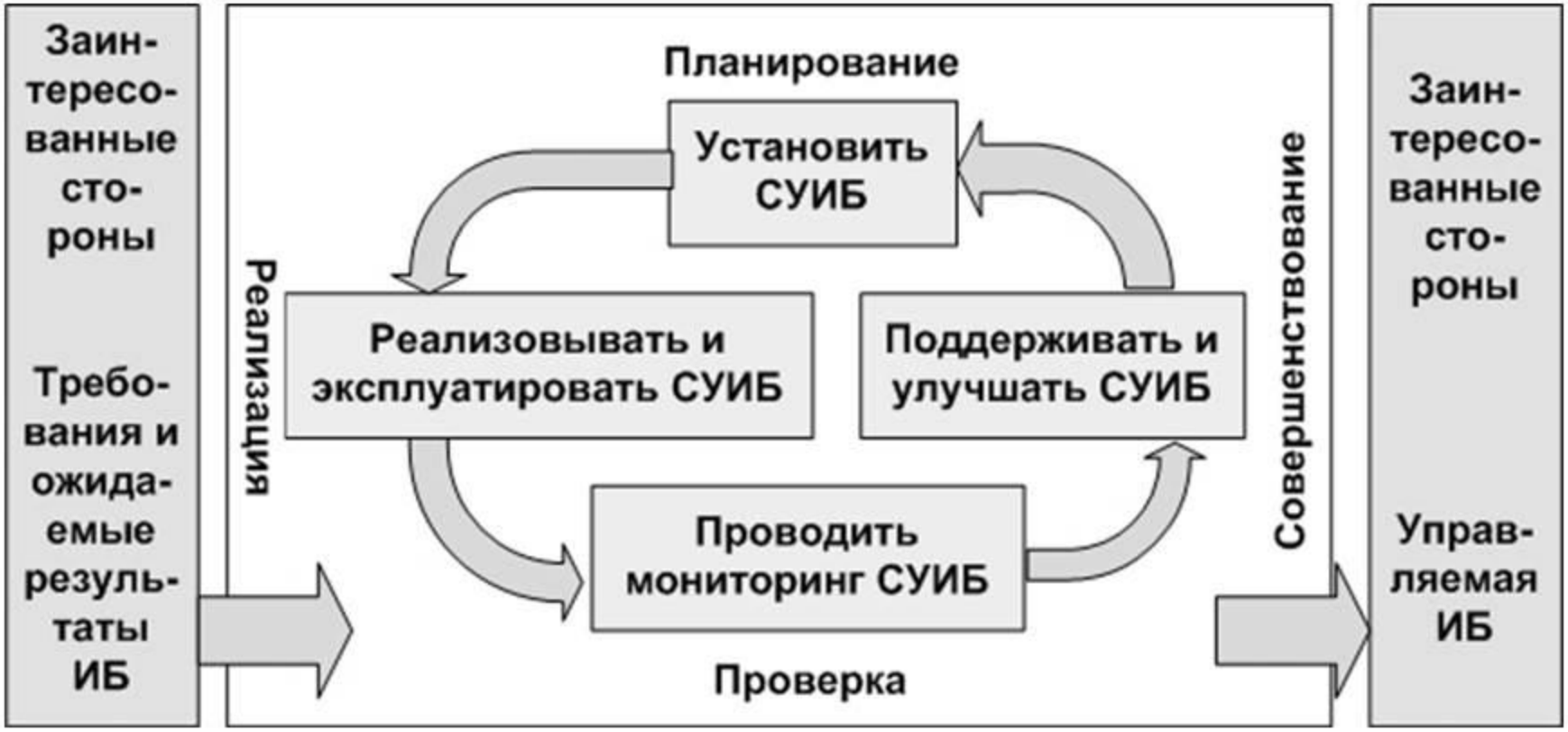
4.4.Система управления ИБ

СУИБ - Выгоды от использования СУИБ (окончание):

- выявление угроз ИБ для бизнес-процессов;
- достижение адекватности ОИБ существующим рискам;
- предупреждение возникновения инцидентов ИБ и снижение ущерба в случае их возникновения;
- повышение культуры ИБ в организации;
- интеграция защитных мер в бизнес-процессы;
- оптимизация (за счет формализации всех процессов ОИБ) и обоснование расходов на ИБ;
- снижение финансовых рисков и рисков прямых потерь;
- снижение рисков для инвесторов за счет повышения прозрачности процессов внутри организации;
- экономия времени, ресурсов и затрат на начальной стадии сбора информации при проведении любых аудитов ИБ;
- создание информации, порождаемой в процессе использования СУИБ, для всех заинтересованных сторон и т. д.

4.4.Система управления ИБ

Методологическая основа СУИБ: процессный подход в рамках управления ИБ: *1.Планирование СУИБ; 2.Реализация СУИБ; 3.Проверка СУИБ; 4.Совершенствование СУИБ*



4.4.Система управления ИБ

Методологическая основа СУИБ: процессный подход в рамках управления ИБ: 1.Планирование СУИБ; 2.Реализация СУИБ; 3.Проверка СУИБ; 4.Совершенствование СУИБ

4.4.Система управления ИБ

Управление обеспечением ИБ ИТТ организации

Процесс управления ИБ ИТТ :

- *интегрируется в общий процесс управления ИТТ;*
- *основывается на определенных принципах (например, изложенных в ГОСТ Р ИСО/МЭК 13335–1);*
- *имеет определенные этапы, например (ГОСТ Р ИСО/МЭК ТО 13335-3):*
  - *анализ требований по ОИБ ИТТ;*
  - *разработка плана выполнения этих требований;*
  - *реализация положений выработанного плана;*
  - *управление и административный контроль над процессом управления ИБ ИТТ.*

Благодарю за внимание!

Толстой Александр Иванович

AlTolstoj@mephi.ru