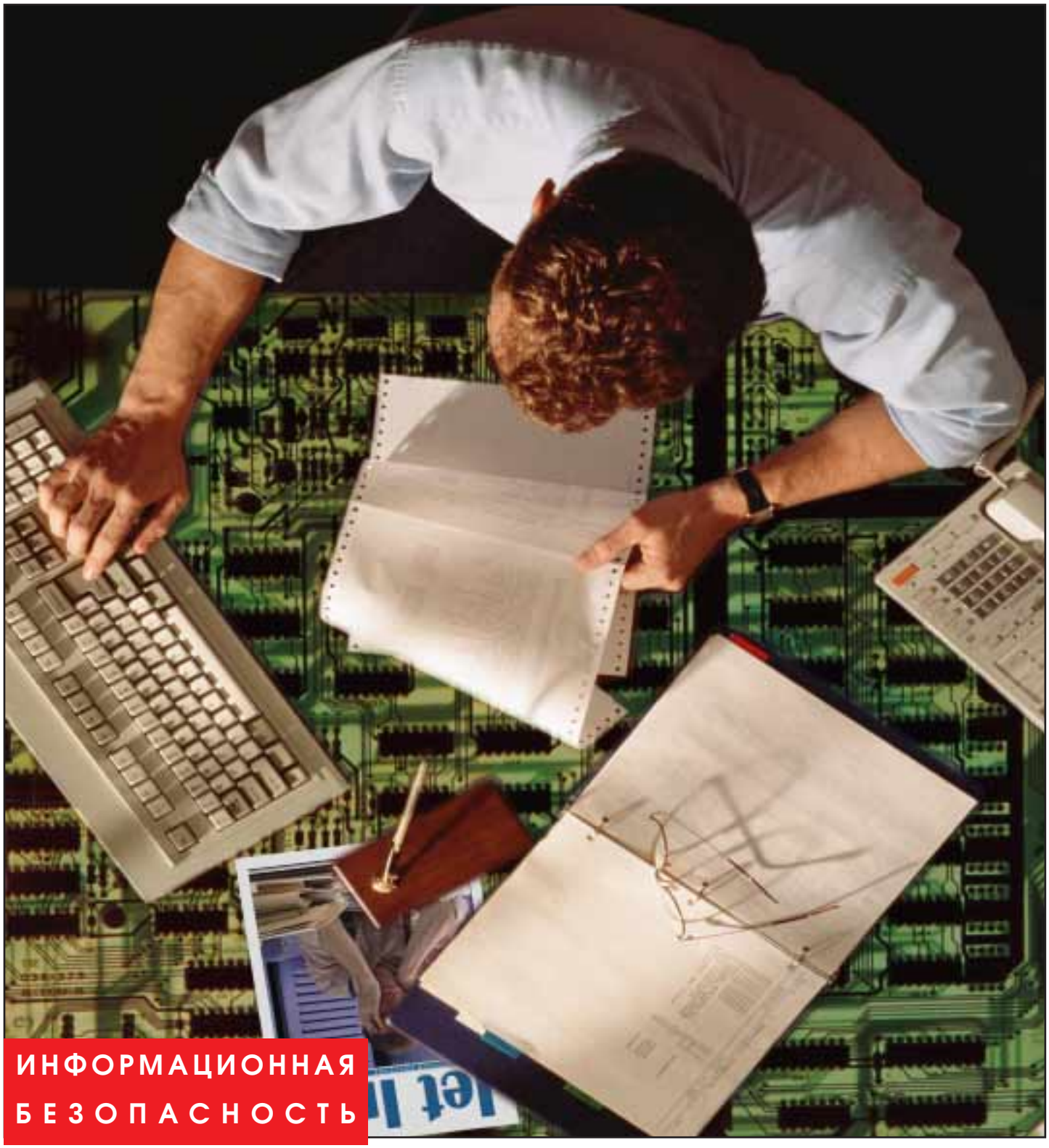
Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ № 10 (89)/2000



ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

СОДЕРЖАНИЕ НОМЕРА

Зачем проводить аудит информационных систем?

Гузик Сергей

Определение и задачи аудита

Под термином аудит Информационной Системы понимается системный процесс получения и оценки объективных данных о текущем состоянии ИС, действиях и событиях, происходящих в ней, устанавливающий уровень их соответствия определенному критерию и предоставляющий результаты заказчику.

В настоящее время актуальность аудита резко возросла, это связано с увеличением зависимости организаций от информации и ИС. Российский рынок насыщен аппаратно-программным обеспечением, многие организации в силу ряда причин (наиболее нейтральная из которых — это моральное старение оборудования и программного обеспечения) видят неадекватность ранее вложенных средств в информационные системы и ищут пути решения этой проблемы. Их может быть два: с одной стороны — это полная замена ИС, что влечет за собой большие капиталовложения, с другой — модернизация ИС. Последний вариант решения этой проблемы — менее дорогостоящий, но открывающий новые проблемы, например, что оставить из имеющихся аппаратно-программных средств, как обеспечить совместимость старых и новых элементов ИС.

