Учебная дисциплина «Управление информационной безопасностью»

Тема 1

Концептуальные основы обеспечения ИБ

Толстой Александр Иванович

к.т.н., доцент

Доцент кафедры «Информационная безопасность банковских систем»

НИЯУ МИФИ,

Факультет «Кибернетика и информационная безопасность», кафедра

Москва, 2016

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Эволюция понятия (с 1970г.)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Эволюция понятия (с 1970г.)

«безопасность данных» (англ. data security),
«компьютерная безопасность» (computer security),
«безопасность информации» или «информационная безопасность» (information security),
«безопасность ИТ» (IT security),
«сетевая безопасность» (network security),
«безопасность систем» (systems security),
«защита информации» (information protection)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Эволюция понятия (с 1970г.)

«безопасность данных» (англ. data security),
«компьютерная безопасность» (computer security),
«безопасность информации» или «информационная безопасность» (information security),
«безопасность ИТ» (IT security),
«безопасность систем» (systems security) и
«защита информации» (information protection),
«сетевая безопасность» (network security).

Россия:
«безопасность информации» или «информационная безопасность» (information security),
«защита информации» (information protection).

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

БЕЗОПАСНОСТЬ (Б)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

БЕЗОПАСНОСТЬ (Б)

Б - состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз (Закон РФ от 05.03.1992 № 2446-1 «О безопасности»)

Б – … (Закон РФ от 28.12.2010 № 390-ФЗ)

Б – отсутствие недопустимого риска, связанного с возможностью нанесения ущерба (ГОСТ Р 1.1-2002)

Б (защищаемого объекта - предприятие, организация, учреждение, домовладение и т.п.) - **состояние защищенности объекта от угроз причинения ущерба (вреда) жизни и здоровью людей, имуществу физических и юридических лиц, государственному и муниципальному имуществу, техническому состоянию, инфраструктуре жизнеобеспечения, внешнему виду, интерьеру(ам), ландшафтной архитектуре, окружающей природной среде (ГОСТ Р 53704-2009 «Системы безопасности комплексные и интегрированные. Общие технические требования»).**

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Доктрина информационной безопасности Российской Федерации:

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Доктрина информационной безопасности Российской Федерации:

«Под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства»

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Доктрина информационной безопасности Российской Федерации:

«Под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства»

Интересы личности в информационной сфере:
реализация конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также на защиту информации, обеспечивающей личную безопасность

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Доктрина информационной безопасности Российской Федерации:

«Под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства»

Интересы личности в информационной сфере:
реализация конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также на защиту информации, обеспечивающей личную безопасность

Интересы государства в информационной сфере:
создание условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, безусловное обеспечение законности и правопорядка, развитие равноправного и взаимовыгодного международного сотрудничества

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Чаще всего понимают:

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Чаще всего понимают:

- ***защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры;***
- ***механизм защиты, обеспечивающий конфиденциальность, целостность и доступность информации;***
- ***свойство информации сохранять конфиденциальность, целостность и доступность.***

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Безопасность информации:

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Безопасность информации:

- *состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз*

Руководящий документ Гостехкомиссии России от 30 марта 1992 г. «Защита от несанкционированного доступа к информации. Термины и определения»

- *состояние защищенности информации, при котором обеспечивается ее конфиденциальность, доступность и целостность*

Рекомендациям по стандартизации Р 50.1.053-2005 «Информационные технологии. Основные термины и определения в области технической защиты информации» и ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Безопасность информации:

- *состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз*

Руководящий документ Гостехкомиссии России от 30 марта 1992 г. «Защита от несанкционированного доступа к информации. Термины и определения»

- *состояние защищенности информации, при котором обеспечивается ее конфиденциальность, доступность и целостность*

Рекомендациям по стандартизации Р 50.1.053-2005 «Информационные технологии. Основные термины и определения в области технической защиты информации» и ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»

- *Угроза потенциальная причина инцидента, который может нанести ущерб системе или 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];**

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Свойства информации:

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Свойства информации:

Конфиденциальность: *доступ к информации только авторизованных пользователей*

Доступность: *доступ к информации и связанным с ней активам авторизованных пользователей по мере необходимости*

