Аудит обеспечения безопасности информации, обрабатываемой в определённых защищаемых объектах информатизации по типам и категориям объектов.

3.1. ИСПДн.

3.1.1. Оценка полноты организации правовых и организационных мер во исполнение законодательства в области защиты персональных данных, а именно:

- анализ представленного в Роскомнадзор уведомления об обработке (о намерении осуществлять обработку) персональных данных;
- анализ соответствия содержания и объема обрабатываемых персональных данных заявленным целям обработки;
- выявление случаев, когда обработка персональных данных правомерна только при наличии согласия субъекта персональных данных;
- анализ соответствия имеющихся образцов форм согласия субъектов персональных данных требованиям законодательства;
- проверка соответствия порядка обработки персональных данных, осуществляемой без использования средств автоматизации, требованиям законодательства;
- проверка соответствия договоров с третьими лицами, содержащих поручение обработки персональных данных, требованиям законодательства.

3.1.2. Аудит подготовленности к проверке Роскомнадзора.

3.1.3. Аудит соответствия единой отраслевой технической политике и требованиям отраслевых методических документов (в сфере образования, в сфере энергетики и жкх и т.д.).

3.1.4. Обследование состояния технической защиты информации и выполнения требований ФСБ России и ФСТЭК России в области защиты ИСПДн:

- устанавливается необходимость обработки ПДн и обоснованность обрабатываемого перечня ПДн на данном объекте информатизации;
- определяются (уточняются) угрозы безопасности информации и модель вероятного нарушителя применительно к конкретным условиям функционирования;
- определяются условия расположения объектов информатизации относительно границ КЗ;
- определяются конфигурация и топология автоматизированных систем и систем связи в целом и их отдельных компонент, физические, функциональные и технологические связи как внутри этих систем, так и с другими системами различного уровня и назначения;
- определяются технические средства и системы, предполагаемые к использованию и системах связи, условия их расположения, общесистемные и прикладные программные средства;
- определяются режимы обработки информации в ИСПДн в целом и в отдельных компонентах;
- определяется уровень защищенности ИСПДн;
- определяется степень участия персонала в обработке (обсуждении, передаче, хранении) информации.

В результате аудита выдаются:

- описание ИСПДн и существующей системы мер по защите информации, описание технологии обработки информации;
- заключение о соответствии организационной документации в области защиты информации и принятых административно-правовых и организационно-режимных мер действующим требованиям в области защиты персональных данных;
- рекомендации по доработке организационно-распорядительной документации Заказчика в части защиты персональных данных, в том числе в соответствии с изменениями законодательства в области защиты персональных данных текущего года;
- техническое задание на создание системы защиты информационных систем персональных данных Заказчика с расчётом стоимости работ.

3.2. ОВТ, обрабатывающие служебную тайну и другую конфиденциальную информацию.

Проверка состояния защиты информации и выдача рекомендаций по защите информации по следующим каналам утечки информации:

3.2.1. Побочные электромагнитные излучения информативного сигнала от технических средств и линий передачи информации.
3.2.2. Наводки информативного сигнала, обрабатываемого техническими средствами, на провода и линии, выходящие за пределы контролируемой зоны объектов информатизации (на линии вспомогательных технических средств и систем, на цепи заземления и электропитания).
3.2.3. Изменения тока потребления, коррелированные с обрабатываемыми техническими средствами информативными сигналами.
3.2.4. Радиоизлучения, модулированные информативным сигналом, возникающие при наличии паразитной генерации в узлах (элементах) технических средств.
3.2.5. Съем информации путем контактного или индукционного подключения к кабельным линиям связи.
3.2.6. Несанкционированный доступ к информации, обрабатываемой в автоматизированных системах.
3.2.7. Съем информации с аппаратных средств ЭВТ, автоматизированных систем при их передаче в другие организации, сдаче в ремонт и т.д.
3.2.8. Просмотр информации с экранов дисплеев и других средств ее отображения с помощью оптических средств.
3.2.9. Воздействие (физическое, дистанционное, электромагнитное и т.д.) на технические или программные средства в целях нарушения целостности (уничтожения, искажения) информации, работоспособности технических средств, средств защиты информации, адресности и своевременности информационного обмена, в том числе через специально внедренные электронные и программные средства («закладки»).