Более существенная причина проведения аудита состоит в том, что при модернизации и внедрении новых технологий их потенциал полностью не реализуется. Аудит ИС позволяет добиться максимальной отдачи от средств, инвестируемых в создание и обслуживание ИС.

Кроме того возрасла уязвимость ИС за счет повышения сложности элементов этой ИС, увеличения строк кода программного обеспечения, новых технологий передачи и хранения данных.

Спектр угроз расширился. Это обусловлено следующими причинами:

- передача информации по сетям общего пользования;
- «информационная война» конкурирующих организаций;
- высокая (типичная для России) текучка кадров с низким уровнем порядочности.

По данным некоторых западных аналитических агенств до 95% попыток несанкционированного доступа к конфиденциальной информации происходит по инициативе бывших сотрудников организации.

Проведение аудита позволит оценить текущую безопасность функционирования ИС, оценить риски, прогнозировать и управлять их влиянием на бизнес-процессы организации, корректно и обоснованно подойти к вопросу обеспечения безопасности информационных активов организации, основные из которых:

- идеи;
- знания;
- проекты;
- результаты внутренних обследований.

В настоящее время многие системные интеграторы на Российском телекоммуникационном рынке декларируют поставку полного, законченного решения. К сожалению, в лучшем случае, все сводится к проектированию и поставке оборудования и программного обеспечения. Построение информационной инфраструктуры «остается за кадром» и к решению не прилагается. Оговоримся, что в данном случае под информационной инфраструктурой понимается отлаженная система, выполняющая функции обслуживания, контроля, учета, анализа, документирования всех процессов, происходящих в информационной системе.

Все чаще и чаще у клиентов к системным интеграторам, проектным организациям, поставщикам оборудования возникают вопросы следующего содержания:

- Что дальше? (Наличие стратегического плана развития организации, место и роль ИС в этом плане, прогнозирование проблемных ситуаций).
- Соответствует ли наша ИС целям и задачам бизнеса? Не превратился ли бизнес в придаток информационной системы?

- Как оптимизировать инвестиции в ИС?
- Что происходит внутри этого «черного ящика» — ИС организации?
- Сбои в работе ИС, как выявить и локализовать проблемы?
- Как решаются вопросы безопасности и контроля доступа?
- Подрядные организации провели поставку, монтаж, пуско-наладку. Как оценить их работу? Есть ли недостатки, если есть, то какие?
- Когда необходимо провести модернизацию оборудования и ПО? Как обосновать необходимость модернизации?
- Как установить единую систему управления и мониторинга ИС? Какие выгоды она предоставит?
- Руководитель организации, начальник отдела ОИТП должны иметь возможность получать достоверную информацию о текущем состоянии ИС в кратчайшие сроки. Возможно ли это?
- Почему все время производится закупка дополнительного оборудования?
- Сотрудники отдела ОИТП постоянно чему-либо учатся, есть ли в этом необходимость?
- Какие действия предпринимать в случае возникновения внештатной ситуации?
- Какие возникают риски при размещении конфиденциальной информации в ИС организации? Как минимизировать эти риски?
- Как снизить стоимость владения ИС?
- Как оптимально использовать сложившуюся ИС при развитии бизнеса?

На эти и другие подобные вопросы нельзя мгновенно дать однозначный ответ. Только рассматривая все проблемы в целом, взаимосвязи между ними, учитывая нюансы и недостатки можно получить достоверную, обоснованную информацию. Для этого в консалтинговых компаниях во всем мире существует определенная специфическая услуга — аудит Информационной Системы.

ISACA (Ассоциация аудита и контроля информационных систем)

Подход к проведению аудита ИС, как отдельной самостоятельной услуги, с течением времени упорядочился и стандартизировался. Крупные и средние аудиторские компании образовали ассоциации — союзы профессионалов в области аудита ИС, которые занимаются созданием и сопровождением стандартов аудиторской деятельности в сфере ИТ. Как правило, это закрытые стандарты, тщательно охраняемое «ноу-хау».

Однако, существует ассоциация ISACA, занимающаяся открытой стандартизацией аудита ИС.

Ассоциация ISACA основана в 1969 году и в настоящее время объединяет около 20 тысяч членов из более чем 100 стран, в том числе и России. Ассоциация координирует деятельность более чем 12 тыс. аудиторов информационных систем.

Основная декларируемая цель ассоциации — это исследование, разработка, публикация и продвижение стандартизованного набора документов по управлению информационной технологией для ежедневного использования администраторами и аудиторами информационных систем.

В помощь профессиональным аудиторам, руководителям ОИТП, администраторам и заинтересованным пользователям ассоциацией ISACA и привлеченными специалистами из ведущих мировых консалтинговых компаний был разработан стандарт CoBiT.

CoBiT (Контрольные Объекты Информационной Технологии)

CoBiT — **К**онтрольные **ОБ**ъекты **И**нформационной **Т**ехнологии — открытый стандарт, первое издание, которое в 1996 году было продано в 98 странах по всему миру и облегчило работу профессиональных аудиторов в сфере информационных технологий. Стандарт связывает информационные технологии и действия аудиторов, объединяет и согласовывает многие другие стандарты в единый ресурс, позволяющий авторитетно, на современном уровне получить представление и управлять целями и задачами, решаемыми ИС. CoBiT учитывает все особенности информационных систем любого масштаба и сложности.

