



Система управления информационной безопасностью. Управление активами

Толстой Александр Иванович

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

Москва, 2016



ГОСТ Р ИСО/МЭК 27000

ИТ. Методы и средства обеспечения безопасности. Системы менеджмента ИБ. Общий обзор и терминология

ISO/IEC 27000

Information technology — Security techniques — Information security management systems — Overview and vocabulary

Система менеджмента информационной безопасности (СМИБ) (information security management system (ISMS):

часть общей системы менеджмента, основанная на подходе бизнес-рисков, по созданию, внедрению, функционированию, мониторингу,²

**ГОСТ Р ИСО/МЭК 27002-2012
ИТ. Методы и средства обеспечения
безопасности. Свод норм и правил менеджмента
информационной безопасности**

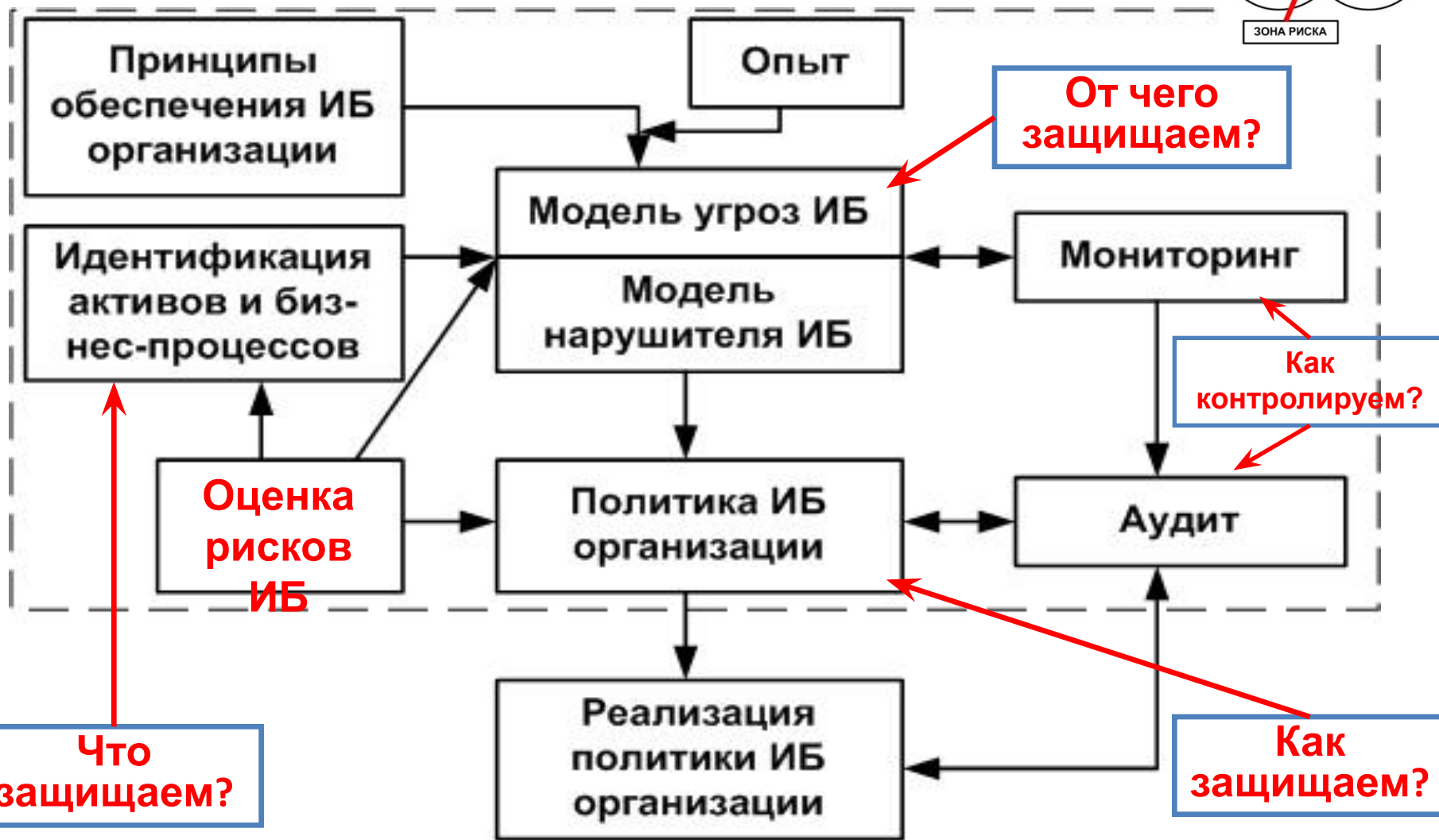
ISO/IEC 27002:2005

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

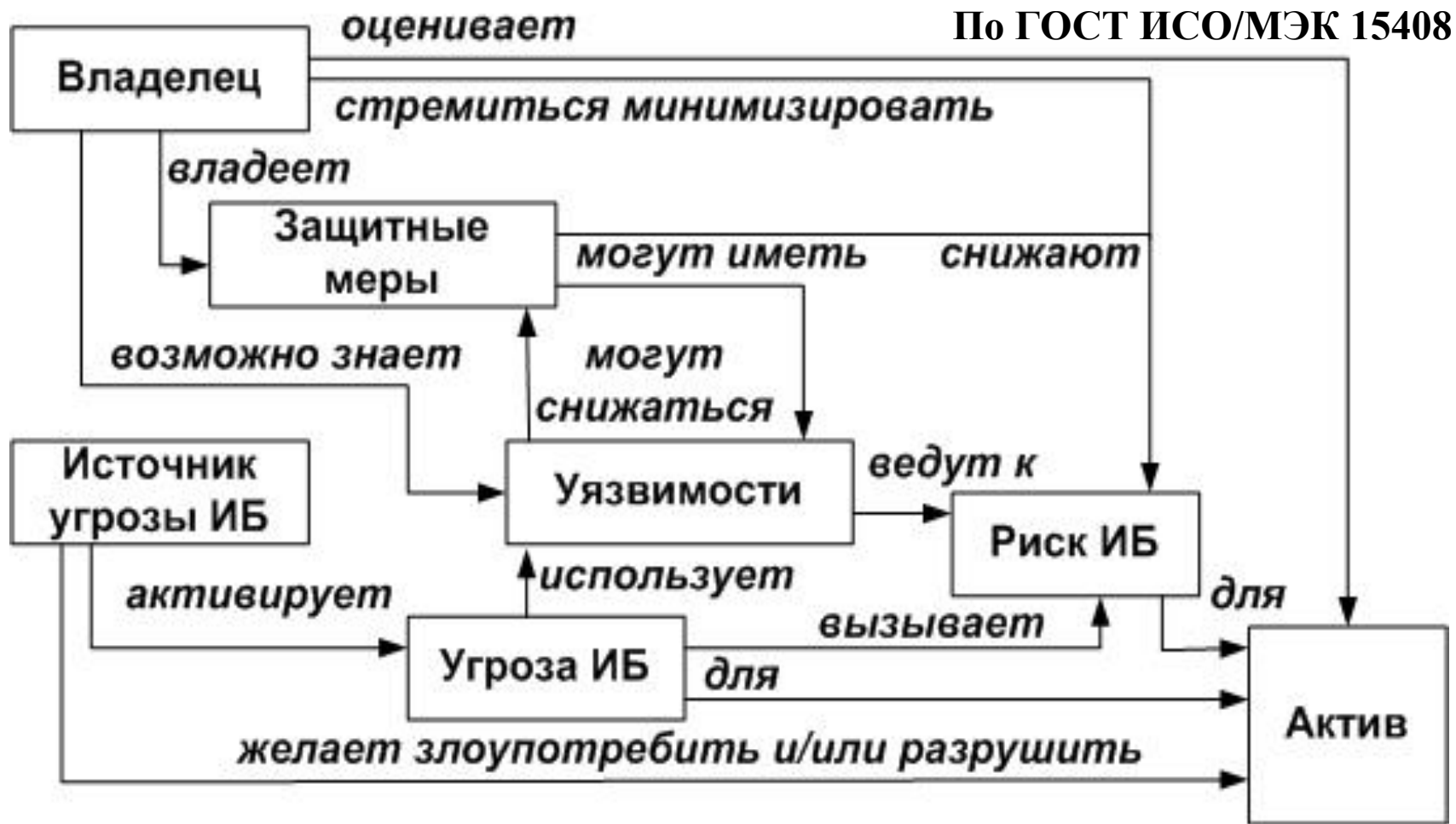
Система управления ИБ: Основные процессы СУИБ



