При существовании повышенных требований к информационной безопасности, наиболее приемлемым является третий подход к аудиторскому исследованию. В данном случае аудитору наряду с базовыми требованиями стандартов необходимо надлежащим образом исследовать:

- бизнес- и ИТ-процессы с позиции информационной безопасности;
- ресурсы аудируемого субъекта и их ценность;
- существующие и потенциальные угрозы информационной безопасности;
- уязвимости, т.е. слабые места в существующей у субъекта защите информации.

Все ресурсы необходимо исследовать с позиции оценки угроз, то есть воздействия вероятных или спланированных действий внутренних или внешних злоумышленников, а также различных нежелательных событий естественного происхождения.

Ценность (важность) ресурса, как правило, определяется масштабами ущерба, наносимого в случае нарушения информационной безопасности. На практике обычно рассматривают следующие виды ущерба:

- данные были изменены, удалены или стали недоступны;
- аппаратно-программные средства были разрушены или повреждены;
- нарушена целостность программного обеспечения и пр.

Осуществляя аудиторское исследование информационной безопасности аудитору необходимо выяснить, может ли быть нанесен ущерб аудируемому субъекту в результате успешного прохождения следующих видов угроз:

- удаленные или локальные атаки на ИТ-ресурсы;
- стихийные бедствия;
- ошибки, искажения или преднамеренные действия ИТ персонала;
- сбои в работе информационных технологий, вызванные в программном обеспечении или неисправностями аппаратных средств.

Сама оценка рисков может быть дана с использованием как качественных, так и количественных шкал. Аудитору необходимо правильно их идентифицировать и про ранжировать в соответствии со степенью их критичности для конкретного аудируемого субъекта. На основе проведенного исследования и оценки рисков вырабатываются адекватные им мероприятия (контрмеры) по их снижению до приемлемого уровня. В каждом конкретном случае рекомендации должны быть конкретными и применимыми к исследуемой информационной системе. Кроме того, рекомендации необходимо обосновать экономически. Следует помнить, что контрмеры по защите организационного уровня должны иметь приоритет перед аппаратно-программными методами защиты. Обязательной составляющей цикла аудита информационной безопасности является периодическая проверка соответствия реализованного по результатам аудирования режима безопасности политике безопасности и на соответствие установленным критериям.

Логическим завершением любого цикла аудиторского исследования информационных систем является подготовка и предоставление заинтересованным пользователям отчета о проделанной работе и надлежащим образом обоснованных рекомендаций. С этой целью аудитор должен всесторонне

изучить и оценить выводы, сделанные на основе проведенного исследования. Структура отчета, как правило, не регламентирована.

4.5. Аудит состояния информационной инфраструктуры

Современный этап формирования рыночных отношений, как уже неоднократно отмечалось ранее, характеризуется широким разнообразием форм собственности, диверсификацией практически всех отраслей экономики, высокой неопределенностью и все возрастающей динамикой постоянных изменений, как во внешнем окружении экономических субъектов (бизнес-систем), так и внутри самих этих субъектов. Современные бизнес-системы с развитием их внешнего окружения становятся все более сложными образованиями. При этом усложняется сама структура управления ими, а обработка и передача надлежащей информации становится существенной частью их бизнес-процессов.

В настоящее время информационные технологии являются одним из основных инструментов обеспечения адаптивности и конкурентоспособности экономических субъектов. По мере изменения требований их внешнего окружения меняются требования, предъявляемые к программным продуктам и ИТ-сервисам (ИТ-услугам), что приводит к добавлению в их информационную инфраструктуру все новых и новых программно-аппаратных платформ. При этом все возрастающая их сложность и разнородность оказывают влияние на управляемость всей информационной системой, стабильность и эффективность ее работы.

Под информационной инфраструктурой в данном контексте следует понимать отлаженную систему, выполняющую функции обслуживания, документирования, учета, контроля и анализа всех процессов, происходящих с информационными потоками хозяйствующего субъекта. Иными словами, инфраструктура - это технология и устройства (например, аппаратное обеспечение, операционные системы, системы управления базами данных, сетевое оборудование, мульти-медиа, а также та среда, в которой все это находится и поддерживается), которые обеспечивают работу приложений.