Основополагающее правило, положенное в основу CoBiT, следующее: **ресурсы ИС должны управляться набором естественно сгруппированных процессов для обеспечения организации необходимой и надежной информацией** (рис. 1).

А теперь немного разъяснений по поводу того, какие ресурсы и критерии их оценки используются в стандарте CoBiT:

Трудовые ресурсы — под трудовыми ресурсами понимаются не только сотрудники организации, но также руководство организации и контрактный персонал. Рассматриваются навыки штата, понимание задач и производительность работы.

Приложения — прикладное программное обеспечение, используемое в работе организации.

Технологии — операционные системы, базы данных, системы управления и т.д.

Оборудование — все аппаратные средства ИС организации, с учетом их обслуживания.

Данные — данные в самом широком смысле — внешние и внутренние, структурированные и неструктурированные, графические, звуковые, мульти-медиа и т.д.

Все эти ресурсы оцениваются CoBiT на каждом из этапов построения или аудита ИС по следующим критериям:

- **Эффективность** – критерий, определяющий уместность и соответствие информации задачам бизнеса.
- **Технический уровень** – критерий соответствия стандартам и инструкциям.
- **Безопасность** – защита информации.
- **Целостность** – точность и законченность информации.
- **Пригодность** – доступность информации требуемым бизнес-процессам в настоящем и будущем. А также защита необходимых и сопутствующих ресурсов.
- **Согласованность** – исполнение законов, инструкций и договоренностей, влияющих на бизнес-процесс, то есть внешние требования к бизнесу.

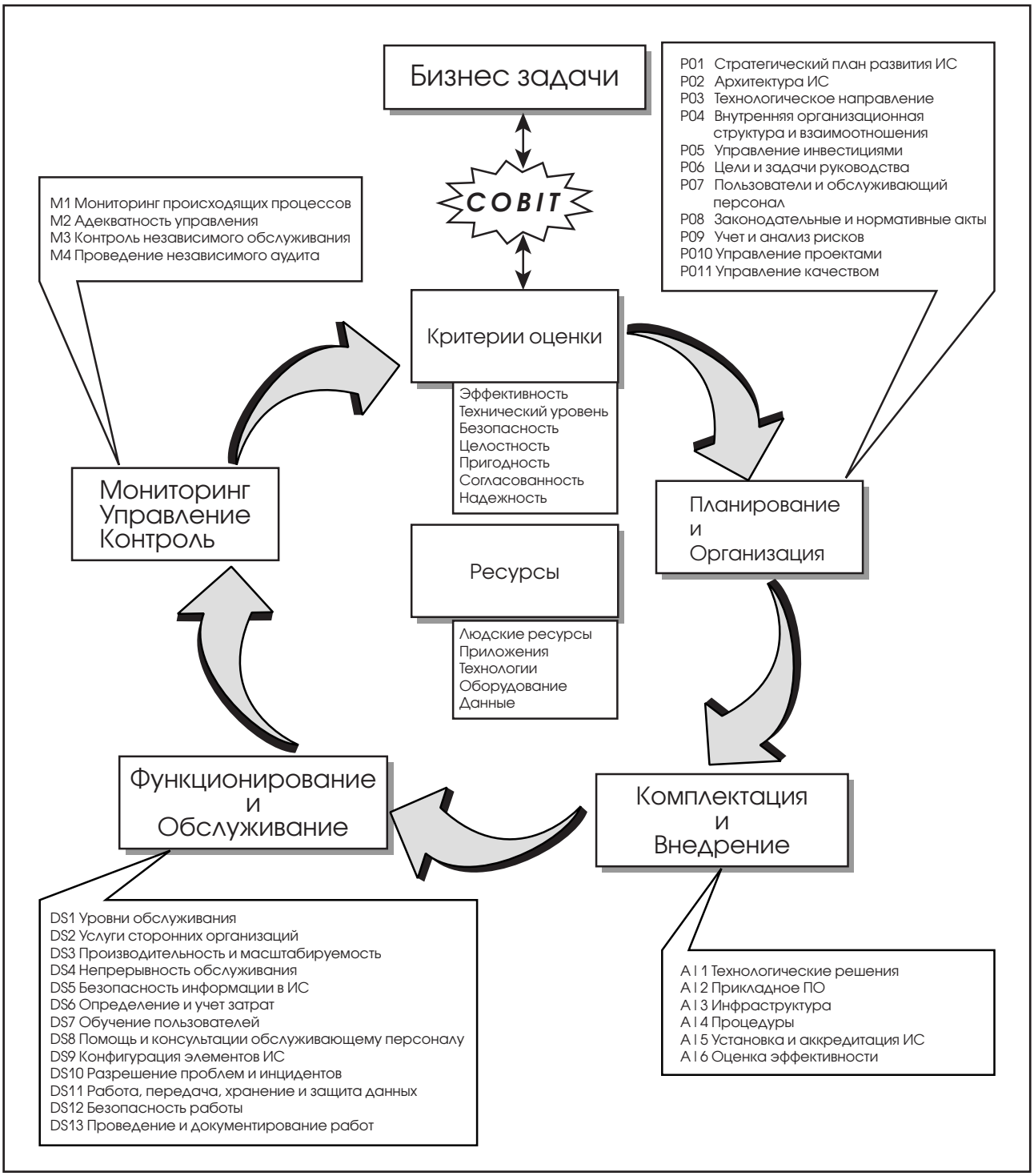


Рис. 1. Структура стандарта CoBIT.

