Контроль целостности и управление СЗИ

В этой главе

- *Контроль за работой пользователей*
- *Управление доступом к рабочим местам в ИС*
- *Использование паролей*
- *Управление доступом к сервисам*
- *Защита целостности данных и программ от вредоносного программного обеспечения*
- *Контроль за состоянием безопасности ИС*
- *Системы обнаружение атак*
- *Как работает сканер безопасности?*
- *Консалтинг в информационной безопасности*

<<< Этапы	Направления >>>	010				020				030				040				050			
		Защита объектов ИС				Защита процессов и программ				Защита каналов связи				ПЭМИН				Управление системой защиты			
	Основы >>>	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства
		011	012	013	014	021	022	023	024	031	032	033	034	041	042	043	044	051	052	053	054
100	Определение информации, подлежащей защите	111	112	113	114	121	122	123	124	131	132	133	134	141	142	143	144	151	152	153	154
200	Выявление угроз и каналов утечки информации	211	212	213	214	221	222	223	224	231	232	233	234	241	242	243	244	251	252	253	254
300	Проведение оценки уязвимости и рисков	311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344	351	352	353	354
400	Определение требований к СЗИ	411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444	451	452	453	454
500	Осуществление выбора средств защиты	511	512	513	514	521	522	523	524	531	532	533	534	541	542	543	544	551	552	553	554
600	Внедрение и использование выбранных мер и средств	611	612	613	614	621	622	623	624	631	632	633	634	641	642	643	644	651	652	653	654
700	Контроль целостности и управление защитой	711	712	713	714	721	722	723	724	731	732	733	734	741	742	743	744	751	752	753	754

Контроль за работой пользователей (700)

Управление защитой...

Пользователи должны знать свои обязанности по обеспечению контроля доступа, особенно — использования паролей. Доступ пользователя к ресурсам ИС должен предоставляться в соответствии с политикой управления доступом. В частности, рекомендуется предоставить пользователям только прямой доступ к сервисам, использование которых им разрешено. Особое внимание администраторам безопасности следует уделять контролю сетевых подключений к конфиденциальным или критически важным приложениям, а также контролю за работой пользователей в зонах повышенного риска, например в общедоступных местах или местах, находящихся вне организации.

Управление доступом к рабочим местам в ИС (750)

Доступ к рабочим местам в ИС следует предоставлять только зарегистрированным пользователям. ***Системы управления доступом должны обеспечивать:***

- идентификацию и аутентификацию пользователей, а также при необходимости терминала и местонахождение каждого зарегистрированного пользователя;
- ведение журнала учета попыток доступа (успешных и неудачных) к ИС;
- по необходимости ограничивать подключение пользователей в неурочное время.

Организация доступа для работы в ИС (750)

На этапе подготовительной работы по организация доступа в ИС рекомендуется рассмотреть следующие вопросы.

Регистрация пользователей (750)

Должны существовать документы с описанием доступных пользователю сервисов, допустимых правил работы в ИС и правил обеспечения режима ЗИ. Сервисы ИС должны не предоставлять доступ, пока не будут закончены процедуры определения полномочий. ***Для управления доступом к многопользовательским сервисам должна быть разработана процедура регистрации пользователей. Эта процедура должна:***

- проверять, предоставлено ли пользователю разрешение на использование сервиса ответственным за его использование;
- вести учет всех зарегистрированных лиц, использующих ИС;
- проверять, достаточен ли уровень доступа пользователя к системе и не противоречит ли он политике безопасности, принятой в организации, например, не компрометирует ли он принцип разделения обязанностей;
- своевременно аннулировать права доступа у пользователей, покинувших организацию;
- периодически проверять и удалять устаревшие идентификаторы и учетные записи.

Управление привилегиями (750)

Использование специальных привилегий следует ограничить и контролировать, поскольку это один из основных факторов, способствующих нарушению режима ЗИ. ***В многопользовательских ИС должна существовать система контроля предоставления привилегий. При организации такой системы рекомендуется:***

- идентифицировать привилегии, связанные с каждым программным продуктом или сервисом, поддерживаемым системой, а также категории сотрудников, которым их необходимо предоставить;
- предоставлять привилегии отдельным лицам только в случае крайней необходимости и в зависимости от ситуации, т.е. только когда они необходимы для выполнения ими своих функций;.
- реализовать автоматический процесс определения полномочий и вести учет всех предоставленных привилегий;
- по возможности использовать системные программы, для которых нет необходимости предоставлять специальные привилегии пользователям;
- пользователи, имеющие большие привилегии для специальных целей, должны для обычной работы использовать другой пользовательский идентификатор.

Управление пользовательскими паролями (750)

Назначение паролей необходимо контролировать. ***Примерные требования к системе контроля таковы:***

- обязать пользователей хранить в секрете персональные пароли и пароли рабочих групп;
- когда пользователи должны сами выбирать свои пароли, выдать им надежные временные пароли. Временные пароли выдаются также в случае, когда пользователи забывают свои пароли;
- передавать временные пароли пользователям надежным способом. Избегать передачи паролей через посредников или посредством незащищенных (незашифрованных) сообщений электронной почты. Пользователь должен подтвердить получение пароля.

Пересмотр прав доступа пользователей (750)

Пересмотр прав доступа пользователей...

Для обеспечения эффективного контроля за соблюдением режима ЗИ, необходимо организовать процесс пересмотра прав доступа пользователей через регулярные промежутки времени. Такой процесс должен обеспечивать:

- пересмотр полномочий доступа пользователей через регулярные промежутки времени (6 месяцев);
- пересмотр разрешения на предоставление специальных привилегий через более короткие промежутки времени (3 месяца).

Использование паролей (750)

Пользователи должны следовать установленным процедурам поддержания режима ЗИ при выборе и использовании паролей. ***Предлагаются следующие рекомендации:***

- выбирать пароли, содержащие не менее шести символов;
- при этом не следует использовать:
  - название месяцев года, дней недели;
  - фамилии, инициалы, регистрационные номера автомобилей;
  - названия и идентификаторы организаций;
  - номера телефонов или группы символов, состоящие только из цифр или только из букв;
  - более двух одинаковых символов, следующих один за другим;
  - группы символов, состоящие только из цифр;
  - изменять пароли через регулярные промежутки времени (месяц) и избегать повторного или "циклического" использования старых паролей;
  - чаще менять пароли для привилегированных системных ресурсов (к системным утилитам);
  - менять временные пароли при первом входе в системы;
  - не включать пароли в процедуры автоматического входа в системы (макросы, функциональные клавиши);
  - не допускать использования одного пароля несколькими пользователями;
  - обеспечивать хранение паролей в секрете;
  - менять пароли, когда есть указания на возможную компрометацию их;
  - использовать один надежный пароль, если необходим доступ к нескольким сервисам, защищенным паролями.

