Аудит процессов и систем влияющих на ИБ учреждения

Аудит организационных, административных, правовых аспектов деятельности учреждения, влияющих на ИБ.

Рассматриваются следующие вопросы:

- вопросы менеджмента ИБ: процедуры вовлечения персонала в процессы ИБ, участие и роль руководства, анализ и оценка штатной структуры учреждения в целом и подразделений, задействованных в вопросах обеспечения безопасности информации и влияния их на ИБ;
- порядок взаимодействия между подразделениями в ходе выполнения рабочих задач, имеющих влияние на ИБ учреждения, координация деятельности подразделений;
- состояние политик ИБ (регламентов, инструкций, процедур).

Это достаточно большая и важная часть аудита. Программа и методики аудита по данному вопросу содержат подробное описание проверяемых процедур, правил и политик. Оценка качества политик ИБ учреждения предусматривает детальную оценку каждого документа Заказчика и аналитическое обоснование его работоспособности, актуальности и соответствия НМД в области защиты информации в зависимости от категории информации и объекта информатизации. Итогом аудита данного направления является выдача детальных рекомендаций в отношении как имеющейся политики ИБ учреждения, так и по созданию и внедрению новых организационно-распорядительных, правовых и административных инструментов. По выбору заказчика оценка может проводиться на соответствие политик безопасности нормативно-методическим документам России, СМИБ (ГОСТ ИСО), отраслевым стандартам (ЦБР СТО БР ИББС и др.). Не маловажным является демонстрация по итогам анализа последствий отсутствия политик ИБ (либо наоборот демонстрация работоспособности политик и правил в части устранения реальных угроз безопасности информации);

- состояние документооборота: наличие, ведение закрытого (ограниченного) документооборота и правила работы с ним, рекомендации по организации такого документооборота, приём и передача документов ограниченного распространения, порядок уничтожения носителей, внутренний электронный документооборот, его роль и место в ИБ учреждения;
- оценка возможности сертификации учреждения в системе менеджмента информационной безопасности.

2.2. Обследование состояния ИТ инфраструктуры и инженерных систем:

- аудит процессов использования средств вычислительной техники, в том числе:

аудит безопасности домена на основе службы каталогов MS Active Directory, аудит FSMO ролей, позволит минимизировать негативные последствия выхода из строя контроллера домена с последующей разработкой рекомендаций по размещению FSMO-ролей, аудит объектов групповой политики в части аутентификации, авторизации, аудита (Group Policy Object, GPO), при помощи шаблонов безопасности позволит упростить выполнение задач администрирования, поскольку обеспечивает приведение к единой конфигурации безопасности заданного множества компьютеров в рамках одного домена, с последующей разработкой рекомендаций по настройке шаблонов GPO, аудит установленных обновлений ОС Microsoft (позволит выяснить установлены ли последние обновления безопасности и какие системы в них нуждаются, с последующей разработкой рекомендаций по установке и настройке Службы обновления Windows Server – Windows Server Update Services (WSUS), что позволит ИТ-администраторам централизованно развёртывать новейшие обновления продуктов Microsoft на компьютерах, работающих под управлением операционных систем семейства Windows), обследование Web и Почтового серверов; проверка настроек политики безопасности на серверах; обследование всех рабочих станций в офисе на предмет соблюдения правил информационной безопасности и возможности их использования инсайдерами в качестве инструмента атак;

- проверка возможности перехвата сетевых пакетов в локальной сети:

- построение актуальной «Карты» сети, обнаружение конфигураций "по умолчанию", обнаружение модемов, обнаружение других не задекларированных устройств.

Данная часть аудита позволит выдать следующие рекомендации:

рекомендации по нейтрализации уязвимостей (снижению возможного ущерба от их использования злоумышленниками);

рекомендации по изменению конфигурации и настроек компонентов АС, используемых защитных механизмов;

рекомендации по установке необходимых обновлений (patches, hot-fixes) установленного программного обеспечения;

рекомендации по изменению политик безопасности на Серверах и Рабочих станциях, в настройках файрволла.

- оценка установленного порядка обслуживания СКС (ЛВС);

- анализ состава и уязвимостей используемого штатного прикладного программного обеспечения:

- функции и процедуры, относящиеся к разным прикладным программам и несовместимые между собой (не функционирующие в одной операционной среде) из-за конфликтов, связанных с распределением ресурсов системы;

- функции, процедуры, изменение определенным образом параметров которых позволяет использовать их для проникновения в операционную среду ИСПДн и вызова штатных функций операционной системы, выполнения несанкционированного доступа без обнаружения таких изменений операционной системой;

- фрагменты кода программ («дыры», «люки»), введенные разработчиком, позволяющие обходить процедуры идентификации, аутентификации, проверки целостности и др., предусмотренные в операционной системе;

- отсутствие необходимых средств защиты (аутентификации, проверки целостности, проверки форматов сообщений, блокирования несанкционированно модифицированных функций и т.п.);

