**Организация аудита информационной безопасности информационной системы**

**Андрушка Игорь Молдавская Экономическая Академия  
TIE - 238**

**Введение**

Современная информационная система организации представляет собой распределенную и неоднородную систему, использующую различные программно-аппаратные компоненты и имеющую точки выхода в сети общего пользования *(например, Интернет)*. В связи с этим значительно усложняется задача правильного и безопасного конфигурирования компонент и обеспечения защищенного взаимодействия между ними, и, как следствие, увеличивается количество уязвимых мест в системе.

Наличие уязвимостей в системе дает возможность потенциальному нарушителю провести успешную атаку и нанести ущерб деятельности организации. Появление «слабых мест» может быть обусловлено различными причинами, как объективного *(например, недоработки в базовом программном обеспечении)*, так и субъективного характера *(например, неправильная настройка оборудования)*.

Выявление и устранение уязвимостей, а также оценка общего уровня защищенности является чрезвычайно важной составляющей обеспечения безопасности, позволяющей существенно повысить уровень защищенности информационных и иных ресурсов системы.



*Рис. 1 Роль аудита информационной безопасности*

**Цели и назначение аудита**

К основным целям аудита информационной безопасности можно отнести следующие:

* Получение объективной и независимой оценки текущего состояния защищенности информационных ресурсов.
* Получение максимальной отдачи от средств, инвестируемых в создание системы информационной безопасности.
* Оценка возможного ущерба от несанкционированных действий.
* Разработка требований к построению системы защиты информации.
* Определение зон ответственности сотрудников подразделений.
* Расчет необходимых ресурсов.
* Разработка порядка и последовательности внедрения системы информационной безопасности.

Аудит может проводится в следующих вариантах:

* *Комплексный аудит* – перед созданием системы информационной безопасности
* *Точечный* – формирование требований к проведению модернизации системы защиты
* *Периодичный* – внешняя регламентная проверка уровня защищенности системы.
* *Проверочный* – экспертиза и оценка используемых, либо планируемых к использованию систем и решений.

### Этапы аудита

Процесс аудита информационных систем можно представить в виде своеобразных весов *(рис. 2)*, где на одной чаше рассматриваются системы безопасности доступа, на другой — контроль бизнес-процессов, а в качестве опоры служит техническая инфраструктура, которая, в свою очередь, основана на принятых методах авторизации, конфигурации системы, а также на политиках и процедурах, принятых в организации.

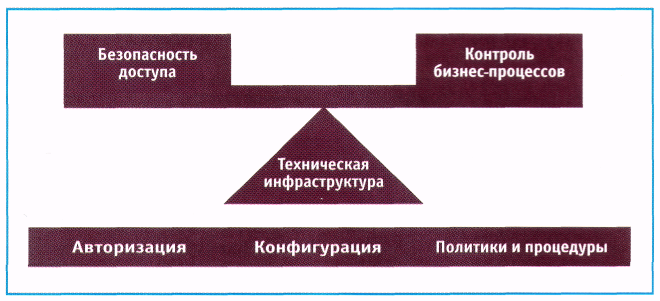


Рис. 2 Процесс аудита информационных систем

Работы по аудиту безопасности ИС включают в себя ряд последовательных этапов (рис. 3), которые в целом соответствуют этапам проведения комплексного аудита ИС, который включает в себя следующее:

1. комплексное обследование - включает сбор информации об используемых информационных ресурсах - системное программное обеспечение, локальные сети и телекоммуникации, прикладные системы, а также анализ существующих организационно-правовых процессов. По результатам обследования формируется (уточняется) перечень критичных ресурсов и разрабатывается перечень угроз для данных ресурсов;
2. проведение оценки защищенности - включает работы по обнаружению уязвимостей технических средств, анализу технологической защищенности, а также адекватности организационных процедур. На основе выявленных недостатков проводиться оценка рисков, включающая основные способы преодоления системы защиты, степень критичности и возможность реализации;
3. аттестация системы - включает мероприятия по обследованию (оценки) существующих мер и мероприятий по защите информации, оценки их адекватности, а также соответствие требования ведущих стандартов;
4. по результатам Аудита разрабатывается План исправления выявленных недостатков. Задача планирования состоит в определении приоритетов исправления обнаруженных недостатков, разработки очередности и методологии их устранения. Дополнительно предусматривается разработка концептуальных и процедурных документов, таких как Концепция информационной безопасности, Общие требования и рекомендации по защите информации, Политики безопасности и др.