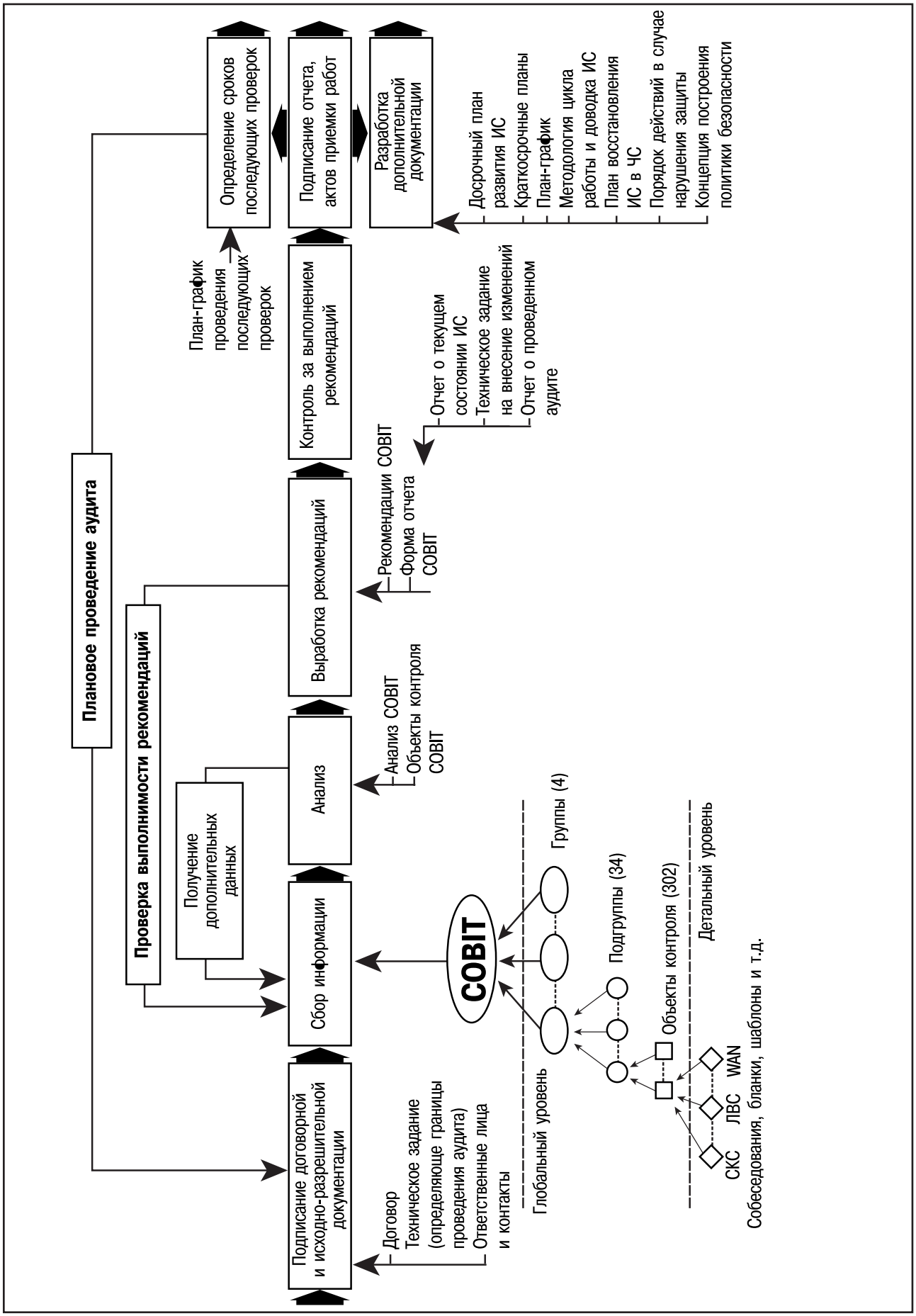


Рис. 2. Общая последовательность проведения аудита ИС

- **Надежность** – соответствие информации, предоставляемой руководству организации, осуществление соответствующего управления финансированием и согласованность должностных обязанностей.

CoBiT базируется на стандартах аудита ISA и ISACF, но включает и другие международные стандарты, в том числе принимает во внимание утвержденные ранее стандарты и нормативные документы:

- технические стандарты;
- кодексы;
- критерии ИС и описание процессов;
- профессиональные стандарты;
- требования и рекомендации;
- требования к банковским услугам, системам электронной торговли и производству.

Стандарт разработан и проанализирован сотрудниками соответствующих подразделений ведущих консалтинговых компаний и используется в их работе наряду с собственными разработками.