Целостность: *достоверность и полнота информации и методов ее обработки;*

ГОСТ Р ИСО/МЭК 17799-2005

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Свойства информации:

Конфиденциальность: *доступ к информации только авторизованных пользователей*

Доступность: *доступ к информации и связанным с ней активам авторизованных пользователей по мере необходимости*

Целостность: *достоверность и полнота информации и методов ее обработки;*

ГОСТ Р ИСО/МЭК 17799-2005

Аутентичность или подлинность (authenticity) - *свойство, гарантирующее, что субъект или ресурс идентичны заявленным;*

Неотказуемость или неоспоримость (non-repudiation) – *способность удостоверять имевшее место действие или событие так, чтобы эти события или действия не могли быть позже отвергнуты* **[ГОСТ Р ИСО/МЭК 13335-1-2006];**

Достоверность или функциональность (reliability) –
свойство соответствия преднамеренному поведению и результатам
[ГОСТ Р ИСО/МЭК 13335-1-2006];

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

- *состояние **защищенности** национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.*

Доктрина информационной безопасности РФ

- *безопасность, связанная с угрозами в **информационной сфере** (состояние защищенности интересов (целей) организации БС РФ в условиях **угроз**),.*

Стандарт Банка России СТО БР ИББС-1.0

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

- *состояние **защищенности** национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.*

Доктрина информационной безопасности РФ

- *безопасность, связанная с угрозами в **информационной сфере** (состояние защищенности интересов (целей) организации БС РФ в условиях **угроз**),.*

Стандарт Банка России СТО БР ИББС-1.0

- **Защищенность** достигается обеспечением совокупности **свойств ИБ** — доступности, целостности, конфиденциальности **информационных активов**.
- **Информационный актив:** информация с реквизитами, позволяющими ее идентифицировать; имеющая ценность для организации, находящаяся в распоряжении организации и представленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме.
- **Информационная сфера** представляет собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение, хранение и использование информации, а также системы регулирования возникающих при этом отношений.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации или средства ее обработки.

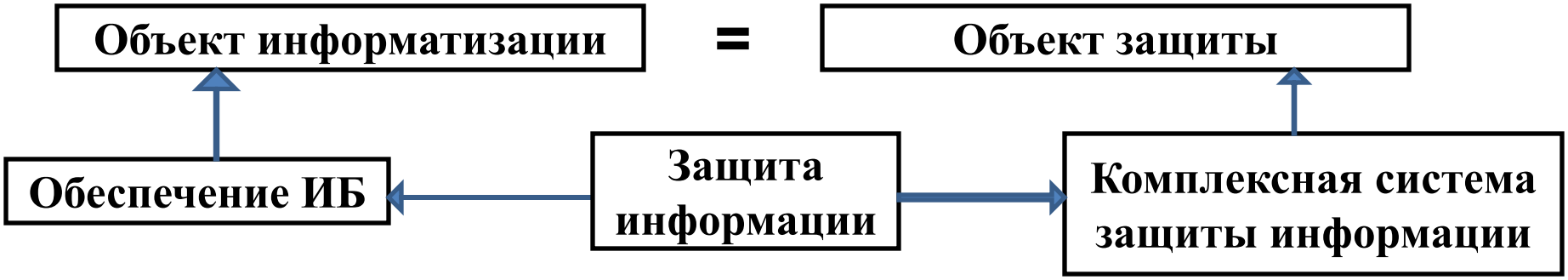
ГОСТ Р 53113.1-2008 «Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения»

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

состояние защищённости информации, которое достигается обеспечением совокупности для нее свойств доступности, целостности, конфиденциальности, аутентичности, подотчетности, неотказуемости и достоверности.