*Рис 3. Этапы проведения аудита информационной безопасности*

В зависимости от целей и способа проведения аудита информационной безопасности инициатором этого мероприятия, как уже было отмечено выше, является заинтересованная сторона. Наиболее часто инициатором аудита является организация в лице его руководства.

Как правило на этапе обследования решаются следующие организационные вопросы:

* права и обязанности аудитора четко определяются и документально закрепляются в его должностных инструкциях, а также в положении о внутреннем *(внешнем)* аудите;
* аудитором подготавливается и согласовывается с руководством план проведения аудита информационной безопасности.

На этапе обследования также определяются границы проведения обследования. Границы проведения обследования обычно определяются в следующих терминах:

* список обследуемых физических, программных и информационных ресурсов;
* площадки *(помещения)*, попадающие в границы обследования;
* основные виды угроз безопасности, рассматриваемые при проведении аудита;
* организационные *(законодательные, административные и процедурные)*, физические, программно-технические и прочие аспекты обеспечения безопасности, которые необходимо учесть в ходе проведения обследования, и их приоритеты *(в каком объеме они должны быть учтены)*.

Далее следует сбор информации аудита, который является наиболее сложным и длительным. Это, как правило, связано с отсутствием необходимой документации на информационную систему и с необходимостью плотного взаимодействия аудитора со многими должностными лицами организации.

Компетентные выводы относительно положения дел в компании с информационной безопасностью могут быть сделаны аудитором только при условии наличия всех необходимых исходных данных для анализа. Получение информации об организации, функционировании и текущем состоянии ИС осуществляется аудитором в ходе специально организованных интервью с ответственными лицами компании, путем изучения технической и организационно-распорядительной документации, а также исследования ИС с использованием специализированного программного инструментария.

Обеспечение информационной безопасности организации – это комплексный процесс, требующий четкой организации и дисциплины. Он должен начинаться с определения ролей и распределения ответственности среди должностных лиц, занимающихся информационной безопасностью. Поэтому первый пункт аудиторского обследования начинается с получения информации об организационной структуре пользователей ИС и обслуживающих подразделений. В связи с этим аудитору требуется документация, касающаяся схемы организационной структуры ИС. Обычно, в ходе интервью аудитор задает опрашиваемым вопросы, касающиеся использования информации, циркулирующей внутри ИС.

Назначение и принципы функционирования ИС во многом определяют существующие риски и требования безопасности, предъявляемые к системе. Поэтому на следующем этапе аудитора интересует информация о назначении и функционировании ИС. На данном этапе аудитор может использовать документацию, содержащую следующие данные:

* описание автоматизированных функций;
* схема информационных потоков;
* описание структуры комплекса технических средств информационной системы;
* описание структуры программного обеспечения;
* описание структуры информационного обеспечения;
* описание технических заданий используемых приложений;

Далее, аудитору требуется более детальная информация о структуре ИС. Это позволяет выяснить, каким образом осуществляется распределение механизмов безопасности по структурным элементам и уровням функционирования ИС.

Подготовка значительной части документации на ИС, обычно, осуществляется уже в процессе проведения аудита. Когда все необходимые данные по ИС, включая документацию, подготовлены, можно перейти к следующему этапу - их анализу.

Используемые аудиторами методы анализа данных определяются выбранными подходами к проведению аудита, которые могут существенно различаться. Но в общем, можно выделить 3 подхода:

*Первый подход*, самый сложный, базируется на анализе рисков. Опираясь на методы анализа рисков, аудитор определяет для обследуемой ИС индивидуальный набор требований безопасности, в наибольшей степени учитывающий особенности данной ИС, среды ее функционирования и существующие в данной среде угрозы безопасности. Данный подход является наиболее трудоемким и требует наивысшей квалификации аудитора. На качество результатов аудита, в этом случае, сильно влияет используемая методология анализа и управления рисками и ее применимость к данному типу ИС.

Если для проведения аудита безопасности выбран данный подход, то на этапе анализа данных аудита обычно выполняются следующие группы задач:

1. Анализ ресурсов ИС, включая информационные ресурсы, программные и технические средства, а также людские ресурсы.
2. Анализ групп задач, решаемых системой, и бизнес процессов.
3. Построение *(неформальной)* модели ресурсов ИС, определяющей взаимосвязи между информационными, программными, техническими и людскими ресурсами, их взаимное расположение и способы взаимодействия.
4. Оценка критичности информационных ресурсов.
5. Определение наиболее вероятных угроз безопасности в отношении ресурсов ИС и уязвимостей защиты, делающих возможным осуществление этих угроз.
6. Оценка вероятности осуществления угроз, величины уязвимостей и ущерба, наносимого организации в случае успешного осуществления угроз.
7. Определение величины рисков для каждой тройки: угроза – группа ресурсов – уязвимость.

