

**УТВЕРЖДЕНЫ**

**Приказом ПАО «НК «Роснефть»**

**от «26» декабря 2019 г. № 861**

**Введены в действие «26» декабря 2019 г.**

**ВВЕДЕНЫ В ДЕЙСТВИЕ**

**с «13» января 2020 г.**

**Приказом ООО «Славнефть-Красноярскнефтегаз» от «13» января 2020 г. № 7**

|  |
| --- |
| **МЕТОДИЧЕСКИЕ УКАЗАНИЯ КОМПАНИИ** |

**Требования и рекомендации по технической защите**

**речевой конфиденциальной информации**

**№ П3-11.01 М-0037**

**ВЕРСИЯ 1.00**

**МОСКВА**

**2019**

# СОДЕРЖАНИЕ

[**ВВОДНЫЕ ПОЛОЖЕНИЯ 3**](#_Toc18582035)

[НАЗНАЧЕНИЕ 3](#_Toc18582036)

[ОБЛАСТЬ ДЕЙСТВИЯ 3](#_Toc18582037)

[ПЕРИОД ДЕЙСТВИЯ И ПОРЯДОК ВНЕСЕНИЯ ИЗМЕНЕНИЙ 4](#_Toc18582038)

[**1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ 5**](#_Toc18582039)

[**2. ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ 8**](#_Toc18582040)

[**3. ОБЩИЕ ПОЛОЖЕНИЯ 9**](#_Toc18582041)

[3.1. ОБЪЕКТЫ ЗАЩИТЫ РЕЧЕВОЙ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, КАНАЛЫ УТЕЧКИ РЕЧЕВОЙ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ 9](#_Toc18582042)

[3.2. ОРГАНИЗАЦИЯ И ПРОВЕДЕНИЕ РАБОТ ПО ЗАЩИТЕ РЕЧЕВОЙ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ 10](#_Toc18582043)

[3.3. ОРГАНИЗАЦИЯ И ПРОВЕДЕНИЕ РАБОТ ПО ЗАЩИТЕ РЕЧЕВОЙ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЯХ 11](#_Toc18582044)

[3.4. ОРГАНИЗАЦИЯ И ПРОВЕДЕНИЕ РАБОТ ПО ЗАЩИТЕ РЕЧЕВОЙ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В ПОМЕЩЕНИЯХ ДЛЯ СОВЕЩАНИЙ КОМПАНИИ 13](#_Toc18582045)

[**4. ТРЕБОВАНИЯ И РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ РЕЧЕВОЙ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ 15**](#_Toc18582046)

[4.1. ОБЩИЕ ПОЛОЖЕНИЯ 15](#_Toc18582047)

[4.2. ОСНОВНЫЕ ТРЕБОВАНИЯ И РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ, ЦИРКУЛИРУЮЩЕЙ В ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЯХ 15](#_Toc18582048)

[4.3. ОСНОВНЫЕ ТРЕБОВАНИЯ И РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ, ЦИРКУЛИРУЮЩЕЙ В ПОМЕЩЕНИЯХ ДЛЯ СОВЕЩАНИЙ 17](#_Toc18582049)

[4.4. ЗАЩИТА ИНФОРМАЦИИ, ЦИРКУЛИРУЮЩЕЙ В СИСТЕМАХ ЗВУКОУСИЛЕНИЯ И ЗВУКОВОГО СОПРОВОЖДЕНИЯ ВИДЕОИНФОРМАЦИИ 18](#_Toc18582050)

[4.5. ЗАЩИТА ИНФОРМАЦИИ ПРИ ПРОВЕДЕНИИ АУДИО- И ВИДЕОЗАПИСИ 19](#_Toc18582051)

[**5. ССЫЛКИ 21**](#_Toc18582052)

# ВВОДНЫЕ ПОЛОЖЕНИЯ

НАЗНАЧЕНИЕ

Настоящие Методические указания устанавливают порядок организации работ по технической защите речевой конфиденциальной информации, циркулирующей на объектах информатизации (защищаемых помещениях и помещениях для совещаний) Компании, а также устанавливают требования и рекомендации по предотвращению утечки речевой конфиденциальной информации по техническим каналам и циркулирующей в системах звукоусиления и звукового сопровождения видеоинформации.