Пользовательское оборудование, оставленное без присмотра (750)

Пользователи должны обеспечить надлежащую защиту оборудования, оставленного без присмотра. Оборудование, установленное на рабочих местах пользователей (рабочие станции или файловые серверы) может потребовать организации защиты от несанкционированного доступа.

Пользователи должны знать процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

Рекомендуется:

- завершить сеансы связи по окончании работы, если их нельзя защитить посредством соответствующей блокировки;
- использовать логическое отключение от серверов по окончании сеанса связи. Не ограничиваться выключением ПК или терминала;

• защитить не используемые ПК или терминалы путем блокировки ключом или других средства контроля доступа.

Отслеживание времени простоя терминалов (750)

Для бездействующих терминалов в зонах с повышенным риском нарушения ЗИ (в общедоступных местах или вне пределов досягаемости) необходимо установить допустимое время простоя для предотвращения доступа незарегистрированных пользователей. По истечении этого времени экран терминала должен очищаться, а сеансы связи с приложениями и сетевыми сервисами завершаться. Допустимое время простоя должно задаваться исходя из анализа риска несанкционированного доступа к пользовательскому терминалу.

Ограничение периода подключения (750)

Дополнительную защиту сервисов от НСД можно обеспечить посредством ограничения допустимого периода подключения. Ограничение разрешаемого периода подключения терминала к ИС позволяет уменьшить вероятность НСД к ресурсам ИС. Возможность применения такого средства контроля следует рассмотреть для ИС с терминалами, установленными в зонах повышенного риска нарушения ЗИ.

Приведем перечень таких ограничений:

• использование определенных интервалов времени разрешенного доступа, например для пакетной передачи файлов или регулярных интерактивных сеансов связи небольшой продолжительности;

• ограничение времени подключения обычным часовым режимом работы организации и получение специального разрешения для работы в сверхурочное время.

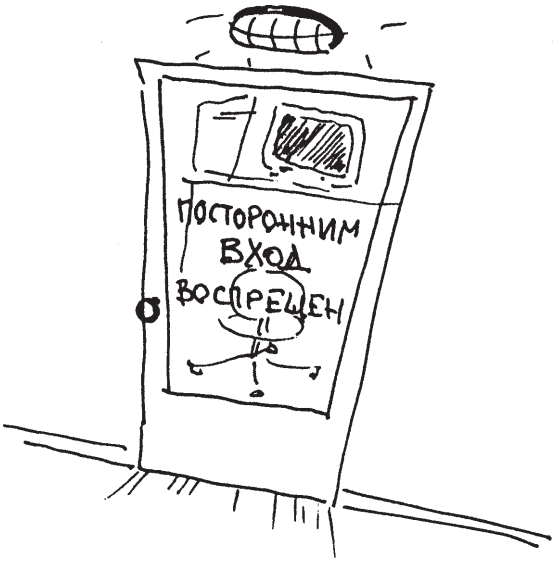
Ограничение доступа к сервисам (754)

Пользователям и обслуживающему персоналу ИС следует предоставлять доступ к сервисам в соответствии с принятой политикой управления доступом к информации. ***Рекомендуется рассмотреть возможность использования следующих средства контроля:***

• доступ к приложениям (сервисам) через систему меню, обеспечивающую контроль полномочий доступа пользователей;

• ограничение доступа пользователей к информации о структурах данных и функциях ИС, доступ к которым им не разрешен, посредством соответствующего редактирования пользовательской документации;

• контроль за выходной информацией приложений на предмет содержания в них конфиденциальной информации. Такая информация должна посылаться только на определенные терминалы и компьютеры. Необходим периодический анализ выходной информации и удаление при необходимости лишней информации.



Ограничение доступа к сервисам...

Управление доступом к сервисам (720)

Электронная почта (730)

В организации должны быть заданы четкие правила относительно статуса и использования электронной почты. ***Для уменьшения риска нарушения ЗИ, связанного с применением электронной почты, рекомендуется:***

• учитывать уязвимость электронных сообщений по отношению к несанкционированному перехвату и модификации;

• учитывать вероятность неправильной адресации или направления сообщений не по назначению, а также надежность и доступность сервиса в целом.

Системы электронного документооборота (720)

При использовании систем электронного документооборота следует учитывать выполнение требований ЗИ:

- необходимость исключения некоторых категорий конфиденциальной информации, в случае, если в данной системе не обеспечивается надлежащий уровень защиты;
- необходимость определения правил и средств контроля для администрирования коллективно используемой информации (электронные доски объявлений);
- использование средств ограничения доступа к информации, относящейся к различным рабочим группам;
- определение категории персонала и представителей сторонних организаций, которым разрешено использовать систему и участки, из которых можно получить доступ к ней.

Управление доступом к приложениям (720)

Для предотвращения несанкционированного доступа к информации в ИС, необходимо использовать логические средства контроля доступа. Логический доступ к приложениям следует предоставлять только зарегистрированным пользователям.

Приложения должны выполнять следующие функции:

- контролировать доступ пользователей к данным и приложениям в соответствии с политикой управления доступом, принятым в организации;
- обеспечивать защиту от несанкционированного доступа к системным программ, способным обойти средства контроля и создать возможность НСД;
- не нарушать защиту других систем, с которыми они разделяют информационные ресурсы.

Использование системных программ (720)

В ИС могут использоваться системные программы, способные обойти средства контроля ОС и приложений. Необходимо ограничить и тщательно контролировать использование таких системных утилит.

Рекомендуется использовать следующие средства контроля (по возможности):

- защиту системных утилит с помощью паролей;
- изоляцию системных утилит от прикладного программного обеспечения;
- предоставление доступа к системным утилитам минимальному числу пользователей;
- предоставление специального разрешения на использование системных утилит;
- ограничение доступности системных утилит, например временем внесения санкционированного изменения;
- регистрацию всех случаев использования системных утилит;
- определение и документирование уровней полномочий доступа к системным утилитам;
- удаление всех ненужных утилит и системных программ

Управление доступом к библиотекам исходных текстов программ (720)

Для сведения риска повреждения программного обеспечения к минимуму необходимо осуществлять жесткий контроль за доступом к библиотекам исходных текстов программ.