Применение стандарта CoBiT возможно как для проведения аудита ИС организации, так и для изначального проектирования ИС. Обычный вариант прямой и обратной задач. Если в первом случае – это соответствие текущего состояния ИС лучшей практике аналогичных организаций и предприятий, то в другом – изначально верный проект и, как следствие, по окончании проектирования – ИС, стремящаяся к идеалу. В дальнейшем мы будем рассматривать аудит ИС, подразумевая при этом, что на любом этапе возможно решение обратной задачи – проектирования ИС.

Несмотря на малый размер разработчики старались, чтобы стандарт был прагматичным и отвечал потребностям бизнеса, при этом сохраняя независимость от конкретных производителей, технологий и платформ.

На базовой блок-схеме CoBiT отражена последовательность, состав и взаимосвязь базовых групп. Бизнес-процессы (в верхней части схемы) предъявляют свои требования к ресурсам ИС, которые анализируются с использованием критериев оценки CoBiT на всех этапах построения и проведения аудита.

Четыре базовые группы (домена) содержат в себе тридцать четыре подгруппы, которые, в свою очередь состоят из трехсот двух объектов контроля. Объекты контроля предоставляют аудитору всю достоверную и актуальную информацию о текущем состоянии ИС.

Отличительные черты CoBiT:

1. Большая зона охвата (все задачи от стратегического планирования и основополагающих документов до анализа работы отдельных элементов ИС).
2. Перекрестный аудит (перекрывающиеся зоны проверки критически важных элементов).
3. Адаптируемый, наращиваемый стандарт.

Рассмотрим преимущества CoBiT перед многочисленными западными и отечественными разработками. Прежде всего, это его **достаточность** – наряду с возможностью относительно легкой адаптации к особенностям Российских ИС. И, конечно же, то, что стандарт легко **масштабируется** и **наращивается**. CoBiT позволяет использовать любые разработки производителей аппаратно-программного обеспечения и анализировать полученные данные не изменяя общие подходы и собственную структуру.

Практика проведения аудита ИС

Представленная на рис. 2 блок-схема отражает, хотя и не в деталях, ключевые точки проведения аудита ИС. Рассмотрим их подробнее.

На этапе подготовки и подписания исходно-разрешительной документации определяются границы проведения аудита:

1. Границы аудита определяются критическими точками ИС (элементами ИС), в которых наиболее часто возникают проблемные ситуации.
2. На основании результатов предварительного аудита всей ИС (в первом приближении) проводится углубленный аудит выявленных проблем.

В это же время создается команда проведения аудита, определяются ответственные лица со стороны Заказчика. Создается и согласовывается необходимая документация.

Далее проводится сбор информации о текущем состоянии ИС с применением стандарта CoBiT, объекты контроля которого получают информацию обо всех нюансах функционирования ИС как в двоичной форме (Да/Нет), так и форме развернутых отчетов. Детальность информации определяется на этапе разработки исходно-разрешительной документации. Существует определенный оптимум между затратами (временными, стоимостными и т.д.) на получение информации и ее важностью и актуальностью.

Проведение анализа – наиболее ответственная часть проведения аудита ИС. Использование при анализе недостоверных, устаревших данных недопустимо, поэтому необходимо уточнение данных, углубленный сбор информации. Требования к проведению анализа определяются на этапе сбора информации. Методики анализа информации существуют в стандарте CoBiT, но если их не хватает не возбраняется использовать разрешенные ISACA разработки других компаний.

Результаты проведенного анализа являются базой для выработки рекомендаций, которые после предварительного согласования с Заказчиком должны быть проверены на выполнимость и актуальность с учётом рисков внедрения.

Контроль выполнения рекомендаций — немаловажный этап, требующий непрерывного отслеживания представителями консалтинговой компании хода выполнения рекомендаций.

На этапе разработки дополнительной документации проводится работа, направленная на создание документов, отсутствие или недочеты в которых могут вызвать сбои в работе ИС. Например, отдельное углубленное рассмотрение вопросов обеспечения безопасности ИС.

Постоянное проведение аудита гарантирует стабильность функционирования ИС, поэтому создание план-графика проведения последующих проверок является одним из результатов профессионального аудита.

Результаты проведения аудита

Результаты аудита ИС организации можно разделить на три основных группы:

1. Организационные — планирование, управление, документооборот функционирования ИС.
2. Технические — сбои, неисправности, оптимизация работы элементов ИС, непрерывное обслуживание, создание инфраструктуры и т.д.
3. Методологические — подходы к решению проблемных ситуаций, управлению и контролю, общая упорядоченность и структуризация.

Проведенный аудит позволит обоснованно создать следующие документы:

- Долгосрочный план развития ИС.
- Политика безопасности ИС организации.
- Методология работы и доводки ИС организации.
- План восстановления ИС в чрезвычайной ситуации.

Список выгод проведения аудита более обширен, но, к сожалению, рамки обзорной статьи не позволяют предоставить подробное изложение положительных моментов, обоснование и скрытую взаимосвязь между ними.