1. Концептуальные основы обеспечения ИБ

Традиционный подход:



Определения(ГОСТ Р 50922-2006):

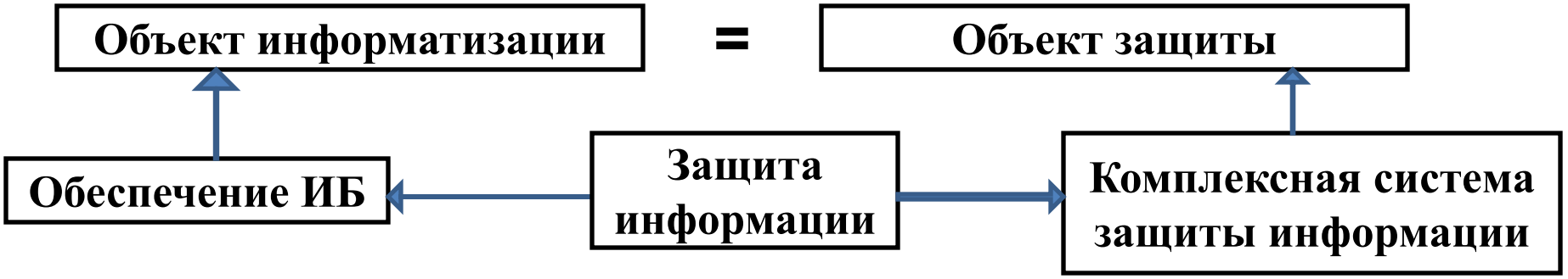
***«защита информации»* – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию;**

***«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**

1. Концептуальные основы обеспечения ИБ

Традиционный подход:



Определения(ГОСТ Р 50922-2006):

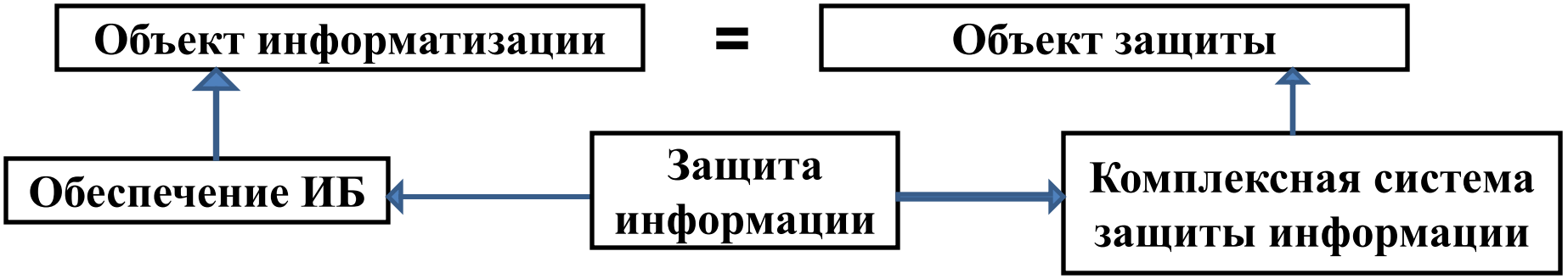
***«защита информации»* – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию;**

***«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**

1. Концептуальные основы обеспечения ИБ

Традиционный подход:



Определения(ГОСТ Р 50922-2006):

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

«базовые защитные меры» - **минимальный набор защитных мер, установленный для системы или организации;**

«мера защиты информации» - ???

1. Концептуальные основы обеспечения ИБ

Определения: *«мера защиты информации» -*

Организационные меры защиты информации:

- ограничение доступа к помещениям, где информация содержится и обрабатывается;
- допуск только проверенных лиц к конфиденциальной информации;
- хранение информации в закрытых для посторонних сейфах;
- блокировка просмотра содержания обрабатываемых материалов;
- криптографическая защита при передаче каналами связи;
- своевременное уничтожение остаточной информации.

Организационно-технические меры защиты информации:

- организация независимого питания оборудования, содержащего и обрабатывающего ценную информацию;
- установка кодовых замков;
- использование жидкокристаллических или плазменных дисплеев, струйных принтеров и термопринтеров, избегая высокочастотного электромагнитного излучения;
- уничтожение информации при списании или отправки компьютера в ремонт;
- минимальная защита снятия информации акустическим способом с помощью мягких прокладок, установленных под оборудованием;

1. Концептуальные основы обеспечения ИБ

Традиционный подход: кризис

«Кризис подхода» - 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

1. Концептуальные основы обеспечения ИБ

«Кризис подхода» - 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.

1. Концептуальные основы обеспечения ИБ

«Кризис подхода» - 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.