Рекомендуется придерживаться следующих правил:

- не хранить библиотеки исходных текстов программ в ИС,
- назначить ответственного за хранение библиотеки исходных текстов программ,
- хранить распечатки программ в библиотеках исходных текстов,
- ограничить доступ к библиотекам исходных текстов программ,
- не хранить разрабатываемые программы в библиотеках исходных текстов рабочих программ,
- обновление библиотек исходных текстов программ и выдача текстов программ программистам должны производиться только назначенным ответственным сотрудником после получения разрешения на доступ к приложению в установленной форме,
- фиксировать все случаи доступа к библиотекам исходных текстов программ в контрольном журнале,
- устаревшие версии исходных текстов программ следует архивировать с указанием даты окончания их использования вместе со всем вспомогательным программным обеспечением и информацией об организации выполнения заданий для этой версии ПО,
- сопровождение и копирование библиотек исходных текстов программ осуществлять в соответствии с процедурами управления процессом внесения изменений.

Изоляция уязвимых мест в защите ИС (720)

При наличии уязвимых мест в защите ИС может потребоваться организация выделенной (изолированной) вычислительной среды. Возможно применение других специальных мер: запуск приложения на выделенном компьютере или разделения ресурсов только с надежными прикладными системами.

В общем случае ***рекомендуется придерживаться следующих правил:***

- уязвимые места в ИС должны быть явно определены и документированы;
- при запуске уязвимого приложения в коллективно используемой среде необходимо явно указать прикладные процессы, с которыми оно может работать одновременно.

Отслеживание событий, представляющих угрозу ЗИ (350)

Для выявления несанкционированных действий и обеспечения соответствия политике управления доступом рекомендуется соблюдать перечисленные ниже правила.

Регистрация событий (350)

Регистрация событий...

Все чрезвычайные ситуации и события, связанные с нарушением режима ЗИ, необходимо регистрировать в журнале. Последний следует хранить в течение заданного периода времени. Кроме неудавшихся попыток входа в систему, целесообразно также регистрировать случаи успешного доступа. ***Контрольный журнал должен включать:***

- идентификаторы пользователей;
- дату и время входа и выхода из системы;
- идентификатор или местонахождение терминала (по возможности).

Слежение за использованием сервисов (750)

Необходимо установить процедуры слежения за использованием сервисов ИС. Пользователям должны быть доступны только явно разрешенные сервисы. Уровень контроля следует определить с помощью оценки рисков. Рекомендуется следить за следующими событиями:

- неудачными попытками доступа в ИС;
- попытки несанкционированного использования восстановленных пользовательских идентификаторов;
- использованием ресурсов с привилегированным доступом;
- отдельными действиями, потенциально опасными с точки зрения нарушения режима ЗИ;
- использованием конфиденциальных ресурсов.

Все действия, связанные со слежением и регистрацией, должны быть формально разрешены руководством.

Служба безопасности (720)

Для эффективной защиты информации в ИС организации, как правило, создается подразделение безопасности, на специалистов которого возлагается решение следующих основных задач:

- организация и поддержание контролируемого доступа пользователей к ресурсам ИС на всех этапах ее жизненного цикла;
- слежение за состоянием безопасности ИС и оперативное реагирование на происходящие в ней несанкционированные действия пользователей.

В связи с применением дополнительных средств защиты информации ***администратору безопасности предстоит выполнять такие операции:***

- устанавливать СЗИ на компьютеры организации (установка и внедрение СЗИ);
- настраивать СЗИ путем задания прав доступа пользователей как к ресурсам компьютеров, так и к ресурсам сети (эксплуатация СЗИ);
- контролировать состояние защищенности ИС путем оперативного мониторинга и анализа системных журналов (контроль за состоянием безопасности ИС).

Защита целостности данных и программ от вредоносного программного обеспечения (720)

Существует, как известно, ряд вредоносных методов, позволяющих нарушать целостность данных и программ: "компьютерные вирусы", "сетевые черви", "Троянские кони" и "логические бомбы". Администраторы ИС и пользователи должны быть всегда готовы к возможности проникновения вредоносного программного обеспечения в ИС и оперативно принимать меры по обнаружению его внедрения и ликвидации последствий его атак.

Защиты от вирусов (720)

В основе защиты от вирусов должны лежать знание и понимание правил безопасности, надлежащие средства управления доступом к системам.

В частности:

- организация должна проводить политику, требующую установки только лицензированного программного обеспечения;
- противовирусные программные средства должны регулярно обновляться и использоваться для профилактических проверок (желательно ежедневных);
- необходимо проводить регулярную проверку целостности критически важных программ и данных. Наличие лишних файлов и следов несанкционированного внесения изменений должно быть зарегистрировано в журнале и расследовано;
- дискеты неизвестного происхождения следует проверять на наличие вирусов до их использования;
- необходимо строго придерживаться установленных процедур по уведомлению о случаях поражения ИС компьютерными вирусами и принятию мер по ликвидации последствий от их проникновения;
- следует иметь планы обеспечения бесперебойной работы организации для случаев вирусного заражения, в том числе планы резервного копирования всех необходимых данных и программ и их восстановления. Эти меры особенно важны для сетевых файловых серверов, поддерживающих большое количество рабочих станций.

Контроль за состоянием безопасности ИС (700)

Администратору безопасности необходимо контролировать состояние ИС как оперативно, путем слежения за состоянием защищенности компьютеров ИС, так и не оперативно — путем анализа содержимого журналов регистрации событий СЗИ.

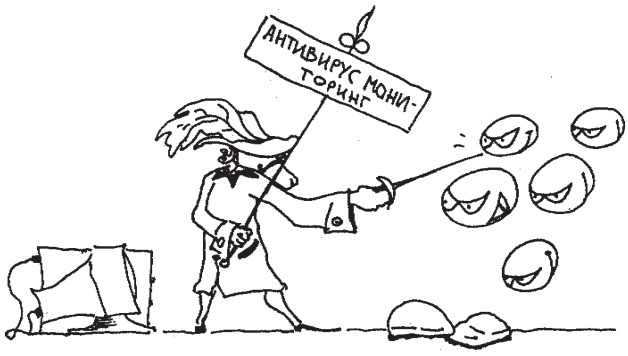
Использование сервера управления доступом для оперативного контроля за состоянием рабочих станций и работой пользователей позволяет отказаться от постоянного присутствия в сети администратора безопасности. В этом случае сервер управления доступом автоматически регистрирует несанкционированные действия, происходящие в сети, и всегда обладает оперативной информацией о состоянии станций.