Настоящие Методические указания разработаны с учетом требований:

* ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»;
* ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения»;
* ГОСТ РО 0043-004-2013 «Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний»;
* нормативно-методического документа «Специальные требования и рекомендации по технической защите конфиденциальной информации», утвержденного приказом Гостехкомиссии России от 30.08.2002 № 282,

и других нормативных правовых актов по защите информации.

ОБЛАСТЬ ДЕЙСТВИЯ

Настоящие Методические указания обязательны для исполнения работниками:

* Службы безопасности ПАО «НК «Роснефть»;
* структурных подразделений ПАО «НК «Роснефть»;
* подконтрольных ПАО «НК «Роснефть» Обществ Группы, зарегистрированных на территории Российской Федерации (за исключением Обществ, в которых отсутствует списочный состав и/или по которым приняты решения о реализации процедуры ликвидации/банкротства), в отношении которых Уставами Обществ, акционерными и иными соглашениями с компаниями-партнерами не определен особый порядок реализации акционерами/участниками своих прав, в том числе по управлению Обществом,

при организации и проведении работ по обеспечению технической защиты речевой конфиденциальной информации в Компании.

Структурные подразделения ПАО «НК «Роснефть» и Общества Группы при оформлении договоров со специализированными организациями, оказывающими услуги по защите речевой конфиденциальной информации, обязаны включать в договоры соответствующие условия для соблюдения специализированной организацией требований, установленных настоящими Методическими указаниями.

Настоящие Методические указания носят рекомендательный характер для исполнения работниками иных Обществ Группы, не являющихся подконтрольными ПАО «НК «Роснефть» Обществами Группы.

Требования Методических указаний становятся обязательными для исполнения в подконтрольном ПАО «НК «Роснефть» Обществе Группы и ином Обществе Группы после их введения в действие в Обществе Группы в соответствии с Уставом Общества Группы с учетом специфики условий договоров или соглашений о совместной деятельности и в установленном в Обществе Группы порядке.

Распорядительные, локальные нормативные и иные внутренние документы не должны противоречить настоящим Методическим указаниям.

ПЕРИОД ДЕЙСТВИЯ И ПОРЯДОК ВНЕСЕНИЯ ИЗМЕНЕНИЙ

Настоящие Методические указания являются локальным нормативным документом постоянного действия.

Настоящие Методические указания утверждаются, вводятся в действие, изменяются и признаются утратившими силу в ПАО «НК «Роснефть» на основании приказа   
ПАО «НК «Роснефть».

1. **ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ**

**ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ КОРПОРАТИВНОГО ГЛОССАРИЯ**

***АТТЕСТАЦИОННЫЕ ИСПЫТАНИЯ*** *–* определение количественных и качественных характеристик объекта информатизации и его системы защиты информации с целью оценки их соответствия требованиям безопасности информации [ГОСТ РО 0043-004-2013]*.*

***ВСПОМОГАТЕЛЬНЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА И СИСТЕМЫ (ВТСС)*** *–* технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации, устанавливаемые совместно с основными техническими средствами и системами в защищаемых помещениях [ГОСТ РО 0043-004-2013].

*Примечание: к ним относятся:*

* *телефонные средства и системы;*
* *средства и системы передачи данных в системе радиосвязи;*
* *средства и системы охранной и пожарной сигнализации;*
* *средства и системы оповещения и сигнализации;*
* *контрольно-измерительная аппаратура;*
* *средства и системы кондиционирования;*
* *средства и системы проводной радиотрансляционной сети и приема программ радиовещания и телевидения (абонентские громкоговорители, системы радиовещания, телевизоры и радиоприемники и т.д.);*
* *средства электронной оргтехники;*
* *средства и системы электрочасофикации;*
* *иные технические средства и системы.*

***ЗАКЛАДОЧНОЕ УСТРОЙСТВО*** – элемент средства съема информации или воздействия на неё, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации [Рекомендации по стандартизации. Техническая защита информации. Основные термины и определения. № Р 50.1.056-2005].

***ЗАЩИЩАЕМАЯ ИНФОРМАЦИЯ*** – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями,  устанавливаемыми собственником информации [ГОСТ Р 50922-2006].

***ИНФОРМАТИВНЫЙ СИГНАЛ*** – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта защищаемая информация, передаваемая, хранимая или обрабатываемая в основных технических средствах и системах и обсуждаемая в выделенных (защищаемых) помещениях   
[ГОСТ РО 0043-004-2013].

