Аудит систем и подсистем защиты информации

По следующим основным направлениям:

1. На соответствие СМИБ (ГОСТ ИСО), а именно следующим:

- ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»;
- ГОСТ Р ИСО /МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью».
- ГОСТ Р ИСО/МЭК 15408-1-2008, ГОСТ Р ИСО/МЭК 15408-2-2008, ГОСТ Р ИСО/МЭК 15408-3-2008 и др.

Программа и методика, согласованная с Заказчиком будет содержать подробное описание оценки рисков и других мероприятий по данному направлению.

2. На соответствие требованиям НПА и НМД РФ в области ИБ по пунктам определённым выше в рамках аудита по категориям защищаемых объектов информатизации.

Также возможен контроль эффективности системы защиты информации (аттестационные испытания) с использованием методик испытаний, действующих в РФ и ГОСТ РО 0043-003-2012 и ГОСТ РО 0043-004-2013, что логически является последним этапом оценки соответствия по данному пункту.

3. Аудит мер комплексной защиты объектов.

Состав рассматриваемых вопросов и осуществляемых мероприятий:

- анализ и оценка защищённости с использованием инструментальных средств (программного обеспечения): сканеров безопасности, программ проверки полномочий доступа и т.п.
- анализ эффективности и работоспособности политик ИБ, правил и процедур влияющих на обеспечение ИБ, в том числе оценка и анализ проведения следующих процедур и политик ИБ:
- резервного копирования и восстановления информации
- технического обслуживания, ремонта СВТ, СКС, СКУД и видеонаблюдения, инженерных коммуникаций
- политик межсетевого экранирования и организации удалённого доступа
- политик разграничения прав пользователей и доступа к ресурсам СВТ
- политики защиты от «суперпользователя»
- реагирование на форс-мажоры, технические сбои и т.п.
- парольные политики
- процедуры антивирусной защиты
- процедуры обнаружения вторжений и атак;
- обследование и оценка состояния эксплуатационной документации на средства защиты информации, эффективность использования и выполнение правил эксплуатации средств активной защиты (в том числе в разрезе требований Роскомнадзора), соблюдение требований по использованию средств криптографической защиты информации (в т.ч. рекомендации по работе удостоверяющих центров и т.п.);
- обследование состояния правил учёта и хранения СЗИ, в том числе СКЗИ;
- проверка лицензионных условий соискателя на лицензию ФСТЭК на деятельность по технической защите конфиденциальной информации и лицензию ФСБ на деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации). Аудит готовности будет проводиться на основании административных регламентов ФСТЭК и ФСБ, практического опыта сотрудников, проходивших данные процедуры, опыта работы сотрудников данных ФОИВ в запасе;
- анализ эффективности структуры управления системой защиты информации учреждения;
- анализ работы с носителями информации, состояния их учёта и правил эксплуатации;
- оценка правильности работы при выводе из эксплуатации как объекта информатизации в целом так и его частей и носителей информации;

- оценка знаний персоналом действующих политик ИБ и нормативно-методических актов, своего места и роли в процессах обеспечения ИБ.

- анализ и оценка подверженности имеющейся объектов учреждения промышленному шпионажу, в том числе:

- оценка возможности ведения оптической и фотографической разведки

- оценка состояния работ по контролю за границами контролируемой зоны

- оценка возможности ведения радиоразведки. В ходе данных работ возможно составление «радиокарты» района (здания, местности), радиоконтроль с применением современного оборудования в диапазоне частот до 30 ГГц с выявлением и детализацией всех радиосигналов на объектах. Данная информация в дальнейшем может позволять достаточно быстро выявлять возможные каналы утечки информации по радиоканалу.

- оценка возможности ведения акустической и виброакустической разведки (через ограждающие конструкции, слаботочные системы, инженерные коммуникации в том числе вентиляцию и систему отопления, окна).

- оценка возможности ведения компьютерная разведки (системы тематического поиска, программы-агенты, средства мониторинга, снифферы и т.п.)

- анализ угроз НДВ в ПО и выдача рекомендаций по их минимизации.

- анализ безопасного использования мобильных устройств с выдачей рекомендаций.

Программа и методики аудита в части определённых совместно с Заказчиком вопросов будут также содержать необходимость моделирования возможных атак противника, в ходе которого будут определяться места ближайшего расположения противника по отношению к защищаемым объектам, возможные направления и методы атак.