Принципы управления ИБ:



Принципы управления ИБ:



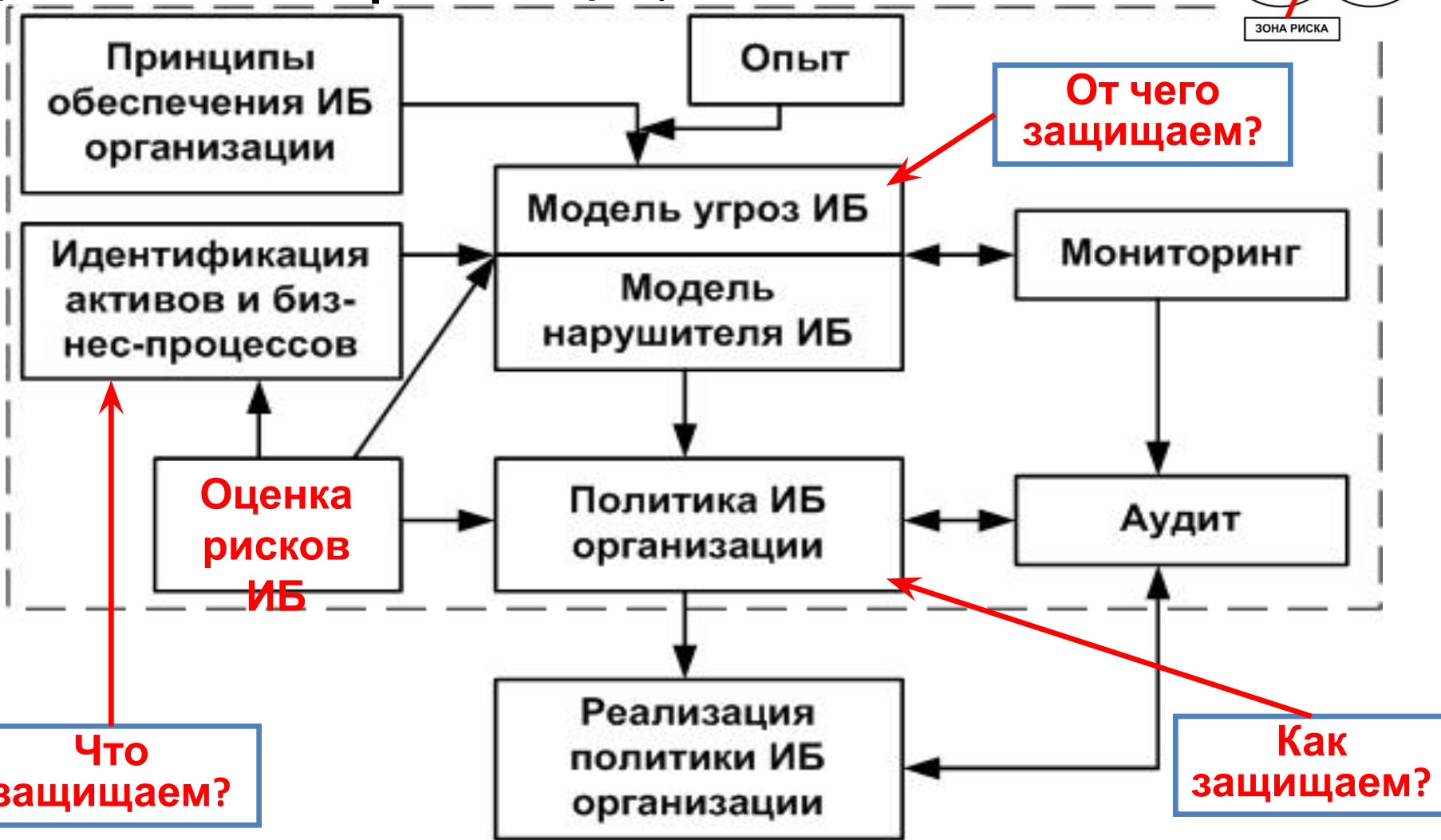
Управление активами

Цель: Обеспечить соответствующую защиту активов организации.