1. Концептуальные основы обеспечения ИБ

Современный подход: управленчески-ориентированный

Информационная безопасность - состояние защищённости информации, которое достигается обеспечением совокупности для нее свойств доступности, целостности, конфиденциальности, аутентичности, подотчетности, неотказуемости и достоверности.

Обеспечение ИБ – это системный процесс, а не состояние.

Процессом надо управлять!

Эффективность обеспечения ИБ определяется эффективностью управления

1. Концептуальные основы обеспечения ИБ

Основные идеи новой концептуальной схемы (модели) 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.

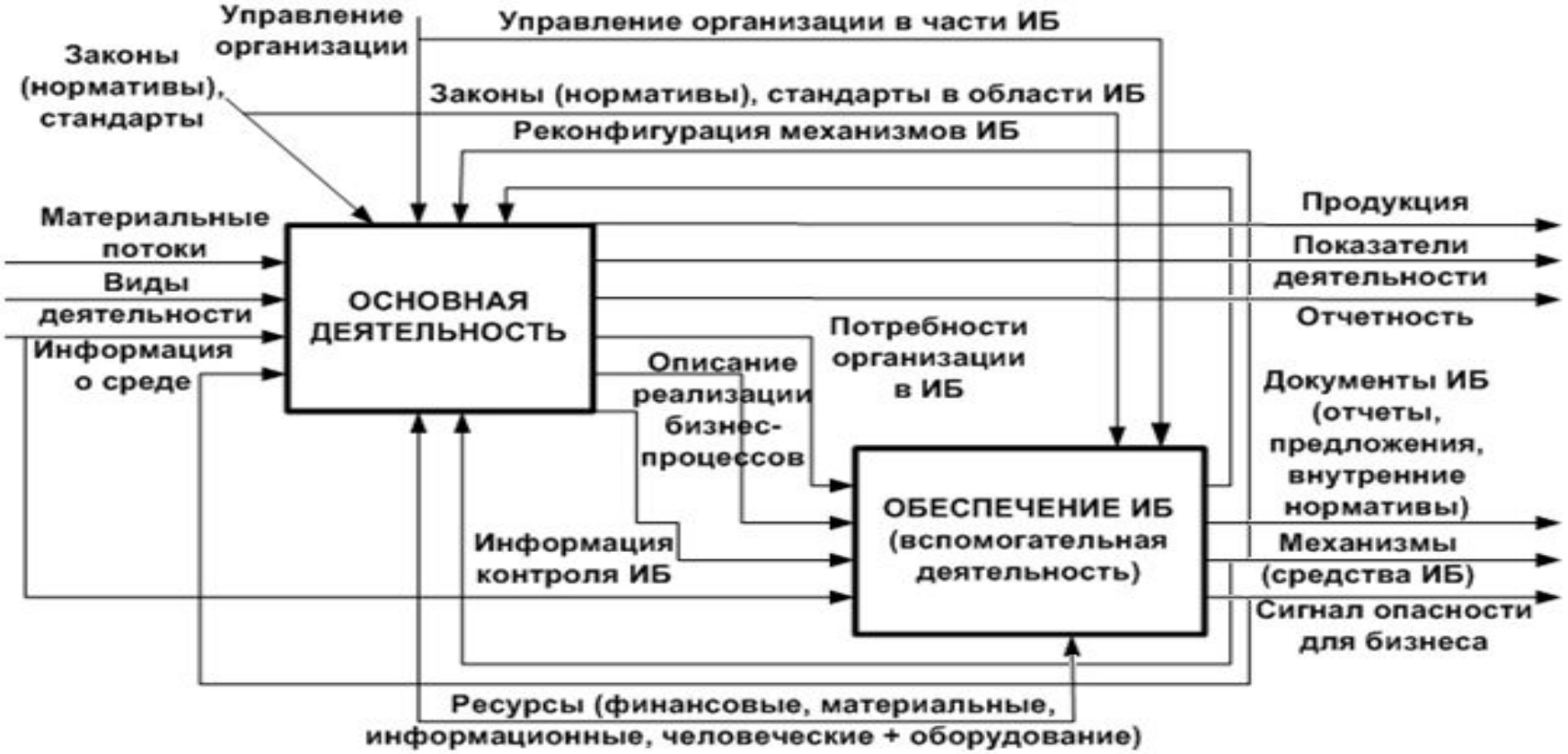
Процессы по обеспечению ИБ –

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

1. Концептуальные основы обеспечения ИБ

Основные идеи новой концептуальной схемы (модели) обеспечения ИБ:

