Аудит информационной безопасности

Необходимость проведения аудита

- Возрастающая роль ИТ в поддержке бизнес-процессов:
  - возрастающие требования к ИБ автоматизированных систем;
  - цена ошибок и сбоев информационных систем возрастает.
- Возрастающая сложность информационных процессов:
  - повышенные требования к квалификации персонала, ответственного за обеспечение ИБ;
  - выбор адекватных решений, обеспечивающих приемлемый уровень ИБ при допустимом уровне затрат, становится все более сложной задачей.

Для нейтрализации воздействия этих причин необходимо

- отслеживать соответствие квалификации персонала, ответственного за обеспечение ИБ и стоящих задач;
- получить объективную оценку состояния подсистемы ИБ.

- С этой целью создаются организации аудиторов в области ИБ, ставящие своей целью:
  - проведение экспертизы соответствия системы ИБ некоторым требованиям,
  - оценку системы управления ИБ,
  - повышение квалификации специалистов в области ИБ.

  Статус таких организаций может быть как государственный (при национальных институтах стандартов) так и независимых международных организаций.

ISO (Международная Организация по Стандартизации)
IEC (Международная Электротехническая Комиссия)

- Формируют специализированную систему всемирной стандартизации
- В области информационных технологий, ISO и IEC организован совместный технический комитет – ISO/IEC JTC 1/SC 27.
- Проекты Международных Стандартов, принятые совместным техническим комитетом передаются в государственные органы для голосования.
- Публикация в качестве Международного Стандарта требует одобрения не менее 75 процентов проголосовавших государственных органов.

Стандарты ISO/IEC

- **ISO/IEC 27000** Определения и основные принципы. Планируется унификация со стандартами COBIT и ITIL. Проект стандарта находится в разработке
- **ISO/IEC 27001:2005** Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования. (**BS 7799-2:2005**). Выпущен в июле 2005 г.
- **ISO/IEC 27002:2005** Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью (ранее **ISO/IEC 17799:2005**)
- **ISO/IEC 27003** Руководство по внедрению системы управления информационной безопасностью. Выпуск запланирован на 2008 г.
- **ISO/IEC 27004** Измерение эффективности системы управления информационной безопасностью. Выпуск запланирован на 2008 г.
- **ISO/IEC 27005:2008** Информационные технологии. Методы обеспечения безопасности. Управление рисками информационной безопасности (на основе BS 7799-3:2006). Выпущен в июне 2008 г.

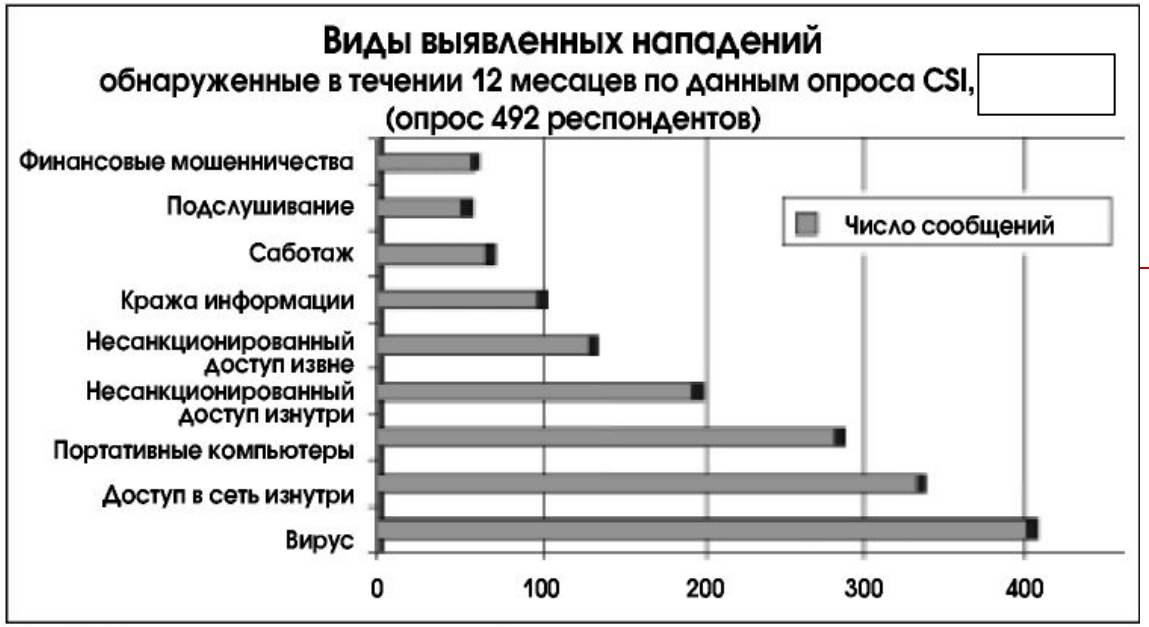
Построение системы управления ИБ в соответствии со стандартами ISO/IEC

- Предполагает
  - явно декларированных целей в области безопасности;
  - эффективной системы менеджмента ИБ, имеющей совокупность показателей для оценки ИБ в соответствии с декларированными целями, инструментарий для обеспечения ИБ и оценки текущего ее состояния;
  - некоторой методики проведения аудита ИБ, позволяющей объективно оценить положение дел в области ИБ.

