**Этапы и вопросы, рассматриваемые в рамках аудита (экспертизы) информационной безопасности**

**Аудит ИБ состоит из следующих этапов**

* сбор информации о состоянии нормативной, нормативно-правовой и организационно-распорядительной документации в области обеспечения информационной безопасности (далее – ИБ);
* сбор информации о потоках информации и состоянии безопасности локальной и корпоративной вычислительной сети;
* сбор информации о конфигурации безопасности рабочих станций;
* сбор информации о состоянии периметра безопасности информационно-коммуникационной инфраструктуры;
* сбор информации о соответствии серверного помещения нормативным документам в сфере ИБ.

**При сборе информации о состоянии нормативной, нормативно-правовой и организационно- распорядительной документации в области обеспечения ИБ, изучаются следующие документы:**

* Согласованная с Уполномоченным органом (Службой государственной безопасности Республики Узбекистан) и утвержденная политика информационной безопасности (далее – ИБ);
1. Письма согласования политики ИБ с Уполномоченным органом;
2. Журнал(ы) ознакомления сотрудников с политикой ИБ;
3. Наличие в политике ИБ матрицы доступа, реестра информационных ресурсов с указанием степени её критичности, перечня разрешённого программного обеспечения, парольной политики и др.
* План мероприятий, направленных на эффективное обеспечение ИБ

в организации на текущий год;

1. Подтверждающие записи об исполнении пунктов данного плана мероприятий;
* Отчетная документация о последнем проведенном аудите ИБ
по требованиям ИБ;
* Положение о специализированном подразделении по ИБ
* в организации и должностные инструкции данного подразделения или должностная инструкция ответственного(ых) сотрудника(ов) по ИБ
* Приказ о назначении ответственного сотрудника по ИБ
в организации;
* Перечень конфиденциальной информации;
* Соглашение с работниками о неразглашении конфиденциальной информации;
	+ Копии сертификатов соответствия лицензионных программных продуктов и аппаратного обеспечения ИС;
	+ Программа по подготовке и повышению осведомленности персонала в области ИБ: документы, подтверждающие прохождение обучения
	и повышения квалификации работников в области обеспечения ИБ;
	+ Сертификаты на средства криптографической защиты информации (если имеются);
	+ Перечень прикладного ПО общего и специального назначения;
	+ Перечень серверов, коммуникационного оборудования, установленного в ОИ, подлежащих аудиту по требованиям ИБ;
	+ Схема распределения серверов и рабочих станций по сегментам сети (топология);
	+ Регламент реагирования на инциденты ИБ в организации.

**При сборе информации о потоках информации и состоянии безопасности локальной и корпоративной вычислительной сети, изучаются следующие минимальные сведения исследуемого объекта информатизации:**

* Схематическое изображение технологических связей между подразделениями на уровне потоков обмена данными с указанием множеств подсетей и вычислительных устройств, входящих в состав информационной (автоматизированной) системы;
* Перечень критически важных данных, циркулирующих
в информационной системе исследуемого объекта информатизации;
* Состояние сетевой безопасности приложений, систем, интерфейсов и баз данных (включая среду функционирования сетевых и клиентских приложений);
* Состояние безопасности систем на уровне протокола TCP/IP при обращении с ресурсов, расположенных вне контролируемой зоны;
* Состояние сетевой безопасности устройств передачи трафика
по проводным и беспроводным каналам;
* Состояние соответствия систем мониторинга сетевой безопасности заявленным требованиям.