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



1. Концептуальные основы обеспечения ИБ

Основные идеи новой концептуальной схемы (модели) 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**

1. Концептуальные основы обеспечения ИБ

Основные идеи новой концептуальной схемы (модели) 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.

1. Концептуальные основы обеспечения ИБ

Основные идеи новой концептуальной схемы (модели) обеспечения ИБ:

1. Концептуальные основы обеспечения ИБ

Основные идеи новой концептуальной схемы (модели) 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

4.1.Исходная концептуальная схема обеспечения ИБ

Основные идеи новой концептуальной схемы (модели) 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.

4.1.Исходная концептуальная схема обеспечения ИБ

Основные идеи новой концептуальной схемы (модели) 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) При любом вмешательстве в объект в первую очередь страдает ее безопасность

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

1. Концептуальные основы обеспечения ИБ

Основные идеи новой концептуальной схемы (модели) 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];

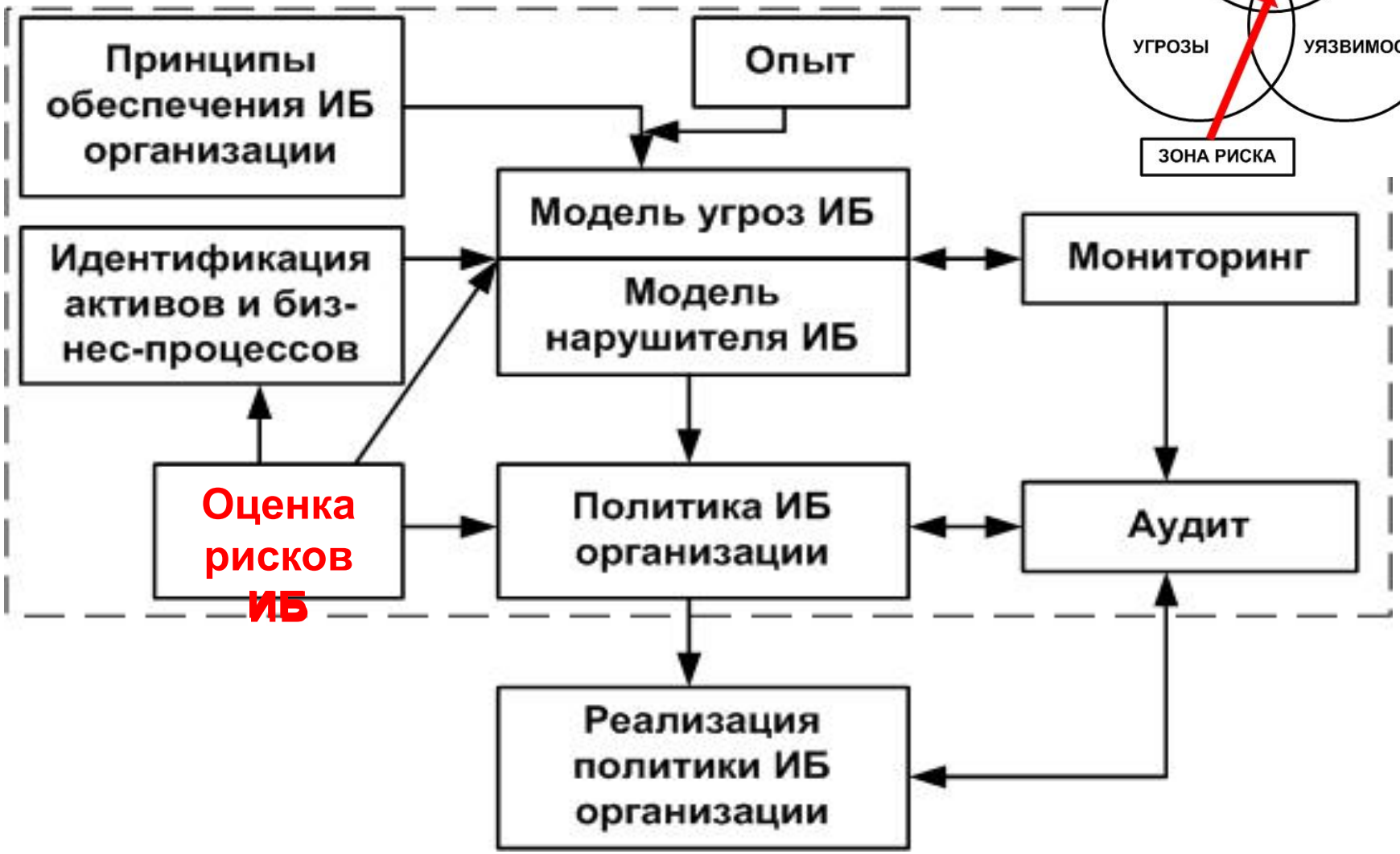
«Уязвимость» (vulnerability) - слабость одного или нескольких активов, которая может быть использована одной или несколькими угрозами [ГОСТ Р ИСО/МЭК 13335-1-2006];