Эффект может дать только комплексный подход к аудиту

- проверка на соответствие определенным требованиям не только программно-технической составляющей некоторой информационной технологии, но и решений на:
  - процедурном уровне (организация работы персонала и регламентация его действий), и
  - административном уровне (корректность существующей программы обеспечения ИБ и практика ее выполнения).

- *Иллюстрацией этого положения являются данные Института компьютерной безопасности (Computer Security Institute, CSI).*



Данные Института компьютерной безопасности (Computer Security Institute, CSI).

Процедура проведения аудита информационных систем в соответствии с международным стандартом

ISO/IEC 27002:2005 «Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью» (ранее ISO/IEC 17799:2005)

Подготовка организации к аудиту

Подготовительные мероприятия включают подготовку документации и проведение внутренней проверки соответствия системы управления ИБ требованиям стандарта.

Документация должна содержать:

- политику безопасности;
- границы защищаемой системы;
- оценки рисков;
- управление рисками;
- описание инструментария управления ИБ;
- ведомость соответствия – документ, в котором оценивается соответствие требованиям стандартов поставленных целей в области ИБ и средств управления ИБ.

Внутренняя проверка соответствия системы управления ИБ требованиям стандарта

- Состоит в проверке выполнения каждого положения стандарта.
- Проверяющие должны ответить на два вопроса:
  - выполняется ли данное требование, и если нет, то
  - каковы точные причины невыполнения?
- На основе ответов составляется ведомость соответствия.

- Основная цель этого документа – дать аргументированное обоснование имеющим место отклонениям от требований стандарта.
- После завершения внутренней проверки устраняются выявленные несоответствия, которые организация сочтет нужным устранить.

Аудит подсистемы ИБ на соответствие стандарту ISO/IEC 27002:2005

- Аудиторы должны проанализировать все существенные аспекты с учетом:
  - размера проверяемой организации
  - специфики ее деятельности
  - ценности информации, подлежащей защите.
- Как следствие, опыт и компетентность аудитора являются очень существенными факторами.

Задачи аудита (сертификации)

- В результате проведения аудита создается список :
  - замечаний;
  - выявленных несоответствий требованиям стандартов;
  - рекомендаций по их исправлению.
- Аудиторы должны гарантировать, что были выполнены все требования процедуры сертификации.

Категории несоответствий

- И аудиторам, и проверяемой организации необходимо иметь четкое представление о степени серьезности обнаруженных недостатков, их категориях и способах исправления.
- Используются следующие категории несоответствия:
  - *Существенное несоответствие.*
    - Не выполняется одно или несколько базовых требований стандартов, либо установлено, что используются неадекватные меры по защите конфиденциальности, целостности или доступности критически важной информации.
  - *Несущественное несоответствие.*
    - Не выполняются некоторые второстепенные требования, что несколько повышает риски или снижает эффективность защитных мер.
- Каждое несоответствие должно иметь ссылку на соответствующее требование стандартов.
- *В случае, если выявлено значительное количество несущественных несоответствий, аудитор должен рассмотреть вопрос о возможном появлении существенного несоответствия*

Пути устранения несоответствий

- После выявления несоответствий аудитор и представители организации должны наметить пути их устранения
- Если аудитор считает, что подсистему ИБ возможно усовершенствовать, то он может составить замечание.
- Организации сами определяют, какие действия им следует предпринять в ответ на замечание.
- Замечания фиксируются, и при последующих проверках аудиторы должны выяснить, что было сделано.

Организация аудита. Подготовка и планирование аудита

- Процедура проведения аудита планируется заранее.
- План проведения аудита должен быть подготовлен для всех первоначальных и контрольных проверок, продолжающихся более одного дня.
- Аудиторы должны быть ознакомлены с законодательными и нормативными требованиями, используемыми в проверяемой организации.

Проверка документации

- Аудит (сертификация) начинается с того, что аудитор получает и анализирует документы, имеющие отношение к подсистеме ИБ.
- Организация должна представить следующие документы:
  - концепцию политики ИБ, границы подсистемы ИБ, документы по оценке рисков;
  - руководство по реализации политики безопасности, содержащее общую схему подсистемы ИБ и документированные процедуры обеспечения ИБ;
  - ведомость соответствия – документ, составленный аудитором при предыдущей проверке. Содержание этого документа будет рассмотрено ниже.
- По окончании проверки представляется отчет, в котором должны быть отражены следующие моменты:
  - декларируемые цели в области ИБ достижимы (являются реалистичными);
  - ведомость соответствия не противоречит стандартам в области ИБ и политике безопасности;
  - должным ли образом описаны все соответствующие аспекты в процедурах обеспечения ИБ.