3.3. Защищаемые помещения руководства учреждений, в которых воспроизводится конфиденциальная информация.
3.3.1. Анализ на предмет утечки по следующим техническим каналам:
- Акустическое излучение информативного речевого сигнала, которое может быть зарегистрировано путем непосредственного прослушивания акустических сигналов, а также в результате перехвата аппаратурой на основе направленных микрофонов.
- Вибрационные сигналы, возникающие посредством преобразования информативного акустического сигнала при воздействии его на строительные конструкции и инженерно-технические коммуникации выделенных помещений, перехват которых может осуществляться контактными микрофонами - стетоскопами и оптико-электронной (лазерной) аппаратурой.
- Электрические сигналы, возникающие посредством преобразования информативного сигнала из акустического в электрический за счет микрофонного эффекта и распространяющиеся по проводам и линиям передачи информации.
- Радиоизлучения, модулированные информативным речевым сигналом, возникающие при работе различных генераторов, входящих в состав технических средств, или при наличии паразитной генерации технических средств.
- Канал утечки речевой информации, обусловленный воздействием на технические средства высокочастотных сигналов, создаваемых с помощью разведывательной аппаратуры, по эфиру и проводам, либо сигналов промышленных радиотехнических устройств (радиовещательные, радиолокационные станции, средства радиосвязи и т.п.), и модуляцией их информативным речевым сигналом.
3.3.2. Анализ угроз утечки информации за счёт внедрения закладочных устройств негласного съёма-передачи информации и выдача рекомендаций по минимизации угроз внедрения закладочных устройств (при учёте в программе и методике проведения аудита возможно привлечение специалистов лицензиата ФСБ России на оказание услуг по выявлению устройств негласного съёма передачи информации в помещениях и технических средствах).
3.3.3. Анализ наличия технических средств, создающих технические каналы утечки информации и рекомендации по штатному применению используемых технических средств.

3.4. Ключевые системы информационной инфраструктуры (далее КСИИ) и автоматизированные системы управления технологическими процессами (далее АСУ ТП).
Аудит на соответствие требованиям следующих документов:
«Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 18.05.2007);

- «Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 18.05.2007);
- «Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 18.05.2007);
- «Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 19.11.2007)

3.5. Объекты, обрабатывающие государственную тайну (ВП и ОВТ).

Аудит осуществляется по трём основным направлениям: обеспечение технической защиты информации, обеспечение требований к обработке сведений, составляющих государственную тайну и выполнение лицензионных требований к организации, обрабатывающей сведения, составляющие государственную тайну.

Проверка обеспечения технической защиты информации на объектах информатизации осуществляется по перечню вопросов, изложенных в следующих НПА РФ :

- Федеральный закон от 21.07.1993 №5485-1 «О государственной тайне»;
- «Положение о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам», утвержденное постановлением Совета Министров-Правительства РФ от 15.04.1993 № 912-51;
- «Специальные требования и рекомендации по защите информации, составляющей государственную тайну от утечки по техническим каналам», утвержденные решением Гостехкомиссии России от 23 мая 1997 года №55 (СТР-97).

Проверка обеспечение требований к обработке сведений, составляющих государственную тайну осуществляется на предмет выполнения «Инструкции по обеспечению режима секретности в Российской Федерации» от 05.01.2004 № 3-1.

3.6. Государственные и муниципальные информационные системы (далее ГИС (МИС)).

Оценка полноты организации систем защиты информации в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и приказа ФСТЭК России № 17 от 11.02.2013г. "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах".

Аудит выполнения требований нормативно-правовых актов субъекта РФ в области информационной безопасности, в том числе рекомендации по соответствию единой технической политике в области ИБ автономного округа при построении защищённых сегментов и конечных пунктов систем межведомственного взаимодействия.

3.7. Объекты вычислительной техники, обрабатывающую информацию по переводу денежных средств, банковскими платежными агентами (субагентами), операторами платежных систем и операторами услуг платежной инфраструктуры в платежной системе.

Кроме проверки выше изложенных требований к обеспечению защиты информации в ИСПДн и ГИС (МИС) аудит осуществляется на предмет выполнения требований следующих НМД РФ:

Федеральный закон от 27 июня 2011 года N 161-ФЗ "О национальной платежной системе";

Постановление Правительства РФ от 13.06.2012 N 584"Об утверждении Положения о защите информации в платежной системе";

«Положение о требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации», зарегистрировано в Минюсте России 14 июня 2012 г. N 24575;

Письма и распоряжения ЦБ РФ об обеспечении ИБ.