***КОНФИДЕНЦИАЛЬНАЯ ИНФОРМАЦИЯ (СВЕДЕНИЯ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА)*** – сведения, содержащие информацию, составляющую коммерческую тайну Компании, информацию, являющуюся информацией «Для служебного пользования», инсайдерскую информацию, а также персональные данные.

***ОСНОВНЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА И СИСТЕМЫ (ОТСС)*** – технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи информации конфиденциального характера [ГОСТ РО 0043-004-2013].

*Примечание: к ним относятся в контексте данных Методических указаний:*

* *средства и системы звукового усиления речевой информации;*
* *средства и системы звукового сопровождения видеоинформации.*

***ОБЪЕКТ ИНФОРМАТИЗАЦИИ*** – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров [ГОСТ Р 51275-2006].

*Примечание: в контексте настоящих Методических указаний термин объект информатизации означает защищаемое помещение и помещение для совещаний.*

***СРЕДСТВО ЗАЩИТЫ ИНФОРМАЦИИ (СЗИ)*** – техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации [ГОСТ Р 50922-2006].

***СРЕДСТВА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ*** – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

***СТОРОННЯЯ ОРГАНИЗАЦИЯ*** – [организация, не являющаяся дочерним (иным) обществом ПАО «НК «Роснефть» или дочерним (иным) обществом его дочерних обществ.](javascript:term_view(17742))

***ТРЕБОВАНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ*** – требования, выполнение которых позволяет защитить информацию от утечки по техническим каналам, от несанкционированного доступа и от специальных воздействий на неё и её носители [ГОСТ РО 0043-003-2012].

**ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ ДЛЯ ЦЕЛЕЙ НАСТОЯЩЕГО ДОКУМЕНТА**

***АТТЕСТАЦИЯ ЗАЩИЩАЕМОГО ПОМЕЩЕНИЯ*** – комплекс организационных и технических мероприятий, в результате которых подтверждается соответствие системы защиты информации защищаемого помещения требованиям безопасности информации.

***ЗАЩИЩАЕМОЕ ПОМЕЩЕНИЕ (ЗП)*** – помещение (служебный кабинет, актовый, конференц-зал и т.д.), специально предназначенное для проведения конфиденциальных мероприятий (совещаний, обсуждений, переговоров и т.п.), аттестованное по требованиям безопасности информации, установленным Федеральной службой по техническому и экспортному контролю.

***ИНСТРУМЕНТАЛЬНАЯ ПРОВЕРКА*** *–* комплекс мероприятий по защите речевой информации, направленных на поиск и выявление электронных закладочных устройств съема речевой информации, а также технических каналов утечки речевой информации.

***КОНТРОЛИРУЕМАЯ ЗОНА (КЗ)*** – пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание работников и посетителей ПАО «НК «Роснефть» или Общества Группы, а также транспортных средств.

***МЕРОПРИЯТИЯ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА*** – мероприятия (совещания, переговоры и т.п.), при проведении которых обсуждается информация, составляющая коммерческую тайну Компании, информация, являющаяся информацией «Для служебного пользования», инсайдерская информация, а также персональные данные.

***ПОМЕЩЕНИЕ ДЛЯ СОВЕЩАНИЙ (ПС)*** – помещение (служебный кабинет, актовый, конференц-зал и т.д.), предназначенное для проведения конфиденциальных мероприятий (совещаний, обсуждений, переговоров и т.п.), прошедшее экспертную оценку и имеющее положительное экспертное заключение.

***ПОДРАЗДЕЛЕНИЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ (ПЭБ)*** – структурное подразделение Общества Группы, ответственное за обеспечение экономической безопасности Общества Группы.

***СИСТЕМА ЗВУКОВОГО УСИЛЕНИЯ (СЗУ)*** –система, включающая в себя микрофоны, усилительные устройства и динамики, обеспечивающая усиление уровня речевого сигнала, циркулирующего в защищаемом помещении, до требуемой величины, которая считается комфортной для восприятия участниками конфиденциальных мероприятий (совещаний, обсуждений, переговоров и т.п.), расположенными в защищаемом помещении.