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

1. Концептуальные основы обеспечения ИБ

Основные идеи новой концептуальной схемы (модели) обеспечения ИБ:

✔ **Менеджмент рисков ИБ – основа деятельности по обеспечению ИБ**



1. Концептуальные основы обеспечения ИБ

Основные идеи новой концептуальной схемы (модели) 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?

1. Концептуальные основы обеспечения ИБ

Основные идеи новой концептуальной схемы (модели) 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

1. Концептуальные основы обеспечения ИБ

Основные идеи новой концептуальной схемы (модели) 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?

1. Концептуальные основы обеспечения ИБ

Основные идеи новой концептуальной схемы (модели) 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?

1. Концептуальные основы обеспечения ИБ

Основные идеи новой концептуальной схемы (модели) 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.

1. Концептуальные основы обеспечения ИБ

Основные идеи новой концептуальной схемы (модели) обеспечения ИБ:

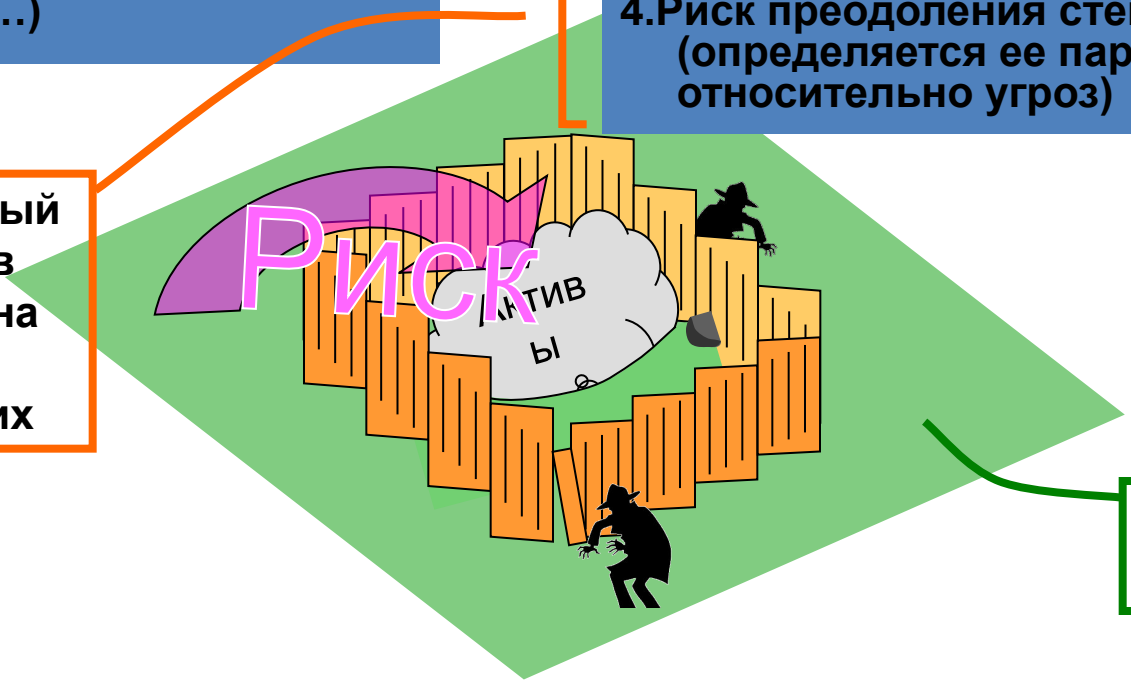
✔

По ГОСТ ИСО/МЭК 15408

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)