Увеличение количества рабочих станций и использование программных средств, включающих большое количество разнообразных компонентов, приводит к существенному увеличению объемов журналов регистрации событий СЗИ. Объем сведений, хранящихся в журналах, может настолько увеличиться, что администратор уже физически не сможет полностью проанализировать их содержимое за приемлемое время.

Для облегчения работы администратора безопасности необходимо реализовать:

- оперативный контроль за состоянием рабочих станций сети и работой пользователей и за регистрацией событий несанкционированного доступа в специальном журнале;
- селекцию определенных событий (по имени пользователя, дате, времени происшедшего события, его категории и т.п.) из системных журналов;
- хранение системных журналов каждой рабочей станции по системе "день/месяц/год" с автоматическим ограничением срока их хранения. По истечении установленного срока журналы уничтожаются;
- специальные возможности по ограничению перечня событий, регистрируемых СЗИ;
- семантическое сжатие данных в журналах регистрации, позволяющее укрупнять регистрируемые события без существенной потери их информативности;
- автоматическая подготовка отчетных документов установленной формы о работе станций сети и имевших место нарушениях, что позволяет существенно снизить рутинную нагрузку на администратора безопасности.

Системы обнаружение атак (750)



Система обнаружения атак...

Атаки на сеть и хосты не всегда возможно перехватить во время их проведения с помощью брандмауэров и другого инструментария защиты. Брандмауэры и системы идентификации можно уподобить замкам и запорам — они препятствуют проникновению внутрь нежелательных визитеров и пропускают только знакомых.

Однако они не в состоянии отследить все, что происходит в сетевой среде. Например, если одни атакующие специализируются на проникновении через брандмауэр, то другие его минуют и проникают с помощью модемного доступа или другими путями.

Кроме того, если атакующему удастся узнать пароль и воспользоваться им, то ни система идентификации, ни брандмауэр не будут знать об этом.

Другая проблема с брандмауэрами состоит в том, что они не достаточно эффективны для контроля за активностью внутри корпоративной сети, откуда (по статистике) и исходит основная угроза. Подобные атаки могут быть инициированы как отдельными сотрудниками, так и другими лицами, имеющими законный доступ в сеть и использующими эту привилегию для нанесения ущерба.

Брандмауэры и системы идентификации жизненно необходимы, но для постоянного контроля за сетевым трафиком и знания о любых нетипичных событиях защиту сети следует укрепить с помощью системы обнаружения атак (СОА). Они способствуют выявлению атак на основании заданных признаков (signature) и известных методов вторжения, а также идентификации статистических отклонений от типичного поведения. Кроме того, многие системы обнаружения атак протоколируют любые подозрительные действия, что дает возможность собрать улики на случай привлечения злоумышленника к суду.

Системы для обнаружения атак делятся на две группы. Они предназначены для контроля либо за хостами и осуществляют мониторинг ОС и приложений, либо за сетью и проводят мониторинг трафика в реальном времени.

СОА должна обладать следующими возможностями:

- выполняться непрерывно в фоновом режиме
- быть отказоустойчивой, иными словами, в случае краха или сбоя систем не требует перестройки или переконфигурации
- защищена от атак
- создавать минимальную дополнительную нагрузку на сеть
- адаптироваться к изменениям в сети, приложениях и устройствах.

Системы обнаружения атак на хосты заслуживают внимания по нескольким причинам. Прежде всего, они могут сообщить о факте атаки и степени ее серьезности. Кроме того, хост представляет собой лучший участок для противодействия атакам. Системы на базе хостов способны предоставлять подробную информацию о том, кто к каким файлам обращается и когда пользователи начинают и завершают сеансы связи с сервером.

Этот класс систем обнаружения атак позволяет также выявить изменения в системных файлах и узнать о попытках установки потенциально вредоносного программного обеспечения. В частности, так называемые потайные ходы представляют собой специализированные программы, с помощью которых хакеры могут на расстоянии контролировать сервер и либо украсть информацию с сервера, либо изменить ее в злонамеренных целях.

Системы на базе хостов имеют и иные преимущества, в частности — относительно невысокую цену. Заказчики могут приобрести несколько агентов, затратив всего лишь пару сотен долларов на каждого. Ввиду того, что системы для хостов выполняются на имеющемся оборудовании (серверах файлов и Web), никаких дополнительных устройств приобретать нет необходимости.

Рынок СОА предлагает также ***системы для обнаружения атак на сеть***. Системы для сети осуществляют мониторинг за сетевым трафиком в реальном времени, в результате они быстрее реагируют на любую проводимую атаку и извещают о ней администратора. Принцип работы систем для сетей заключается в анализе заголовков пакетов, поэтому, в отличие от систем для хостов, они способны обнаружить такие атаки, как отказ в обслуживании, которые иными методами, без анализа пакетов, выявить невозможно. Более того, они могут проверять не только заголовок, но и содержимое пакета.

Системы для сетей способны также прерывать атаки. Благодаря обнаружению в реальном времени они могут остановить проводимую атаку прежде, чем она нанесет серьезный урон, например блокирует критический сервер. Кроме того, в отличие от систем для хостов, системы обнаружения атак на сеть не зависят от конкретной ОС.

Каждый вид систем обнаружения атак служит конкретной цели, так что на практике они выполняют различные функции. В идеале для сокращения риска следует использовать системы обоих типов.

Как работает сканер безопасности? (750)

Сканер — это инструмент эффективной политики безопасности сети, которая складывается из применения различных технических, организационных и законодательных мер.

Сканеры ни в коем случае не заменяют специалистов в области безопасности. Они лишь автоматизируют их работу, помогая быстро проверить сотни узлов, в том числе и находящиеся на других территориях.

Сеть состоит из каналов связи, узлов, серверов, рабочих станций, прикладного и системного программного обеспечения, баз данных и т.д. Все эти компоненты нуждаются в оценке эффективности их защиты. ***Средства анализа защищенности исследуют сеть и ведут поиск"слабых" мест, таких как:***

- "люки" в программах (back door) и программы типа "троянский конь";
- слабые пароли;
- восприимчивость к проникновению из незащищенных систем;
- неправильная настройка межсетевых экранов, Web-серверов и баз данных.