***СИСТЕМА ЗВУКОВОГО СОПРОВОЖДЕНИЯ ВИДЕОИНФОРМАЦИИ (СЗСВ)*** –система, функционирующая автономно в пределах ограждающих конструкций защищаемого помещения, и обеспечивающая передачу звукового сигнала, соответствующего передаваемой на экране устройства отображения видеоинформации, участникам конфиденциального мероприятия, расположенным в защищаемом помещении.

***СПЕЦИАЛЬНЫЕ ИССЛЕДОВАНИЯ*** - комплекс мероприятий в области защиты информации, выполняемый организацией, имеющей лицензию Федеральной службы по техническому и экспортному контролю на проведение данных мероприятий, с использованием контрольно-измерительной аппаратуры по выявлению возможных технических каналов утечки защищаемых сведений (конфиденциальной информации) от основных и вспомогательных технических средств и систем.

***СПЕЦИАЛИЗИРОВАННАЯ ОРГАНИЗАЦИЯ*** – организация, имеющая лицензию Федеральной службы безопасности РФ на специальную проверку технических средств, а также лицензию Федеральной службы по техническому и экспортному контролю по технической защите конфиденциальной информации, предусматривающую возможность выполнения перечня работ и услуг: контроль защищенности конфиденциальной информации от утечки по техническим каналам в защищаемых помещениях; установка, монтаж, испытания, ремонт средств защиты информации; аттестационные испытания и аттестация на соответствие требованиям по защите информации защищаемых помещений.

1. ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

***АТС*** – автоматическая телефонная станция.

***заказчик*** – структурное подразделение ПАО «НК «Роснефть» или Общества Группы, по договору с которым производятся работы по обеспечению технической защиты конфиденциальной информации в Компании.

***ЗАЩИТА (КОНФИДЕНЦИАЛЬНОЙ) ИНФОРМАЦИИ*** -защита речевой конфиденциальной информации.

***КОМПАНИЯ*** – группа юридических лиц различных организационно - правовых форм, включая ПАО «НК «Роснефть», в отношении которых последнее выступает в качестве основного или преобладающего (участвующего) общества.

***ЛНД*** - локальный нормативный документ.

***ОБЩЕСТВО ГРУППЫ (ОГ)*** – хозяйственное общество, прямая и (или) косвенная доля владения ПАО «НК «Роснефть» акциями или долями в уставном капитале которого составляет 20 процентов и более.

***РЕЧЕВАЯ ИНФОРМАЦИЯ*** – речевая конфиденциальная информация.

***РУКОВОДИТЕЛЬ ОГ –*** единоличный исполнительный орган Общества Группы.

***CБ –*** Служба безопасности ПАО «НК «Роснефть».

***СТРУКТУРНОЕ ПОДРАЗДЕЛЕНИЕ (СП)*** – структурное подразделение с самостоятельными функциями, задачами и ответственностью в рамках своих компетенций, определенных положением о структурном подразделении.

***ТОП-МЕНЕДЖЕРЫ ПАО «НК «Роснефть»*** -первые вице-президенты ПАО «НК «Роснефть», вице-президенты ПАО «НК «Роснефть», главный бухгалтер ПАО «НК «Роснефть», финансовый директор ПАО «НК «Роснефть», пресс-секретарь ПАО «НК «Роснефть», советники и руководители структурных подразделений ПАО «НК «Роснефть» в ранге вице-президентов, руководители служб ПАО «НК «Роснефть» в ранге вице-президентов.

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящие Методические указания определяют объекты защиты (конфиденциальной) информации и организационные и технические мероприятия по защите (конфиденциальной) информации от утечки по техническим каналам.

Настоящие Методические указания устанавливают:

* порядок организации и проведения работ по защите (конфиденциальной) информации в ЗП и ПС;
* основные требования и рекомендации по защите (конфиденциальной) информации, циркулирующей в ЗП и ПС;
* состав организационно-распорядительной, технической и иной документации по защите (конфиденциальной) информации;
* требования по защите информации, циркулирующей в СЗУ и СЗСВ, а также при проведении аудио- и видеозаписи.
  1. ОБЪЕКТЫ ЗАЩИТЫ РЕЧЕВОЙ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, КАНАЛЫ УТЕЧКИ РЕЧЕВОЙ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ
  2. Защите подлежит речевая информация, циркулирующая в ЗП, в ПС, в СЗУ, а также звуковая информация в СЗСВ, расположенных в ЗП.