1. Концептуальные основы обеспечения ИБ

Основные идеи новой концептуальной схемы (модели) 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.

1. Концептуальные основы обеспечения ИБ

Основные идеи новой концептуальной схемы (модели) 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,

4.1.Исходная концептуальная схема обеспечения ИБ

Основные идеи новой концептуальной схемы (модели) 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

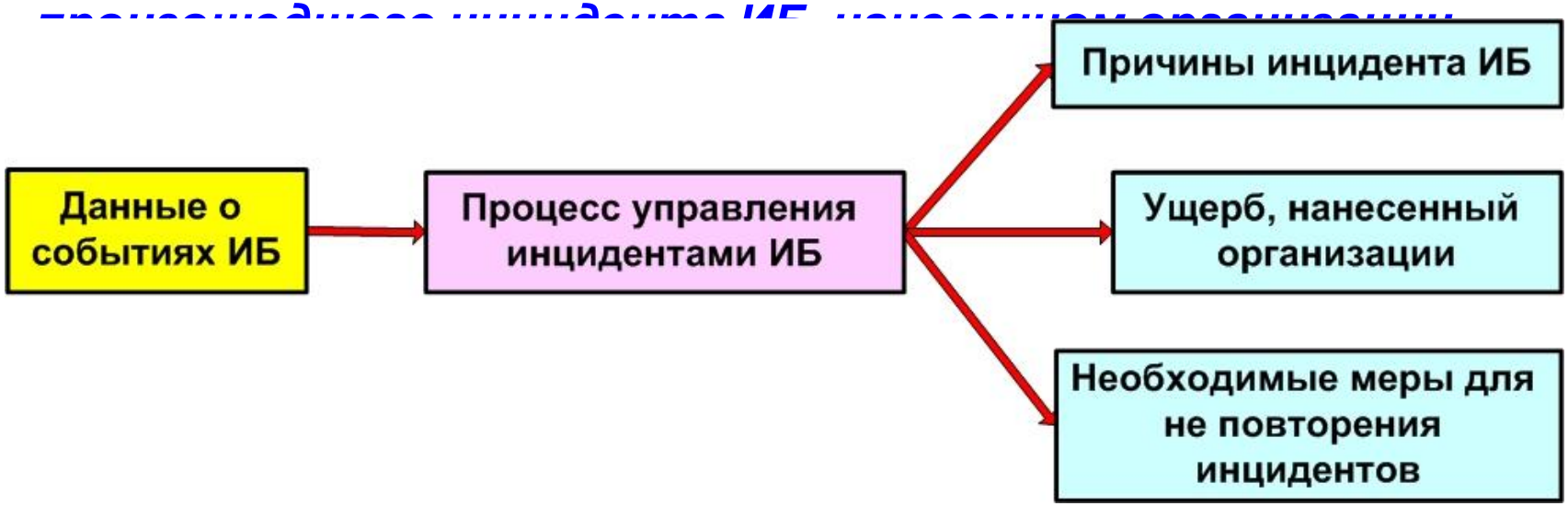
4.1.Исходная концептуальная схема обеспечения ИБ

Основные идеи новой концептуальной схемы (модели) 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



1. Концептуальные основы обеспечения ИБ

Основные идеи новой концептуальной схемы (модели) 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**

1. Концептуальные основы обеспечения ИБ

Основные идеи новой концептуальной схемы (модели) обеспечения ИБ:

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

Назначение СУИИБ

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.