Все активы должны учитываться и иметь назначенного владельца.

Необходимо определять владельцев всех активов, и следует определять ответственного за поддержку соответствующих мер и средств контроля и управления. Реализация определенных мер и средств контроля и управления при необходимости может быть делегирована владельцем, но владелец остается ответственным за надлежащую защиту активов.

Принципы управления ИБ: Активы могут рассматриваться только в контексте целей деятельности организации, но не как иначе



Управление активами: идентификация активов и бизнес процессов

Принципы управления ИБ: активы могут рассматриваться только в контексте целей деятельности организации, но не как иначе

Два этапа:

1. Определить (идентифицировать) основные бизнес процессы, реализуемые на объекте.
2. Описать (идентифицировать) <важные> активы, относящиеся именно к этим бизнес процессам

Управление активами: идентификация активов

Мера и средство контроля и управления: все активы должны быть четко определены, должна составляться и поддерживаться опись всех важных активов.

Рекомендации по реализации:

1. Следует идентифицировать все активы и документально оформлять значимость этих активов.
2. В опись информационных активов следует включить всю информацию, необходимую для восстановления после бедствия, в том числе тип актива, формат, местоположение, информацию о резервных копиях, информацию о лицензировании и ценности для бизнеса.
3. Владение и классификация информации должны быть согласованы и документально оформлены в отношении каждого актива.
4. Основываясь на важности актива, его ценности для бизнеса и его категории секретности, надлежит определить уровни защиты, соответствующие значимости активов.

Управление активами: типы активов:

- a) **информация:** базы данных и файлы данных, договоры и соглашения, системная документация, исследовательская информация, руководства пользователя, учебные материалы, процедуры эксплуатации или поддержки, планы непрерывности бизнеса, меры по переходу на аварийный режим, контрольные записи и архивированная информация;
- b) **программные активы:** прикладные программные средства, системные программные средства, средства разработки и утилиты;
- c) **физические активы:** компьютерное оборудование, средства связи, съемные носители информации и другое оборудование;
- d) **услуги:** вычислительные услуги и услуги связи, основные поддерживающие услуги, например отопление, освещение, электроэнергия и кондиционирование воздуха;
- e) **персонал,** его квалификация, навыки и опыт;
- f) **нематериальные ценности,** например репутация и имидж организации.

Управление активами: идентификация активов:

Описи активов помогают обеспечивать уверенность в том, что активы организации эффективно защищены,

Процесс инвентаризации активов - важное условие для менеджмента риска.

Данные описи могут также потребоваться для других целей, таких как обеспечение безопасности труда, страховые или финансовые (менеджмент активов) вопросы.

Управление активами: владение активами:

Мера и средство контроля и управления: вся информация и активы, связанные со средствами обработки информации должны находиться во владении определенной части организации.

Термином "владелец" определяется физическое или юридическое лицо, которое наделено административной ответственностью за руководство изготовлением, разработкой, хранением, использованием и безопасностью активов.

Термин "владелец" не означает, что данный

Управление активами: владение активами:

Рекомендация по реализации:

Владелец актива должен нести ответственность за:

- a) обеспечение уверенности в том, что информация и активы, связанные со средствами обработки информации, классифицированы соответствующим образом;
- b) определение и периодический пересмотр ограничений и классификаций доступа, принимая в расчет применимые политики управления доступом.

Владение может распространяться на:

- a) процесс бизнеса;
- b) определенный набор деятельности;
- c) прикладные программы;
- d) определенное множество данных.

Дополнительная информация:

Повседневные задачи могут быть переданы, например должностному лицу, ежедневно работающему с активом, но ответственность сохраняется за владельцем.

Управление активами: приемлемое использование активов:

Мера и средство контроля и управления: следует определять, документально оформлять и реализовывать правила приемлемого использования информации и активов, связанных со средствами обработки информации.