Технология анализа защищенности является действенным методом реализации политики сетевой безопасности прежде, чем осуществится попытка ее нарушения снаружи или изнутри организации.

Сканеры предназначены для обнаружения только известных уязвимостей, описание которых имеется у них в базе данных. В этом они подобны антивирусным системам, которым для эффективной работы необходимо постоянно обновлять базу данных сигнатур. Функционировать такие средства могут на сетевом уровне (network-based), уровне операционной системы (host-based) и уровне приложения (application-based). Наибольшее распространение получили средства анализа защищенности сетевых сервисов и протоколов.

Помимо обнаружения уязвимостей, при помощи средств анализа защищенности можно быстро определить все узлы корпоративной сети, доступные в момент проведения тестирования, выявить все используемые в ней сервисы и протоколы, их настройки и возможности для несанкционированного воздействия (как изнутри корпоративной сети, так и снаружи). Также эти средства вырабатывают рекомендации и пошаговые меры, позволяющие устранить выявленные недостатки.

Механизмы работы сканера (754)

Существует два основных механизма, при помощи которых сканер проверяет наличие уязвимости — сканирование (scan) и зондирование (probe).

Сканирование — механизм пассивного анализа, когда сканер пытается определить наличие уязвимости по косвенным признакам — без фактического подтверждения ее наличия. Этот метод наиболее быстрый и простой для реализации. В терминах компании ISS данный метод получил название "логический вывод" (inference). Согласно компании Cisco этот процесс идентифицирует открытые порты, найденные на каждом сетевом устройстве, и собирает связанные с портами заголовки (banner), найденные при сканировании каждого порта. Каждый полученный заголовок сравнивается с таблицей правил определения сетевых устройств, операционных систем и потенциальных уязвимостей. На основе проведенного сравнения делается вывод о наличии или отсутствии уязвимости.

Зондирование — механизм активного анализа, который позволяет убедиться, имеется ли на анализируемом узле уязвимость. Зондирование выполняется путем имитации атаки, использующей проверяемую уязвимость. Этот метод более медленный, чем сканирование, но почти всегда гораздо более точный. В терминах компании ISS данный метод получил название "подтверждение" (verification). Согласно компании Cisco этот процесс использует информацию, полученную в процессе сканирования (логического вывода), для детального анализа каждого сетевого устройства. В этом процессе также используются известные методы реализации атак для того, чтобы полностью подтвердить предполагаемые уязвимости и обнаружить другие уязвимости, которые не могут быть обнаружены пассивными методами, например подверженность атакам типа "отказ в обслуживании" ("denial of service").

Этапы сканирования (750)

Практически любой сканер проводит анализ защищенности в несколько этапов:

Сбор информации о сети ...

1. Сбор информации о сети. На данном этапе идентифицируются все активные устройства в сети и определяются запущенные на них сервисы и демоны. В случае использования систем анализа защищенности на уровне операционной системы данный этап пропуска-

ется, поскольку на каждом анализируемом узле установлены соответствующие агенты системного сканера.

2. ***Обнаружение потенциальных уязвимостей.*** Сканер использует описанную выше базу данных для сравнения собранных данных с известными уязвимостями при помощи проверки заголовков или активных зондирующих проверок. В некоторых системах все уязвимости ранжируются по степени риска. Например, в системе NetSonar уязвимости делятся на два класса: сетевые и локальные. Сетевые уязвимости (например, воздействующие на маршрутизаторы) считаются более серьезными по сравнению с уязвимостями, характерными только для рабочих станций. Аналогично и в Internet Scanner все уязвимости делятся на три степени риска: высокая (High), средняя (Medium) и низкая (Low).

3. ***Подтверждение выбранных уязвимостей.*** Сканер использует специальные методы и моделирует (имитирует) определенные атаки для подтверждения факта наличия уязвимостей на выбранных узлах сети.

4. ***Генерация отчетов***. На основе собранной информации система анализа защищенности создает отчеты, описывающие обнаруженные уязвимости. В некоторых системах (например, Internet Scanner и NetSonar) отчеты создаются для различных категорий пользователей, начиная от администраторов сети и заканчивая руководством компании. Если первых в первую очередь интересуют технические детали, то для руководства компании необходимо представить красиво оформленные с применением графиков и диаграмм отчеты с минимумом подробностей. Немаловажным аспектом является наличие рекомендаций по устранению обнаруженных проблем. И здесь по праву лидером является система Internet Scanner, которая для каждой уязвимости содержит пошаговые инструкции по устранению уязвимостей, специфичные для каждой операционной системы. Часто отчеты также содержат ссылки на FTP- или Web-серверы, содержащие patch и hotfix, устраняющие обнаруженные уязвимости.

5. ***Автоматическое устранение уязвимостей.*** Этот этап изредка реализуется в сетевых сканерах, но широко применяется в системных (например, System Scanner). При этом данная возможность может реализоваться по-разному. Например, в System Scanner создается специальный сценарий (fix script), который администратор может запустить для устранения уязвимости. Одновременно с созданием этого сценария, создается и второй, отменяющий изменения. Это необходимо, когда после устранения проблемы нормальное функционирование узла было нарушено. В других системах возможности "отката" не существует.

В любом случае у администратора, осуществляющего поиск уязвимостей, есть несколько вариантов использования системы анализа защищенности:

- Запуск сканирования только с проверками на потенциальные уязвимости (этапы 1,2 и 4). Это дает предварительное ознакомление с системами в сети. Данный метод гораздо менее разрушителен по сравнению с другими и самый быстрый.
- Запуск сканирования с проверками на потенциальные и подтвержденные уязвимости. Этот метод может вызвать нарушение работы узлов сети во время реализации проверок типа "exploit check".
- Запуск сканирования с пользовательскими правилами для поиска конкретной проблемы.

Консалтинг в информационной безопасности (750)

Для организации защиты информации или проведения аудита существующей ИС необходим штат высококвалифицированных специалистов в области информационной безопасности. Это может быть очень дорого и невыгодно для организации, особенно небольшой. Для проведения обследований и аудита целесообразно привлекать сторонние консалтинговые компании, так как они имеют большой опыт и штат профессионалов в области обеспечения и контроля состояния информационной безопасности.