Требования к представлению информации

Ассоциация ISACA разработала и приняла требования к представлению информации при проведении аудита. Применение стандарта CoBiT гарантирует соблюдение этих требований.

Основное требование — полезность информации. Чтобы информация была полезной, она должна обладать определенными характеристиками, среди которых:

1. **Понятность**. Информация должна быть понятной для пользователя, который обладает определенным уровнем знаний, что не означает, однако, исключения сложной информации, если она необходима.
2. **Уместность**. Информация является уместной или относящейся к делу, если она влияет на решения пользователей и помогает им оценивать прошлые, настоящие, будущие события или подтверждать и исправлять прошлые оценки. На уместность информации влияет ее **содержание** и **существенность**. Информация является существенной, если ее отсутствие или неправильная оценка могут повлиять на решение пользователя. Еще одна характеристика уместности — это **своевременность** информации, которая означает, что вся значимая информация своевременно, без задержки включена в отчет и такой отчет предоставлен вовремя. Неким аналогом принципа уместности в российской практике может служить требование **полноты отражения** операций за учетный период, хотя требование отражения всей информации не тождественно требованию отражения существенной информация.
3. **Достоверность, надежность**. Информация является достоверной, если она не содержит существенных ошибок или пристрастных оценок и правдиво отражает хозяйственную деятельность. Чтобы быть достоверной, информация должна удовлетворять следующим характеристикам:
   a) **правдивость**;
   b) **нейтральность** — информация не должна содержать однобоких оценок, то есть информация не должна предоставляться выборочно, с целью достижения определенного результата;
   c) **осмотрительность** — готовность к учету потенциальных убытков, а не потенциальных прибылей и как следствие — создание резервов. Такой подход уместен в состоянии неопределенности и не означает создание скрытых резервов или искажения информации;
   d) **достаточность информации** — включает такую характеристику, как требование полноты информации, как с точки зрения ее существенности, так и затрат на ее подготовку.

Потребность Российского рынка в данной услуге

При оценке необходимости проведения аудита ИС необходимо акцентировать внимание на следующих моментах (см. Табл. 1):

- сложности решаемых задач — постоянное увеличение, как количественное, так и качественное, задач, решаемых ИС;
- разветвленности ИС — сложность в обслуживании, территориальная распределенность;

Организационные	Технические	Методологические
Оценка стратегического планирования ИС, архитектуры, технологического направления	Понимание проблем, сбоев, узких мест информационной системы организации	Предоставление апробированных подходов к стратегическому планированию и прогнозированию
Общее управление ИС	Оценка технологических решений	Оптимизация документооборота ОИТП
Повышение конкурентоспособности организации	Оценка инфраструктуры	Повышение трудовой дисциплины
Проверка соответствия ИС задачам бизнеса	Комплексное решение вопросов безопасности	Обучение администраторов и пользователей ИС
Обоснование, управление и оценка инвестиций в ИС	Разработка путей решения проблем, минимизация затрат на решение проблемных ситуаций	Предоставление методов получения своевременной и объективной информации о текущем состоянии ИС организации
Снижение стоимости владения ИС	Профессиональный прогноз функционирования и необходимости модернизации ИС	
Управление качеством	Реализация всего потенциала новых технологий	
Управление проектами, выполняемыми в рамках ИС	Повышение эффективности функционирования информационной системы	
Управление рисками	Расширение функционала ИС	
Снижение затрат на обслуживание ИС	Оценка работы сторонних организаций	
	Определение уровней обслуживания ИС	

Табл. 1. Результаты проведения аудита.

- перспективности бизнеса — новые направления, рынки, условия работы;
- руководство организацией — умение и желание руководителей стратегически мыслить, видеть перспективы, открываемые стандартизованным подходом, основанные на передовом опыте.

Кто заинтересован в проведении аудита? Прежде всего, это коммерческие или бюджетные организации и предприятия для обоснования инвестиций в ИС, системные интеграторы, ИТ компании для оценки влияния ИС на основной бизнес-процесс и расширения спектра предлагаемых услуг.

Для компаний, проводящих финансовый аудит — аудит ИС, дополнительная услуга, которая способна повысить рейтинг компании на рынке.

Генеральным подрядчикам работ будет интересна возможность оценить работу субподрядчиков в сфере ИТ.

А также проведение аудита ИС по стандарту CoBiT будет интересно любым предприятиям и организациям, имеющим или планирующим создание ИС и которые заинтересованы в получении ответов на вопросы, приведенные во введении этой статьи.

Выводы

Во всем мире консалтинг в сфере аудита приобрел поистине всеобъемлющий размах — «ни одного серьезного дела без аудита». Но, несмотря на это, при изучении отчетов о проведении аудита ИС, в плане технической грамотности и содержательности рекомендаций выяснилось, что уровень предлагаемых заказчикам отчетов довольно низок. Это объясняется одной немаловажной причиной: подавляющее большинство западных аудиторских компаний, предлагающих свои услуги, в том числе в сфере ИТ, выросли из финансового аудита и приглашают технических специалистов лишь по мере надобности.