Объектами защиты при этом являются:

* ЗП;
* технические средства и системы (СЗУ/СЗСВ) как обрабатывающие речевую/звуковую информацию (ОТСС), так и не обрабатывающие непосредственно речевую информацию, но размещенные в ЗП и ПС (ВТСС);
* ПС.
  1. При ведении переговоров и использовании СЗУ и СЗСВ возможны следующие технические каналы утечки информации:
* акустическое излучение речевого информативного сигнала;
* электрические сигналы, возникающие при преобразовании информативного сигнала из акустического в электрический за счет микрофонного эффекта и распространяющиеся по проводам и линиям, выходящим за пределы КЗ;
* виброакустические сигналы, возникающие при преобразовании информативного акустического сигнала за счет воздействия его на строительные конструкции и инженерно-технические коммуникации ЗП;
* прослушивание разговоров за счет скрытного подключения к различным видам связи;
* побочные электромагнитные излучения информативных сигналов от технических средств и линий передачи речевой информации;
* наводки информативного сигнала, обрабатываемого техническими средствами, на цепи электропитания и линии связи, выходящие за пределы КЗ;
* радиоизлучения, модулированные информативным сигналом, возникающие при работе различных генераторов, входящих в состав технических средств, или при наличии паразитной генерации в узлах (элементах) технических средств;
* радиоизлучения или электрические сигналы от внедренных в технические средства и защищаемые помещения специальных электронных устройств съема речевой информации (закладочные устройства), модулированные информативным сигналом.
  1. Перехват информации с использованием технических средств может вестись:
* из-за границы КЗ из близлежащих строений и транспортных средств;
* из смежных помещений, принадлежащих другим организациям и расположенным в том же здании, что и объект защиты;
* при посещении объектов Компании сторонними лицами.
  1. В качестве средств перехвата информативного сигнала могут использоваться портативные устройства, размещаемые вблизи объекта защиты либо подключаемые к каналам связи, а также электронные устройства съема информации (закладочные устройства), размещаемые внутри или вне ЗП и ПС.
  2. Кроме перехвата информации техническими средствами возможно непреднамеренное попадание защищаемой информации к лицам, не допущенным к ней, но находящимся в пределах КЗ. Это возможно, например, вследствие непреднамеренного прослушивания без использования технических средств конфиденциальных разговоров из-за недостаточной звукоизоляции ограждающих конструкций помещений, и их инженерно-технических систем.
  3. ОРГАНИЗАЦИЯ И ПРОВЕДЕНИЕ РАБОТ ПО ЗАЩИТЕ РЕЧЕВОЙ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

1. Организацию работ по защите речевой информации в СП ПАО «НК «Роснефть»/ОГ и принятие необходимых мер по минимизации ее утечки осуществляет руководитель СП ПАО «НК «Роснефть»/руководитель ОГ.

Реализация мер по обеспечению защиты (конфиденциальной) информации в ПАО «НК «Роснефть» и ОГ осуществляется, при необходимости, с привлечением специализированных организаций.

Контроль обеспечения защиты (конфиденциальной) информации в ПАО «НК «Роснефть» и ОГ осуществляется CБ/ПЭБ:

* в ЗП – с привлечением специализированных организаций в соответствии с п. 3.3.6. настоящих Методических указаний;
* в ПС – в соответствии с п. 3.4.6. настоящих Методических указаний.

1. Мероприятия конфиденциального характера должны проводиться только в ЗП и ПС. В ЗП проводятся мероприятия, связанные с циркулированием информации, содержащей сведения конфиденциального характера, относящихся к категории: «Для служебного пользования», коммерческая тайна Компании, инсайдерская информации и персональные данные. В ПС проводятся мероприятия, связанные с циркулированием информации, содержащей сведения конфиденциального характера, относящихся к категории: коммерческая тайна Компании; инсайдерская информация и персональные данные.
2. Переговоры/совещания конфиденциального характера с участием Главного исполнительного директора ПАО «НК «Роснефть» и топ-менеджеров ПАО «НК «Роснефть» проводятся в ЗП или в ПС. При этом должны осуществляться организационные и, при необходимости, технические меры:

* организован контроль обстановки за пределами помещения, где проводится мероприятие, для исключения появления посторонних лиц и возможности несанкционированного прослушивания;
* непосредственно перед мероприятием может быть проведена инструментальная проверка помещения (на основании служебной записки работника ПАО «НК «Роснефть»/ОГ, ответственного за проведение мероприятия, на имя вице-президента - руководителя Службы безопасности ПАО «НК «Роснефть»/ПЭБ).