**При сборе информации о конфигурации безопасности рабочих станций, исследуются следующие минимальные требования:**

* Идентификационные данные пользователей и рабочих станций, позволяющие идентифицировать исследуемый объект (ФИО, инв.№, и т.д.);
* Сетевые идентификационные параметры рабочей станции (MAC-адрес, IP-адрес, имя компьютера и т.д.);
* Сведения об установленном программном обеспечении;
* Сведения о состоянии использования сетевых портов c сервисами, функционирующих на рабочей станции;
* Сведения об использовании средств удалённого доступа пользователями рабочих станций;
* Сведения о способах разграничения прав доступа к системам, используемым на рабочих станциях;
* Информация о политике использования средств межсетевого экранирования, определённая на рабочей станции;
* Сведения о конфигурации, используемого на рабочей станции антивирусного программного обеспечения;
* Сведения о соответствии перечня установленного программного обеспечения, утверждённого организацией –владельцем;
* Сведения о следах пользования средствами анонимизации трафика;
* Сведения о следах пользования средствами доступа в сеть Интернет
с использованием различных устройств, средств, методов (в обход систем контроля сетевого трафика организации) пользователем;
* Сведения о сетевой активности пользователей рабочих станций
(в том числе, пользования сервисов социальных сетей и средств обмена информацией посредством систем, сервера которых расположены вне контролируемой зоны);
* Сведения о хранении пользователем на рабочей станции конфиденциальной и иной чувствительной информации;
* Сведения о политике разграничения доступа к средствам чтения-записи информации пользователями на электронные носители;
* Эстетическая и техническая целостность рабочего места пользователя, а также кабельных систем коммуникации;
* Сведения о наличии исправных средств обеспечения резервного электрического питания рабочей станции при сбоях, а также средств ограничения физического доступа к внутренним компонентам персонального компьютера;
* Сведения о парольной политике, установленной на рабочей станции.

**При сборе информации о состоянии периметра безопасности информационно-коммуникационной инфраструктуры, изучаются следующие вопросы:**

* Наличие физической охраны (штат охраны) на исследуемом объекте информатизации;
* Организация (контроль) процесса входа-выхода посетителей
на территорию здания, где расположена информационно-коммуникационная инфраструктура объекта;
* Наличие системы охранной сигнализации в точках проникновения на территорию здания, где расположен исследуемый объект информатизации;
* Наличие системы пожарной сигнализации на территории здания,
где расположен исследуемый объект информатизации;
* Проведение постоянной проверки исправности систем пожарной
и охранной сигнализации в установленном порядке;
* Наличие системы видеонаблюдения на территории здания,
где расположен исследуемый объект информатизации;
* Наличие «слепых» зон системы видеонаблюдения, позволяющих злоумышленникам беспрепятственно совершать действия, направленные на компрометацию системы безопасности исследуемого объекта;
* Наличие автоматизированных систем контроля и управления доступом на территорию здания;
* Наличие средств защищенного хранения бумажной и цифровой документированной информации;
* Наличие источников бесперебойного питания мощностью, достаточной для питания критических узлов системы.

**При сборе информации о серверном помещении, собираемых при проведении аудита ИБ, изучаются следующие вопросы:**

* Организация, адрес здания и расположение серверного помещения;
* Наличие внешних стен и оконных проемов;
* Система контроля доступа в серверную;
* Вид замка и двери;
* Железная решетка на оконных проёмах;
* Камеры системы видеонаблюдения;
* Датчики системы охранной сигнализации;
* Датчики системы пожарной сигнализации;
* Наличие системы пожаротушения;
* Состояние сетевых кабелей;
* Состояние кабелей питания;
* Наличие бесперебойных источников питания;
* Система кондиционирования и её питание;
* Наличие термометра и влагомера;
* Наличие системы удалённого мониторинга климата;
* Освещение серверной и её питание
* Наличие трубопроводов в помещении;
* Фальшпол или фальшпотолок;
* Наличие лотков оттока жидкости в случае прорыва трубопровода;
* Журнал вноса-выноса оборудования;
* Журнал выполненных действий;
* Журнал изменения конфигураций;
* Наличие лишних предметов;
* Наличие отдельного от здания заземление;
* Распределительные щиты питания серверной;
* Система газо-дымо-удаления пожаротушения;
* Табло и рычаг извещателя о пожаре внутри серверной;
* Сетевое и серверное оборудование в закрытых стойках;
* Датчики в закрытых стойках;
* Огнетушитель.