3.8. В процессе проведения обследования любого из типов указанных выше объектов защиты учреждения осуществляется постоянное моделирование и оценка существующих современных угроз ИБ. Кроме выявленных угроз ИБ в рамках исполнения пунктов аудита из других частей (глав) применительно к каждому из определённых для защиты объектов (ОВТ, помещения) составляется анализ опасности реализации следующих угроз безопасности информации:

Угрозы конфиденциальности			Угрозы целостности	Угрозы доступности
Угрозы утечки информации по техническим каналам	**Угрозы конфиденциальности информации за счёт НСД к ней**	**Угрозы конфиденциальности информации за счёт действий внутреннего нарушителя (пользователя, имеющего санкционированный доступ)**		
побочные электромагнитные излучения информативных сигналов от технических средств и линий передачи информации	угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/ вывода (BIOS), перехват управления загрузкой внутренним нарушителем (имеющим доступ к техническим средствам ОИ и не имеющих доступ к информации)	угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (копирование, перемещение) операционной системы или какой-либо прикладной программы (например, системы управления базами данных), с применением специально созданных для выполнения НСД программ внутренним нарушителем	угроза непреднамеренных действий пользователей, приводящих к нарушению безопасности функционирования ОИ и СЗИ в ее составе (неумышленная порча оборудования, удаление, искажение программ или файлов с важной информацией, в том числе системных, повреждение каналов связи, неумышленная порча носителей информации и т.п.) и непреднамеренный запуск либо технологических программ, способных при некомпетентном использовании, вызывать потерю работоспособности системы (зависания или зацикливания) или осуществляющих необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.) либо вредоносных программ (программно-математического воздействия) и программных "закладок"	блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку
наводки информативного сигнала, обрабатываемого техническими средствами, на цепи электропитания и линии связи, выходящие за пределы служебных	угроза доступа к остаточной информации (включая бумажные черновики, гибкие магнитные диски) и восстановления удалённых файлов	несанкционированное копирование информации на незарегистрированный носитель информации со стороны лиц, имеющих право доступа к защищаемой информации для передачи (разглашения), а также передача паролей, идентификаторов	угрозы неатропогенного характера (сбоев аппаратуры и программного обеспечения из-за ненадежности элементов и непреднамеренных действий пользователей, сбоев электропитания) и	угроза доступности к информации из-за сбоев в программном обеспечении, а также от угроз неатропогенного (сбоев аппаратуры и программного обеспечения из-за ненадежности

Угрозы конфиденциальности			Угрозы целостности	Угрозы доступности
Угрозы утечки информации по техническим каналам	**Угрозы конфиденциальности и информации за счёт НСД к ней**	**Угрозы конфиденциальности информации за счёт действий внутреннего нарушителя (пользователя, имеющего санкционированный доступ)**		
помещений			стихийного (ударов молний, пожаров, наводнений и т.п.) характера.	элементов и непреднамеренных действий пользователей, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера
радиоизлучения, модулированные информативным сигналом, возникающие при работе различных генераторов, входящих в состав технических средств ИСПДн, или при наличии паразитной генерации в узлах (элементах) технических средств	угрозы «Анализа сетевого трафика» с перехватом передаваемой во внешние и принимаемой из внешних сетей информации	утрата носителя с информацией	уничтожения, хищения аппаратных средств ОИ носителей информации путем физического доступа к элементам ОИ лицами, не имеющими легального доступа в помещение, где последние хранятся	блокирования информации за счет НСД с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)
угрозы утечки видовой информации за счет просмотра информации с помощью оптических (оптикоэлектронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, входящих в состав ОИ	угрозы удаленного запуска приложений и выявления паролей с помощью программных закладок, внедряемых со стороны ССОП		угрозы создания нештатных режимов работы программных (программно-аппаратных) средств за счет преднамеренных изменений служебных данных, игнорирования предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, искажения (модификации) самих данных и т.п	
	угрозы получения НСД путем подмены доверенного объекта		угрозы внедрения вредоносных программ (программно-математического воздействия) и программных "закладок" со стороны внешнего нарушителя,	

Угрозы конфиденциальности			Угрозы целостности	Угрозы доступности
Угрозы утечки информации по техническим каналам	**Угрозы конфиденциальности информации за счёт НСД к ней**	**Угрозы конфиденциальности информации за счёт действий внутреннего нарушителя (пользователя, имеющего санкционированный доступ)**		
			использующего методы социальной инженерии в отношении пользователей	
угрозы внедрения по сети вредоносных программ				
			угрозы типа «Отказ в обслуживании».	
угрозы сканирования, направленные на выявление уязвимостей ОИ, сетевых адресов рабочих станций, открытых портов и служб, открытых соединений и др.				

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.