Здесь изначально и заложено преимущество Российских компаний — системных интеграторов: наличие высококвалифицированных специалистов с огромным практическим опытом в различных сферах телекоммуникационного рынка позволяет им проводить аудит ИС как отдельную специфическую услугу, без существенных изменений в организационной структуре. В случае, если эти организации возьмут на вооружение профессиональный стандарт с апробированной и отлаженной структурой, то профессионализм подобных услуг резко возрастет.

СКАНЕР ЗАЩИЩЕННОСТИ NESSUS:
уникальное предложение на российском рынке

Успех ведения бизнеса напрямую связан с технологией обработки информации, поэтому все большую ценность для любой компании приобретают ее информационно-вычислительные ресурсы. Вопрос защиты как своей информации, так и информационной системы в целом становится все более актуальным.

Практически все корпоративные информационные системы в той или иной мере уязвимы для внешних и внутренних атак. В ряде случаев пользователи даже не подозревают о том, что в их компьютерной сети содержатся уязвимости, позволяющие злоумышленнику несанкционированно проникать в информационную систему. Реальное представление о недостатках защиты корпоративной сети пользователи получают уже после совершенных взломов, кражи конфиденциальной информации или вывода из строя сетевых сервисов.

Для построения подсистемы информационной защиты необходимо определить ресурсы, которые могут подвергаться различного рода атакам как со стороны собственных сотрудников, так и со стороны внешних злоумышленников.

Для предупреждения возможных атак на корпоративные информационные системы используются специализированные продукты, называемые сканерами защищенности.

Принцип работы сетевых сканеров защищенности заключается в поиске доступных ресурсов в сети, идентификации сетевых сервисов, анализе на предмет их уязвимостей и выдаче подробной информации по состоянию защищенности обследованной системы.

Коммерческие релизы сканеров защищенности, поставляемые в нашу страну зарубежными производителями, являются достаточно качественными, надежными и функциональными решениями. Однако, широкому их распространению на внутрироссийском рынке препятствует высокая цена.

Исследования, проведенные компанией «Инфосистемы Джет», позволили сделать вывод, что многие из свободно распространяемых программных продуктов не уступают по техническим характеристикам их коммерческим аналогам. В частности такая ситуация сложилась на рынке сканеров защищенности.

К свободно распространяемым продуктам данного класса относится сканер защищенности Nessus.

Сканер защищенности Nessus

Программный комплекс Nessus является мощным и надежным средством семейства сетевых сканеров. Данное средство позволяет осуществлять поиск уязвимостей в сетевых сервисах, предоставляемых операционными системами, межсетевыми экранами, фильтрующими маршрутизаторами и другими сетевыми компонентами информационной системы. Для поиска уязвимостей используются как стандартные средства тестирования, так и специальные средства, эмулирующие действия злоумышленника по проникновению в системы, подключенные к сети.

По своим функциональным возможностям сканер защищенности Nessus находится в одном ряду, а по некоторым параметрам и превосходит такие широко известные продукты как Internet Scanner компании Internet Security Systems (ISS) и CyberCop Scanner компании Network Associates (NAI).

Отвечая всем необходимым требованиям, предъявляемым к продуктам данного класса (широкий набор категорий проверок, клиент-серверная архитектура, возможность работы под управлением различных операционных систем, удобный графический интерфейс, позволяющий определять параметры анализа, наблюдать за ходом сканирования, создавать и просматривать отчеты), сканер защищенности Nessus имеет следующие исключительные особенности:

- бесплатно распространяемый программный продукт;
- ежедневно пополняемая база данных уязвимостей;
- интеллектуальный подход к распознаванию сканируемых сервисов (поиск сервисов на нестандартных портах, возможность сканирования двух и более одинаковых сервисов, запущенных на нескольких портах одного сетевого устройства);
- кодирование обмена данными между клиентом и сервером.

Продукт содержит как встроенные прототипы вариантов атак, так и подключаемые дополнения (plagins), количество которых постоянно увеличивается.

В отличие от большинства существующих сканеров безопасности, в процессе анализа Nessus не делает никаких априорных предположений о характере функционирования сервисов (в том числе относительно версий соответствующего обеспече-

ГОСУДАРСТВЕННАЯ ТЕХНИЧЕСКАЯ КОМИССИЯ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

**СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ
ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00**

С Е Р Т И Ф И К А Т
№ 361

Выдан 18 сентября 2000 г.
Действителен до 18 сентября 2003 г.

Настоящий сертификат удостоверяет, что программный комплекс **«Сетевой сканер безопасности «Nessus»** (партия из 400 изделий, маркированных специальными защитными знаками с номерами с А 014597 по А 014996), является средством контроля защищенности сетей с TCP/IP-протоколом от несанкционированного доступа к информации, не содержащей сведений, составляющих государственную тайну, и соответствует требованиям Руководящего документа Гостехкомиссии России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля недекларированных возможностей» по **4** уровню контроля и технических условий ДЖЕТ.НЕССУС.2000.ТУ.

Действие настоящего сертификата не распространяется на модули программы «Клиент Nessus (версия 0.99.9.1)».