Перечисленный набор задач, является достаточно общим. Для их решения могут использоваться различные формальные и неформальные, количественные и качественные, ручные и автоматизированные методики анализа рисков. Суть подхода от этого не меняется.

Оценка рисков может даваться с использованием различных как качественных, так и количественных шкал. Главное, чтобы существующие риски были правильно идентифицированы и ранжированы в соответствии со степенью их критичности для организации. На основе такого анализа может быть разработана система первоочередных мероприятий по уменьшению величины рисков до приемлемого уровня.

*Второй подход*, самый практичный, опирается на использование стандартов информационной безопасности. Стандарты определяют базовый набор требований безопасности для широкого класса ИС, который формируется в результате обобщения мировой практики. Стандарты могут определять разные наборы требований безопасности, в зависимости от уровня защищенности ИС, который требуется обеспечить, ее принадлежности *(коммерческая организация, либо государственное учреждение)*, а также назначения *(финансы, промышленности, связь и т.п.)*. От аудитора в данном случае требуется правильно определить набор требований стандарта, соответствие которым требуется обеспечить для данной ИС. Из-за своей простоты *(стандартный набор требований для проведения аудита уже заранее определен стандартом)* и надежности, описанный подход наиболее распространен на практике *(особенно при проведении внешнего аудита)*. Этот подход позволяет при минимальных затратах ресурсов делать обоснованные выводы о состоянии ИС.

В случае проведения аудита безопасности согласно данного подхода, аудитор оценивает применимость требований стандарта к обследуемой ИС и ее соответствие требованиям стандарта. Основываясь на данных о соответствии различных областей функционирования ИС требованиям стандарта, определяется, какие требования безопасности в системе не реализованы. Исходя из этого, делаются выводы о соответствии обследуемой ИС требованиям принятого на предприятии стандарта и даются рекомендации по реализации в системе механизмов безопасности, позволяющих обеспечить такое соответствие.

*Третий подход*, наиболее эффективный, предполагает комбинирование первых двух. Базовый набор требований безопасности, предъявляемых к ИС, определяется выбранным стандартом. Дополнительные требования, в максимальной степени учитывающие особенности функционирования данной ИС, формируются на основе анализа рисков. Этот подход является намного проще первого, т.к. большая часть требований безопасности уже определена стандартом, и, в то же время, он лишен недостатка второго подхода, заключающего в том, что требования стандарта могут не учитывать специфики обследуемой ИС.

### Выработка рекомендаций

Предпоследним этапом аудита информационной безопасности является выработка рекомендаций, выдаваемых аудитором по результатам анализа состояния ИС, определенных используемым подходом, особенностями обследуемой ИС, состоянием дел с информационной безопасностью и степенью детализации, используемой при проведении аудита.

В любом случае, рекомендации аудитора должны быть конкретными и применимыми к данной ИС, экономически обоснованными, аргументированными *(подкрепленными результатами анализа)* и отсортированными по степени важности. При этом мероприятия по обеспечению защиты организационного уровня практически всегда имеют приоритет над конкретными программно-техническими методами защиты.

### Подготовка отчетных документов

Рекомендации аудитора, как правило, оформляются соответствующими документами *(завершающий этап)*. Аудиторский отчет является основным результатом проведения аудита. Его качество характеризует качество работы аудитора. Структура отчета может существенно различаться в зависимости от характера и целей проводимого аудита, однако определенные разделы должны обязательно присутствовать в аудиторском отчете. Он должен содержать:

* описание целей проведения аудита;
* характеристику обследуемой ИС;
* границы проведения аудита и используемых методов;
* результаты анализа данных аудита;
* выводы, обобщающие результаты анализа данных аудита и содержащие оценку уровня защищенности ИС или соответствие ее требованиям стандартов;
* рекомендации аудитора по устранению существующих недостатков и совершенствованию системы защиты.

**Список литературы:**

1. Конфидент «Аудит информационной безопасности», № 4, 2003
2. www.dsec.ru
3. www.usp~compulink.ru