Тест на преодоление защиты (750)

Тест на преодоление защиты (Penetration Test) заключается в попытке обойти принятую в корпоративной сети систему безопасности. При этом консультант выступает в роли злоумышленника (внутреннего или внешнего), задача которого — скомпрометировать корпоративную систему, получить конфиденциальные данные или нарушить функционирование системы. Для того чтобы компания получила наибольшую пользу от этой услуги, о проведении атаки должен знать лишь ограниченный круг лиц в организации, в основном — высшее руководство.

Основными целями предпринимаемой попытки преодоления защиты являются констатация и доказательство возможности взлома системы, а также выявление реакции на атаку персонала (как администраторов, так и рядовых пользователей). Успешная реализация атаки — действенное средство доказать руководству компании необходимость увеличения затрат на обеспечение информационной безопасности, особенно если в результате успешного взлома консультанту удалось незаконно получить конфиденциальную информацию руководства. Кроме того, тест на преодо-

ление защиты является хорошим способом проверить соблюдение персоналом принятой политики безопасности, например правил хранения и смены пароля.

Перед проведением теста заказчику следует обязательно договориться с консультантом о том, какие атаки можно проводить полностью, а какие следует только обозначить как принципиально выполнимые и ограничиться получением подробных инструкций по их реализации. Например, если атака на систему позволяет полностью вывести из строя центральный сервер базы данных, то нецелесообразность ее практической реализации представляется очевидной — убытки от такого тестирования будут слишком велики. Если же в результате атаки возможно раскрытие конфиденциальной информации или получение прав администратора системы, то такую атаку реализовать полезно, так как она показывает уязвимость исследуемой системы, не нанося ей существенного ущерба. Необходимо также помнить, что ответственность за возможный ущерб при успешной реализации атаки полностью ложится на заказчика тестирования, т.е. на компанию.

Недостатком данного метода является отсутствие целостной картины состояния информационной безопасности: заказчик лишь получает информацию о том, что исследуемая система уязвима. Проведение определенной атаки не позволяет выявить весь набор уязвимых и слабых мест системы и тем более не дает никаких рекомендаций по повышению уровня защищенности.

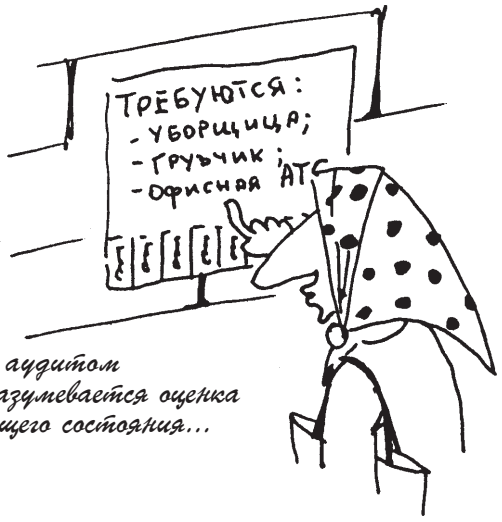
Со своей стороны консультант обязательно должен разъяснить персоналу заказчика, что попытка преодоления защиты в конечном счете имеет целью обеспечение безопасной работы в автоматизированной системе, и лучше, чтобы принципиальную уязвимость выявил специалист в области информационной безопасности, чем злоумышленник. Иначе эксперт рискует сформировать отрицательное отношение к себе и консалтинговой компании со стороны персонала. Таким образом, знание психологии и умение общаться с людьми — отнюдь не бесполезные навыки для консультанта в области информационной безопасности.

Аудит (750)

Под аудитом (Audit) подразумевается оценка текущего состояния компьютерной системы на соответствие некоему стандарту или предъявляемым требованиям.

Это важно

Стандарты могут быть внутри корпоративными или общими (как правительственными, так и коммерческими). ***Одна из главных трудностей при проведении данного типа работ — правильный выбор стандарта***, на соответствие которому будет проверяться автоматизированная система. В общем случае стандарт, по которому проводится аудит, должен содержать требования к нормативно-правовой базе, к системам разграничения доступа, контроля целостности, криптографической защиты информации, а также к механизмам физической защиты компонентов автоматизированной системы. Кроме того, стандарт должен включать требования по обеспечению непрерывности защиты, например требования к порядку и периодичности пересмотра правил категорирования информации или привилегий пользователей.



Под аудитом подразумевается оценка текущего состояния...

В большинстве случаев ***аудит требуется***, когда автоматизированная система предназначена для обработки конфиденциальной или секретной информации. Для каждой категории информации стандартами определяется нижняя граница уровня безопасности автоматизированной системы.

Проведение аудита полезно также после построения автоматизированной системы и ее подсистемы безопасности на этапе приемки в эксплуатацию для оценки степени соблюдения предъявляемых к ней требований. Следует отметить, что аудит автоматизированной системы рекомендуется проводить периодически (например, раз в год), так как состояние любой системы изменяется с течением времени, и к моменту очередного аудита оно может не иметь ничего общего с тем, что было зафиксировано при предыдущем аудите.

В ходе аудита эксперты по формальным критериям стандарта оценивают, в какой мере данный компонент или процесс удовлетворяет приведенным в стандарте требованиям, одновременно формируя список уязвимых мест автоматизированной системы. Отчет об аудите содержит оценку соответствия системы данному стандарту, но не содержит рекомендаций и предложений по устранению выявленных уязвимых мест и повышению уровня защищенности.

Обследование (750)

Определение

Обследование (оценка, Assessment) автоматизированной системы — наиболее сложный и полезный вид работ по консалтингу в информационной безопасности. В рамках этой работы эксперты проводят комплексную оценку автоматизированной системы с учетом ее особенностей. Такая оценка включает анализ информационных потоков аппаратного и программного обеспечения, сетевой инфраструктуры, методов управления и администрирования компонентов.