Подготовительный этап – планирование проведения аудита

- План проведения аудита должен определять подлежащие проверке сферы деятельности организации.
- В плане должно быть указано, какие требования стандарта будут проверяться (согласно Ведомости соответствия).
- Этот план, вместе со всеми изменениями, внесенными в процессе выполнения аудита, прилагается к отчету о проведении аудита.

- **План составляется на основе следующих документов:**
  - Руководство по реализации политики безопасности;
  - Ведомость соответствия.

- Организация должна представить сведения о собственной структуре, текущей деятельности, проектах и т.д.
- Кроме того, потребуется описание используемых информационных технологий, включающее схему сети, а также список всего прикладного программного обеспечения, используемого в организации.

Процедура проведения аудита

- Процедура проведения аудита должна начинаться с официального вступительного собрания.
- На собрании руководству среднего и верхнего звена и сотрудникам, занимающимся вопросами безопасности, должны быть разъяснены следующие вопросы:
  - рамки проведения аудита;
  - объяснение методов оценки;
  - определение несоответствий и действия по их устранению;
  - замечания и возможная реакция на них;
  - план проведения аудита;
  - доступность документации;
  - возможные трудности, которые могут возникнуть в процессе работы – отсутствие ведущих специалистов и т.д.;
  - организация работы с конфиденциальными сведениями, необходимыми для проведения аудита, включая отчет о проведении аудита и замечания о несоответствиях. В частности, администрация должна понимать, что аудитору, возможно, потребуется обратиться к потенциально уязвимым участкам системы.

После проведения аудита проводится заключительное собрание с руководителями верхнего звена

- На нем должны быть рассмотрены следующие вопросы:
  - подтверждение рамок проведенного аудита;
  - краткое изложение найденных несоответствий, согласованных изменений;
  - краткое изложение замечаний и предложений;
  - общие замечания по ходу аудита и комментарии к отчету;
  - выводы: положительное заключение или отказ в сертификации (или продолжение сертификации);
  - подтверждение сохранения конфиденциальности сведений, полученных в ходе аудита.

- *Участники вступительного и заключительного собраний должны быть официально зарегистрированы*

Отчетность

- Главным результатом проведения аудита является официальный отчет, в котором должны быть отражены следующие вопросы:
  - Соответствие собственным требованиям организации в области ИБ и стандарту ISO/IEC 27002:2005 – согласно плану проведения аудита и Ведомости соответствия.
  - Подробная ссылка на основные документы заказчика, включая:
    - политику безопасности;
    - ведомость соответствия;
    - документы с описанием процедур обеспечения ИБ;
    - дополнительные обязательные или необязательные стандарты и нормы, применяемые к данной организации.
    - Общие замечания по выводам проведения аудита.
    - Количество и категории полученных несоответствий и замечаний.
    - Необходимость дополнительных действий по аудиту (если таковая имеется) и их общий план.
    - Список сотрудников, принимавших участие в тестировании.
- Этот отчет является официальным документом проведения аудита и его оригинал должен быть доступен сертифицирующему органу.
- В документе должны быть определены конкретные аспекты обеспечения безопасности (установленные проверяемой организацией и стандартам ISO/IEC 27002:2005), которые будут рассматриваться при каждом посещении.
- Отчет должен обновляться при каждом проведении аудита.

Подготовка кадров и формальные требования к квалификации аудитора

- ***по версии Ассоциации аудита и управления информационными системами (The Information Systems Audit and Control Association & Foundation – ISACA)***
- Аудитор должен иметь
  - высшее образование в одной из областей: вычислительной техники, права, учета и пройти повышение квалификации ассоциации.
  - программа состоит из следующих блоков:
    - Базовые знания в области аудита ИБ – теория и практика управления ИБ и аудита, организация бизнес-процессов.
    - Спецкурсы – сети, законодательство в области информационных технологий, методы обеспечения безопасности и т.д.
    - Информационные технологии в бизнесе – модели и методы исследования бизнес-процессов, обеспечение их ИБ.
- После выполнения квалификационной работы выдается диплом аудитора ИБ.
- Подобные курсы работают при университетах нескольких стран: Австрии, Великобритании, Швеции, США.

Особенности зарубежных подходов

- Нахождение разумного компромисса, выбор приемлемого уровня безопасности при допустимых затратах является обязательным условием постановки задачи обеспечения ИБ.

- Постановка задачи нахождения компромисса между эффективностью подсистемы безопасности и ее стоимостью предполагает, как минимум, что:
  - существует система показателей для оценки эффективности подсистемы безопасности и методика их измерения;
  - существуют люди (должностные лица), уполномоченные принимать решение о допустимости определенного уровня остаточного риска;
  - существует система мониторинга, позволяющая отслеживать текущие параметры подсистемы безопасности.

Нормативные документы, регламентирующие вопросы сертификации и аттестации по требованиям ИБ

- Законы РБ;
- указы Президента БР;
- постановления Правительства РБ;

рассматриваются вопросы сертификации и аттестации по требованиям ИБ, а также лицензирования деятельности в области защиты информации