- ошибки в программах (в объявлении переменных, функций и процедур, в кодах программ), которые при определенных условиях (например, при выполнении логических переходов) приводят к сбоям, в том числе к сбоям функционирования средств и систем защиты информации, к возможности несанкционированного доступа к информации;

- анализ использования ССОП Интернет, определение точек подключения к Internet;

- оценка уровня безопасности при использовании корпоративной почты;

- обнаружение сетевых узлов: ping-сканирование, traceroute;

- определение сетевых приложений: сканирование портов, захват заголовков (network application banner grabbing);

- использование SNMP для профилирования целей и определения возможного местонахождения скрытых подключений к сети;

- тестирование защиты сетевых приложений:

службы каталогов и поиска: DNS, DHCP, LDAP, Finger, удаленные сеансы: Telnet, SSH, R-команды, X-Windows, совместное использование файлов: FTP, TFTP, SMB, NFS, отказ в обслуживании: сетевые лавины (network flooding), лавины пакетов установления соединения (SYN floods), распределенные атаки типа отказ в обслуживании (Distributed Denial of Service, DDoS),

- тестирования Web-сайтов:

локализация Web-серверов,идентификация Web-серверов, сканирование защиты Web-сайта при помощи сканеров Web-приложений,

- тестирования сетевых устройств;

- тестирования межсетевых экранов и защиты периметра:

- рассмотрение демилитаризованной зоны/периметра и конфигураций политики межсетевого экрана, локализация узлов в областях демилитаризованной зоны/периметра цели, профилирование и тестирование фильтрующего маршрутизатора;

- анализ уязвимостей ЭД, почтовых приложений;

- вопросы технического обслуживания, ремонта и т.п. имеющегося парка СВТ и создаваемые в ходе данных работ угрозы и уязвимости;

- оценка общего состояния ИТ инфрастуктуры и воздействие на критерии безопасности информации

- анализ схемы построения ЛВС, схем выхода в ССОП, структуры ЛВС, СКУД, ОПС

- состояние работы по использованию имеющихся в учреждении инструментов (ЛВС, СКУД, АТС и т.д.) для борьбы с инсайдом

- работа СКУД, правила и порядок работы с СКУД, ПС и ОС персонала

- угрозы, создаваемые применением УПАТС, ГТС, мобильных устройств.

2.3. Аудит деятельности основных подразделений учреждения и их сотрудников, задействованных в обеспечении информационной безопасности учреждения:

- подразделения или ответственного за ИБ (ТЗИ)
- ИТ подразделения и администраторов баз данных и специализированных приложений
- подразделения разработки и внедрения ПО
- подразделения делопроизводства
- подразделения режима и охраны
- подразделения кадровой работы

Методики оценки деятельности основаны на СМИБ (ГОСТ ИСО), оценке реальных показателей выполнения требований НМД и НПА РФ в области ИБ, знаний НПА и НМД в области ИБ (в том числе с использованием квалификационных справочников минтруда), количественных показателей в работе (в соответствии с методиками минтруда). Оценку осуществляют самые опытные специалисты Исполнителя, преподаватели согласованных с ФСТЭК и ФСБ России курсов повышения квалификации в области защиты информации и имеющие специализированное образование в области ИБ.

Рассматривается большой объём вопросов касающихся полномочий сотрудников, контроля за деятельностью сотрудников значительно влияющих на вопросы обеспечения ИБ, вопросы организации и планирования труда, вопросы работы сотрудников с инцидентами (в том числе с помощью разработанной совместно с заказчиком модели реальных инцидентов ИБ в том числе нештатных ситуаций и форс мажоров). Работы проводятся квалифицированными сотрудниками, разработавшими более сотни политик ИБ.

Аудит подверженности инсайдерской деятельности и социальной инженерии:

- оценка работы кадровых подразделений и руководителей подразделений;
- работа с сотрудниками учреждения с использованием полиграфа (детектора лжи) и метода компьютерного психосемантического анализа, основанного на способе психозондирования и реализуемого с помощью аппаратно-программного комплекса MinReader 2.0. В ходе данной работы проводится оценка по следующим направлениям:
- принадлежность кандидатов к определенным криминальным кругам;
- наличие или отсутствие недозволенных связей с конкурентами;
- степень лояльности к организации и руководству;
- использования служебного положения в корыстных целях, наносящих ущерб компании: сговор с клиентом, «откаты» и тому подобное;
- патологические мотивы (алкоголизация, наркомания, игровая зависимость, стремление к мести, склонность к неоправданному риску и т.п.);
- наличие личных проблем (неадекватное отношение к охраняемому лицу, долги, неадекватное отношение к оружию, проблемы с законом, семейные проблемы и т.п.);
- криминальные намерения кандидата.
- социальные пентесты (реальное моделирование проведения атак социальной инженерии на сотрудников учреждения по согласованным и описанным в программе и методиках сценариям).