Даже этот начальный этап обследования оказывается целесообразным для большинства клиентов, так как порой клиент не имеет обобщенной и структурированной информации о своей автоматизированной системе и представляет ее как разрозненную совокупность отдельных подсистем. После сбора и упорядочивания информации ***специалисты консалтинговой компании проводят анализ состояния информационной безопасности в несколько этапов.***

- ***Анализ существующей организационной структуры*** информационной безопасности (ИБ), в том числе анализ функций службы, взаимоотношений подразделений по вопросам обеспечения защиты информации, вопросов подчиненности и структуры службы ИБ.
- ***Анализ существующей нормативно-правовой базы*** информационной безопасности автоматизированной системы, в том числе оценка принятой политики безопасности, организационно-распорядительных документов, положений и инструкций по обеспечению защиты информации, а также анализ их соответствия существующим законодательным и нормативным актам.
- ***Анализ мер технической защиты информации***, в том числе анализ существующих мер и средств технической защиты информации, а также порядка их применения, рассмотрение и анализ используемых заказчиком средств разграничения доступа и защиты от несанкционированного доступа (в частности, при работе с Internet), антивирусных средств, межсетевых экранов, защиты с помощью паролей, системы обнаружения вторжений, криптографических средств защиты информации, методов контроля целостности. Кроме того, эксперты анализируют порядок использования встроенных механизмов защиты компонентов автоматизированной системы и оценивают достаточность мер и правильность использования средств технической защиты информации.
- ***Выявление угроз безопасности*** (внутренних и внешних) и существующих уязвимых мест в компонентах системы, а также оценка рисков. Эксперты ранжируют угрозы по вероятности их возникновения в данной автоматизированной системе и мере возможного ущерба от реализации угроз. В результате они составляют список наиболее опасных угроз безопасности, перечень и описание уязвимых мест компонентов, включая описание их источников (модель нарушителя) и механизмов их реализации.
- ***Выработка рекомендаций*** по доработке существующей системы защиты информации компании. Рекомендации могут касаться совершенствования организационно-штатной структуры, доработки и создания нормативных документов, положений и инструкций по обеспечению информационной безопасности. Кроме того, эксперты могут дать рекомендации по применению штатных средств защиты компонентов, а также по использованию дополнительных систем защиты информации и методов контроля и аудита состояния информационной безопасности.

Таким образом, обследование автоматизированных систем позволяет не только оценить степень уязвимости, но и укрепить подсистему информационной безопасности для защиты от угроз, исходящих как извне, так и изнутри, а также управлять рисками и минимизировать возможные потери.

Как выбрать консалтинговую компанию (750)

К кому обратиться, если вы, наконец, решили, что вашей компании или организации необходимы консалтинговые услуги в области информационной безопасности; кого предпочесть, чтобы заказ был качественно выполнен, а итогом работы был не только отчет в виде списка уязвимых мест, полученного автоматическими сканерами безопасности, наподобие SATAN?

Этот вид деятельности специально не регламентирован, поэтому ***оценивать консалтинговые компании приходится по неформальным признакам***. Такими признаками можно считать количество сотрудников, квалификацию персонала, продолжительность работы компании на рынке информационной безопасности, наличие и качество методик и инструментов для проведения аналитических работ, а также стоимость работ.

Количество сотрудников

При обследовании сложной системы наличие лишь небольшого числа сотрудников должно вызывать определенные сомнения в качестве и разумных сроках проведения работ и предоставления отчетных материалов. В современных информационных технологиях разнообразие методов, схем и принципов обеспечения информационной безопасности достаточно велико. ***В составе проводящей обследование группы консультантов должны быть, по крайней мере, специалисты по безопасности операционных систем, СУБД, средств телекоммуникаций, прикладных систем, эксперты в области физической защиты компонентов автоматизированной системы, организации межсетевых экранов, средств защиты от несанкционированного доступа, антивирусных программ, систем криптографической защиты информации и построения VPN, средств обнаружения вторжений.*** Иными словами, у компании-консультанта должен быть штат профессиональных высококвалифицированных экспертов в области информационной безопасности для каждого из компонентов автоматизированной системы заказчика.

Количество сотрудников...

Квалификация сотрудников

Сотрудники, проводящие аудит информационной системы, должны, прежде всего, знать те стандарты, на соответствие которым проводится аудит. Кроме того, при проведении работ аудитор не должен полагаться только на ответы персонала на поставленные вопросы. Во-первых, человек из компании-клиента сам может не знать ответа на вопрос, а во-вторых, случайно или намеренно аудитор может быть введен в заблуждение. Поэтому ***аудитор должен обладать достаточной квалификацией или иметь возможность привлечения необходимого специалиста для проверки соответствия параметров информационной системы выдвигаемым требованиям.***

Однако наиболее высокие требования к специалистам предъявляются при проведении обследования автоматизированной системы. Кроме выявления уязвимых мест и проверки на соответствие стандартам от них требуется составление профессиональных рекомендаций по оптимизации, доработке или созданию подсистемы информационной безопасности. А для этого они должны, во-первых, хорошо разбираться в используемых информационных технологиях, а во-вторых, профессионально знать современные методы и средства защиты информации. Поэтому при выборе консалтинговой компании уместно поинтересоваться наличием профессиональных сертификатов у ее экспертов. Немаловажное значение имеет также наличие грамотных менеджеров проектов, способных координировать работу аналитиков и обобщать их отчеты, при этом тесно сотрудничая с заказчиком для обеспечения качественного и — главное — полезного для него результата.

Надо знать

Продолжительность работы на рынке информационной безопасности и наличие методик

Для проведения Penetration Test время работы компании не имеет, на наш взгляд, определяющего значения. Несмотря на то, что основы методов поиска уязвимых мест как в прикладном программном обеспечении, так и в сетевых сервисах и операционных системах разработаны довольно давно, собственно информационные технологии и их реализации развиваются стремительно. Из-за желания опередить конкурентов время тестирования сокращается до минимума, в результате он, как правило, содержит много невыявленных уязвимых мест. Однако обнаруженные уязвимые места довольно быстро становятся известны общественности и, соответственно, устраняются производителями.

До заключения договора

Если консалтинговая компания претендует на проведение обследования информационной системы, то она должна иметь достаточно длительную историю работы на рынке информационной безопасности, так как в этом случае для успеха крайне важен опыт проведения подобных работ и наличие апробированных методик их проведения. Одинаковых информационных систем не существует, но принципиальные решения по защите, успешно применяемые сотрудниками консалтинговой компании, могут быть тиражированы на другие системы, естественно, с их адаптацией к конкретной информационной системе.

При выборе консалтинговой компании заказчику необходимо поинтересоваться, какие проекты данная компания выполняла до настоящего времени, и озна-

комиться с отзывами предыдущих заказчиков о выполненных работах. Уважающая себя компания-консультант должна подробно отвечать на вопросы заказчика (естественно, не раскрывая конфиденциальную информацию о клиентах).