Структура СУИИБ

1. Концептуальные основы обеспечения ИБ

Основные идеи новой концептуальной схемы (модели) 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:**

1. Концептуальные основы обеспечения ИБ

Основные идеи новой концептуальной схемы (модели) 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**

1. Концептуальные основы обеспечения ИБ

Основные идеи новой концептуальной схемы (модели) 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»***

1. Концептуальные основы обеспечения ИБ

Основные идеи новой концептуальной схемы (модели) обеспечения ИБ:

1. **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);

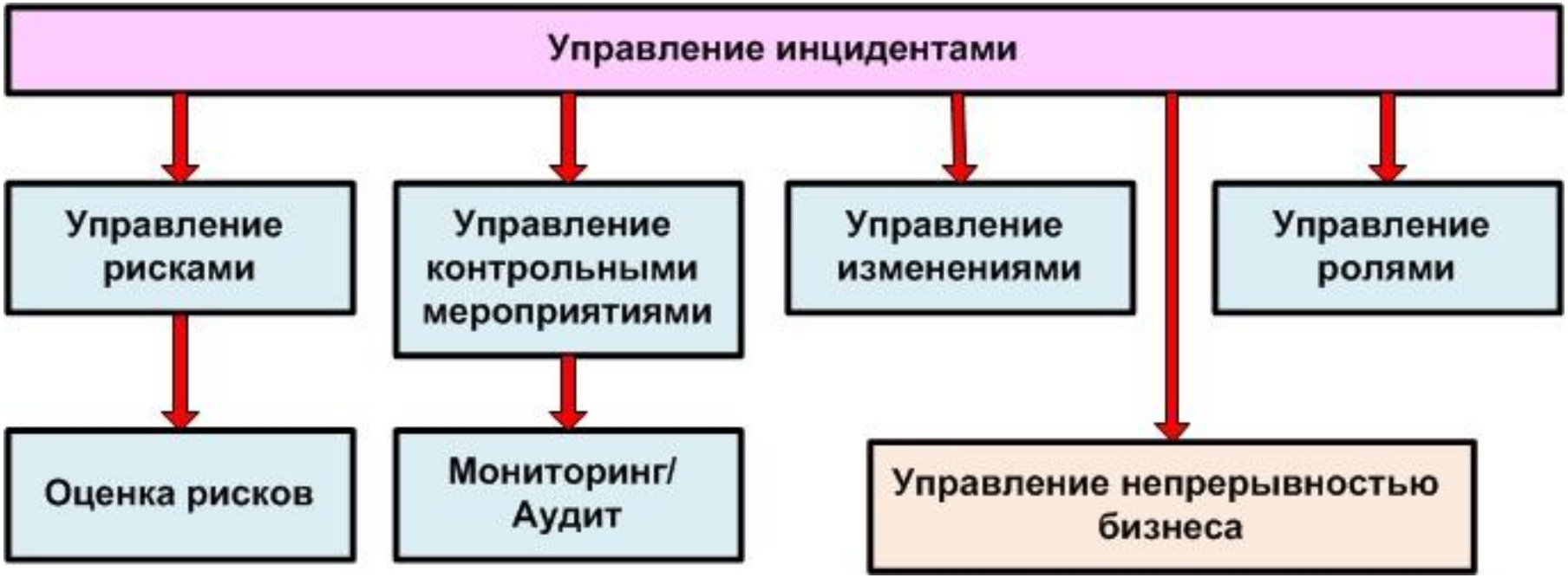
***«процессный подход»:* деятельность по обеспечению ИБ в виде системы процессов в пределах организации;**

***«процесс»:* любое действие, использующее ресурсы и управляемое**

1. Концептуальные основы обеспечения ИБ

Основные идеи новой концептуальной схемы (модели) обеспечения ИБ:

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



1. Концептуальные основы обеспечения ИБ

Современный подход: управленчески-ориентированный

Основные идеи новой концептуальной схемы (модели) 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*

1. Концептуальные основы обеспечения ИБ

Основные идеи новой концептуальной схемы (модели) 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:

1. Концептуальные основы обеспечения ИБ

Основные идеи новой концептуальной схемы (модели) 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:

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***

Благодарю за внимание!

Толстой Александр Иванович

AITolstoj@mephi.ru

8(499)324-97-35