Под информационной технологией понимают «систему правил, определяющих способы сбора, накопления, регистрации, передачи, обработки, хранения, поиска, модификации, анализа, защиты, выдачи необходимой информации всем заинтересованным подразделениям или отдельным пользователям.

Потребность в уверенности относительно полезности, которую дают информационные системы, управление связанными с ними рисками и растущие требования к контролю над информацией в настоящее время считаются ключевыми элементами корпоративного управления. Ценность, риск и контроль определяют суть корпоративного управления информационной системой.

Аудит в современных условиях является практически незаменимым инструментарием при осуществлении разностороннего исследования и оценки информационной инфраструктуры, принятия управленческих решений, прогнозировании развития всей бизнес-системы и ее информационной системы в частности, а также инструментом поддержки управления этими системами. При этом следует учитывать, что информационная система и ее информационная

инфраструктура, являясь по своей сути моделью бизнес-системы, в которой она функционирует, весьма сложное и многофункциональное образование, требующее особого, кропотливого и комплексного подхода к аудиторскому исследованию их состояния. Аудиторское исследование информационной инфраструктуры, основанное на методологии стандарта Cobit, позволяет получить наиболее полную, систематизированную и достоверную информацию о ее текущем состоянии.

Однако прежде чем приступить к реализации процесса аудита состояния информационной инфраструктуры и информационной системы в целом, необходимо тщательным образом провести инвентаризацию аппаратных и программных средств.

В этой связи аудитор должен обследовать и собрать сведения:

- о компьютерной технике и периферийных устройствах;
- серверах;
- сетевом оборудовании;
- оргтехнике;
- системах автоматизации бизнес-процессов;
- системах безопасности (видеонаблюдение, охранно-пожарная сигнализация и пр.);
- коммуникационных системах (мини-АТС, локальных и / или корпоративных сетях);
- системе электроснабжения;
- каналах передачи данных и пр.

Инвентарную базу следует формировать в виде рабочих документов (например, с использованием формата Мкгозоп Excel). При этом в указанных документах необходимо отразить:

- условно неделимый элемент инфраструктуры (АРМ, сервер и пр.), под которым следует понимать его неделимость без вмешательства системного администратора;
- тип оборудования (настольный компьютер, ноутбук, оргтехника, комплектующие персональных компьютеров, периферийные устройства, сервер, сетевое оборудование и пр.);
- ответственного пользователя, под которым в данном контексте понимается сотрудник аудируемого субъекта, использующий конкретное средство;
- описание, раскрывающее детальную характеристику и классификацию системного элемента информационной инфраструктуры (жесткий диск, внешний диск, видеокарта, маршрутизатор, материнская плата, оперативная память, монитор, блок питания и пр.);
- модель системного элемента информационной инфраструктуры;
- число системных элементов;
- расположение элемента:
- статус оборудования (исправный, неисправный, к списанию).

Аналогичным образом осуществляется и инвентаризация сетевого оборудовании. При формировании функциональной схемы сети аудитор должен исследовать функции информационной системы, а также проанализировать схему помещений, в которых расположено активное и пассивное сетевое оборудование. Кроме того,

аудитору необходимо получить информацию обо всех замечаниях о работе этого оборудования.

Осуществляя инвентаризацию установленного на рабочих станциях программного обеспечения, аудитор должен получить надлежащую и достаточную информацию о наиболее часто используемых программных продуктах. С этой целью аудитору необходимо осуществить опросы сотрудников, являющихся их непосредственными пользователями. Кроме того, необходимо осуществить анализ лицензионных соглашений с производителями всего программного обеспечения используемого информационной системой аудируемого субъекта.

Проводя инспектирование работы телефонной связи и схемы обработки телефонных вызовов, аудитору необходимо выявить ее слабые места.

На основе данных проведенной инвентаризации аудитору необходимо осуществить детальное исследование текущего состояния всех элементов информационной инфраструктуры.

Учитывая требования и рекомендации стандарта СоЫ1 при исследовании текущего состояния информационной инфраструктуры в целом и ее составляющих элементов (например, аппаратно-программных средств и пр.) наиболее приемлемым следует считать использование рекомендованных для этих целей моделей зрелости, предложенных Институтом проектирования и разработки программного обеспечения **(**Software Engineering Institute) по заказу Министерства обороны США для классификации и оценки проектов связанных с разработкой программного обеспечения и гарантированного соблюдения качества при выполнении этих проектов.