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией «Центр безопасности информации» (аттестат аккредитации от 23.05.97 г. № СЗИ RU.117.Б08.025) – протокол испытаний от 13.09.2000 г., и экспертного заключения Гостехкомиссии России от 18.09.2000 г.

Заявитель – АОЗТ «Инфосистемы Джет».
Адрес - 103006, Москва, ул.Краснопролетарская, д.6.
Тел. - (095) 973-48-48.

Маркирование специальными защитными знаками сертифицированной продукции и инспекционный контроль соответствия сертифицированных изделий требованиям нормативных документов Гостехкомиссии России и техническим условиям осуществляется испытательной лабораторией «Центр безопасности информации».

ЗАМЕСТИТЕЛЬ ПРЕДСЕДАТЕЛЯ ГОСТЕХКОМИССИИ РОССИИ

А.Е. Гапонов

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации 18 сентября 2000 г.

ния портов, контролируемых сервисами и т.д.), а напротив опознает их и тестирует их безопасность.

Модульность архитектуры сканера обеспечивает необходимую гибкость в процессе его использования.

Клиент и сервер Nessus

Программный продукт Nessus состоит из клиентской (nessus) и серверной (nessusd), устанавливаемых на проверяемый объект, частей. Сервер nessusd предназначен для анализа защищенности сети от сетевых угроз, путем осуществления тестовых попыток несанкционированного доступа с использованием уязвимостей или брешей тех или иных сервисов в защите операционной системы. Сервер можно установить только на Unix-подобную операционную систему — Linux, FreeBSD, Solaris.

С целью повышения безопасности функционирования сканера обмен данными между клиентом и сервером кодируется. Каждый тип атак, выполняемых сервером, реализуется с помощью различных внешних подключаемых модулей.

Для того, чтобы исключить использование сканера неавторизованными пользователями, системный администратор имеет возможность настройки сервера nessusd.

Клиентская часть обеспечения Nessus предоставляет интерфейс пользователя. Клиент nessus использует набор программных средств GTK (the Gimp ToolKit). Клиенты, помимо Unix версий, существуют для Windows 9x, NT, а также имеется клиент в java исполнении.

Число атак, отслеживаемых с помощью сканера Nessus, постоянно увеличивается. Новые внешние модули, эмулирующие атаки, можно инсталлировать, скопировав файлы, содержащие их исходные тексты, с Web-сервера разработчиков.

Nessus – в массы. Предложение компании «Инфосистемы Джет»

Понимая исключительную актуальность задач, связанных с повышением безопасности информационных систем, и рассматривая анализ защищенности в качестве первого шага в направлении этого решения, компания «Инфосистемы Джет» предлагает бесплатный сертифицированный сканер защищенности Nessus. Компания «Инфосистемы Джет» рекомендует этот продукт предприятиям разного масштаба — от небольших офисов до крупных предприятий с развитой сетевой инфраструктурой.

Получая сетевой сканер защищенности Nessus вы получаете первый сертифицированный Гостехкомиссией России свободно распространяемый продукт, единственный в своем классе. Это предложение особенно интересно для крупных корпоративных клиентов, наличие сертификата на соответствующие продукты для которых является необходимостью.

Не все пользователи могут убедить руководство своих организаций в том, что процесс обеспечения ИБ требует определенных вложений. Данный продукт, сертифицированный на соответствие Техническим условиям ДЖЕТ.НЕССУС.2000.ТУ, поставляется бесплатно. С содержанием Технических условий можно ознакомиться направив соответствующий запрос в адрес компании.

Предоставляемый продукт является комплектным, т.е. помимо исходного и откомпилированного программного кода в поставку включена техническая документация на русском языке, необходимая для установки, запуска в эксплуатацию, администрирования и использования программного обеспечения.

Если потребуется помощь в проведении работ по установке и технической поддержке продукта, компания «Инфосистемы Джет» готова предоставить свои услуги для клиентов и предлагает следующие варианты сопровождения.

Первый вариант «стандартный» включает:

- обучение специалистов;
- ответы на вопросы, полученные по почте;
- предоставление обновленной базы уязвимостей с комментариями.

В «расширенный» вариант, дополнительно включены следующие мероприятия:

- визит специалиста компании «Инфосистемы Джет» к клиенту, в течении которого по согласованной программе могут быть проведены работы по инсталляции Nessus, тренинг, интерпретация результатов сканирования и выдача рекомендаций;
- телефонные консультации.

Кроме того на основании результатов сканирования и, возможно, проведя дополнительный аудит информационной системы клиента, специалисты компании могут не только выдать рекомендации, но разработать и реализовать проект по обеспечению защиты его информационных ресурсов.

Данное предложение вступило в силу с 19.09.2000 года.

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ
Издается с 1995 года
Издатель: компания Джет Инфо Паблишер

Главный редактор: Дмитриев В.Ю. *(vlad@jet.msk.su)*
Технический редактор: Антонов А.Н. *(silver@jet.msk.su)*
Россия, 103006, Москва, Краснопролетарская, 6
тел. (095) 972 11 82, 972 13 32
факс (095) 972 07 91
email: JetInfo@jet.msk.su
http://www.jetinfo.ru

Подписной индекс по каталогу Роспечати 32555