Рекомендация по реализации:

1. Всем служащим, подрядчикам и представителям третьей стороны рекомендуется следовать правилам приемлемого использования информации и активов, связанных со средствами обработки информации, включая (например):

а) правила использования электронной почты и Интернета ;

Управление активами: приемлемое использование активов:

Мера и средство контроля и управления: следует определять, документально оформлять и реализовывать правила приемлемого использования информации и активов, связанных со средствами обработки информации.

Рекомендация по реализации:

2. Соответствующему управленческому персоналу должны быть предоставлены конкретные правила или рекомендации.

3. Служащие, подрядчики и представители третьей стороны, использующие или имеющие доступ к активам организации, должны быть осведомлены о существующих ограничениях в отношении использования ими информации и активов организации, связанных со средствами обработки информации и ресурсами.

4. Они должны нести ответственность за использование ими любых средств обработки информации, и любое использование таких средств осуществлять под свою

РС БР ИББС-2.2 «Обеспечение ИБ организаций банковской системы Российской Федерации. Методика оценки рисков нарушения ИБ»:

Виды активов:

Информационный актив: информация с реквизитами, позволяющими ее идентифицировать; имеющая ценность для организации БС РФ; находящаяся в распоряжении организации БС РФ и представленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме.

Объект среды информационного актива: материальный объект среды использования и (или) эксплуатации информационного актива (объект хранения, передачи, обработки, уничтожения и т.д.).

РС БР ИББС-2.2 «Обеспечение ИБ организаций банковской системы Российской Федерации. Методика оценки рисков нарушения ИБ»:

Перечень типов информационных активов в организации БС РФ (пример):

- информация ограниченного доступа;
- информация, содержащая сведения, составляющие банковскую тайну:
 - платежная информация (информация, предназначенная для проведения расчетных, кассовых и других банковских операций и учетных операций);
 - информация, содержащая сведения, составляющие коммерческую тайну;
 - персональные данные;
 - управляющая информация платежных, информационных и телекоммуникационных систем (информация, используемая для технической настройки программно-аппаратных комплексов обработки, хранения и передачи информации):

РС БР ИББС-2.2 «Обеспечение ИБ организаций банковской системы Российской Федерации. Методика оценки рисков нарушения ИБ»:

Перечень типов объектов среды (пример):

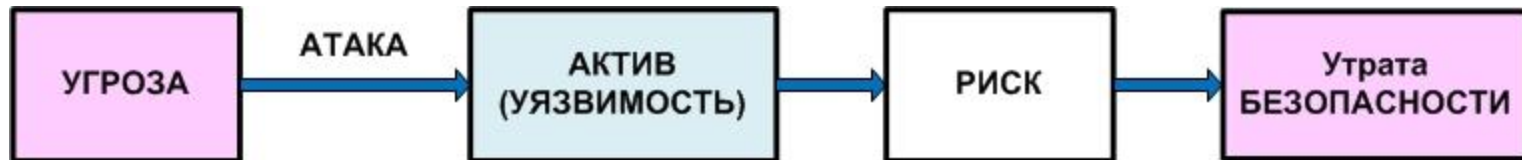
- линии связи и сети передачи данных;
- сетевые программные и аппаратные средства, в том числе сетевые серверы;
- файлы данных, базы данных, хранилища данных;
- носители информации, в том числе бумажные носители;
- прикладные и общесистемные программные средства;
- программно-технические компоненты автоматизированных систем;
- помещения, здания, сооружения;
- платежные и информационные технологические процессы.

Связь «актив» «уязвимость»

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

«Уязвимость» (бреш) (*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)



Управление активами: идентификация активов:

Рекомендация: при идентификации активов необходимо описать уязвимости (слабости) этих активов

Управление активами: идентификация активов и бизнес процессов

Принципы управления ИБ: активы могут рассматриваться только в контексте целей деятельности организации, но не как иначе

Три этапа идентификация активов и бизнес процессов:

1. Определить (идентифицировать) основные бизнес процессы, реализуемые на объекте.
2. Описать (идентифицировать) <важные> активы, относящиеся именно к этим бизнес процессам.

Благодарю за внимание!

Толстой Александр Иванович

AITolstoj@mephi.ru

8(499)324-97-35