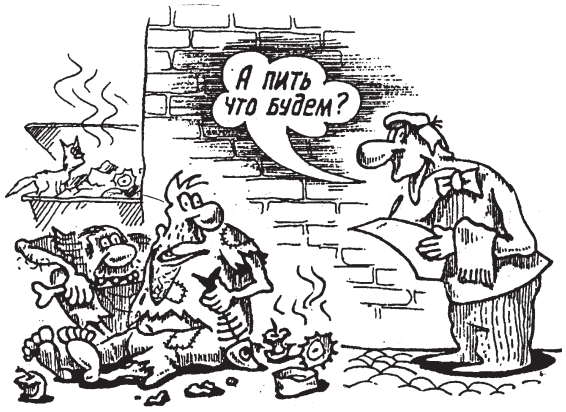
Еще ***до заключения договора на проведение обследования немаловажно получить*** представление о методиках и инструментах, которыми пользуются консультанты. Отработанная методика проведения работ дает гарантию, что ничего важного в их ходе упущено не будет и ни один аспект информационной безопасности не останется без внимания. Использование качественных коммерческих инструментов (например, средств сканирования безопасности, наподобие ISS Internet Scanner) гарантирует, что в автоматизированной системе будет найдено большинство уязвимых мест, поскольку, в отличие от свободно распространяемых систем тестирования, в коммерческих системах сканирования информация о "дырах" в системах безопасности компонентов компьютерной системы обновляется достаточно оперативно — по мере их обнаружения специальными группами экспертов.

До начала проведения работ заказчику необходимо договориться с консалтинговой компанией о форме отчета и основных параметрах его содержания, так как в ответ на один и тот же вопрос одна компания-консультант предоставит лишь распечатку руководящих документов, другая — обзор средств защиты, и только, возможно, третья решит основные проблемы заказчика.

Стоимость работ

Последний, критерий оценки серьезности консалтинговой компании — стоимость проведения работ. Как правило, консалтинговые компании придерживаются одного из двух подходов к ценообразованию и определению состава работ. ***Во-первых***, если заказчик уже имеет фиксированный бюджет на проведение таких работ, то совместно с компанией-консультантом он определяет, что же именно он может получить за эти деньги. ***Во-вторых***, и это представляется наиболее разумным, стоимость работ формируется исходя из потребностей заказчика и состава работ, который становится ясным после первоначальных переговоров консалтинговой компании с заказчиком. В противном случае заказчик рискует получить в итоге совсем не то, что ожидал, и расходы окажутся напрасными.

Обычно радость заказчика от того, что предложенная цена обследования оказалась приемлемой, быстро проходит после получения им отчетных материалов, где, кроме слов о необходимости и важности обеспечения информационной безопасности, содержатся только цитаты из руководящих документов, законов и



Стоимость работ...

стандартов, а также псевдонаучные рассуждения на тему информационной безопасности, и ни слова нет о фактическом состоянии его автоматизированной системы.

Резюме

Использование специальных привилегий следует ограничить и контролировать, поскольку это один из основных факторов, способствующих нарушению режима ЗИ. В многопользовательских ИС должна существовать система контроля предоставления привилегий. При организации такой системы рекомендуется:

- идентифицировать привилегии, связанные с каждым программным продуктом или сервисом, поддерживаемым системой, а также категории сотрудников, которым их необходимо предоставить;
- предоставлять привилегии отдельным лицам только в случае крайней необходимости и в зависимости от ситуации, т.е. только когда они нужны для выполнения ими своих функций;.
- реализовать автоматический процесс определения полномочий и вести учет всех предоставленных привилегий;
- по возможности использовать системные программы, для которых нет необходимости предоставлять специальные привилегии пользователям;
- пользователи, имеющие большие привилегии для специальных целей, должны использовать другой пользовательский идентификатор для обычной работы.

Пользователям и обслуживающему персоналу ИС следует предоставлять доступ к сервисам в соответствии с принятой политикой управления доступом к информации. ***Рекомендуется рассмотреть возможность использования следующих средства контроля:***

• доступ к приложениям (сервисам) через систему меню, обеспечивающую контроль полномочий доступа пользователей;

• ограничение доступа пользователей к информации о структурах данных и функциях ИС, доступ к которым им не разрешен, посредством соответствующего редактирования пользовательской документации;

• контроль за выходной информацией приложений на предмет содержания в них конфиденциальной информации. Такая информация должна посылаться только на определенные терминалы и компьютеры. Должен проводится периодический анализ выходной информации и при необходимости лишняя информация должна удаляться.

Для эффективной защиты информации в ИС организации, ***как правило создается специальное подразделение (администрация безопасности), на специалистов которого возлагается решение следующих основных задач:***

• организация и поддержание контролируемого доступа пользователей к ресурсам ИС на всех этапах ее жизненного цикла;

• слежение за состоянием безопасности ИС и оперативное реагирование на происходящие в ней несанкционированные действия пользователей.

В связи с применением дополнительных средств защиты информации (СрЗИ) администратору безопасности предстоит выполнять следующие действия (операции):

• устанавливать СрЗИ на компьютеры организации (установка и внедрение СрЗИ);

• настраивать СрЗИ путем задания прав доступа пользователей к ресурсам как компьютеров, так и к ресурсам сети (эксплуатация СрЗИ);

• контролировать состояние защищенности ИС путем оперативного мониторинга и анализа системных журналов (контроль за состоянием безопасности ИС).

Сканер – это инструмент эффективной политики безопасности сети, которая складывается из применения различных технических, организационных и законодательных мер.

Сканеры ни в коем случае не заменяют специалистов в области безопасности. Они всего лишь автоматизируют их работу, помогая быстро проверить сотни узлов, в т.ч. и находящихся на других территориях.

Сеть состоит из каналов связи, узлов, серверов, рабочих станций, прикладного и системного программного обеспечения, баз данных и т.д. Все эти компоненты нуждаются в оценке эффективности их защиты. Средства анализа защищенности исследуют сеть и ищут "слабые" места.

Для организации защиты информации или проведения аудита существующей автоматизированной системы необходим штат высококвалифицированных специалистов в области информационной безопасности. Это может быть очень дорого и невыгодно для организации, особенно небольшой. ***Для проведения обследований и аудита целесообразно привлекать сторонние консалтинговые компании***, так как они имеют большой опыт и штат профессионалов в области обеспечения и контроля состояния информационной безопасности.