1. Ответственность за соблюдение требований по технической защите речевой информации в ЗП и ПС возлагается на работников СП ПАО «НК «Роснефть»/ОГ, назначенных ответственными лицами за эксплуатацию указанных помещений, а ответственность за соблюдение требований по безопасности информации при проведении конфиденциальных мероприятий - на руководителей   
   СП ПАО «НК «Роснефть»/руководителей ОГ, а также работников, назначенных ответственными за организацию и проведение конфиденциальных мероприятий.
   1. ОРГАНИЗАЦИЯ И ПРОВЕДЕНИЕ РАБОТ ПО ЗАЩИТЕ РЕЧЕВОЙ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЯХ
2. Для подтверждения соответствия системы защиты информации ЗП требованиям безопасности информации, осуществляется аттестация ЗП по требованиям безопасности информации.

Аттестация ЗП осуществляется по инициативе заказчика (владельца информации).

Необходимо учитывать, что несколько СП ПАО «НК «Роснефть» могут использовать одно ЗП. В ОГ рекомендуется предусмотреть не менее 1 ЗП.

1. Рекомендуется следующий порядок организации работ по защите (конфиденциальной) информации в ЗП:

* руководитель СП ПАО «НК «Роснефть»/руководитель ОГ принимает решение о необходимости определения помещений, специально предназначенных для обсуждения конфиденциальной информации;
* СП ПАО «НК «Роснефть»/ОГ по согласованию со СБ/ПЭБ проводится выбор помещений на объектах Компании, в наибольшей степени соответствующих требованиям по защите (конфиденциальной) информации, предъявляемым к ЗП, указанным в разделе 4.2. настоящих Методических указаний;
* СБ/ПЭБ организуется обследование выбранного помещения с целью определения необходимости и примерного объема проведения мероприятий по обеспечению выполнения требований по защите (конфиденциальной) информации от утечки по техническим каналам;
* к проведению мероприятий по обеспечению выполнения требований по защите (конфиденциальной) информации от утечки по техническим каналам может привлекаться специализированная организация. Аттестация ЗП осуществляется только с привлечением специализированной организации. Выбор специализированной организации осуществляется СБ/ПЭБ в соответствии с действующими ЛНД в Компании и ОГ в области закупочной деятельности.

1. На стадии подготовки ЗП к аттестации по требованиям безопасности информации специализированной организацией оформляются следующие технические документы:

* программа и методики аттестационных испытаний;
* технический паспорт ЗП (форма технического паспорта на ЗП приведена в [Приложении 1](#_Toc14430507) к настоящим Методическим указаниям).

1. На стадии ввода в эксплуатацию СЗИ и ЗП оформляются[[1]](#footnote-1):

* акты установки СЗИ по результатам их приемо-сдаточных испытаний;
* протоколы специальных исследований ОТСС и ВТСС;
* эксплуатационная документация СЗИ;
* протоколы аттестационных испытаний и заключение по их результатам;
* инструкция о порядке проведения мероприятий конфиденциального характера в ЗП;
* аттестат соответствия объекта информатизации требованиям по безопасности информации (форма «Аттестата соответствия» для ЗП приведена в [Приложение 2](#_Toc14430508) к настоящим Методическим указаниям).

1. Рекомендуется периодически (не реже 1 раза в год) силами СБ/ПЭБ проводить инструментальную проверку ЗП с целью выявления возможно установленных в нем закладочных устройств.
2. С целью своевременного выявления и предотвращения утечки речевой информации по техническим каналам необходимо проводить периодический (не реже одного раза в 2 года) контроль состояния защиты информации в ЗП. Контроль осуществляется СБ/ПЭБ:

* с привлечением специализированной организации в части оценки защищенности ЗП от утечки речевой информации по техническим каналам;
* в части оценки знаний и выполнения лицами, ответственными за эксплуатацию ЗП, своих функциональных обязанностей в отношении защиты циркулирующей в ЗП речевой информации.

* 1. ОРГАНИЗАЦИЯ И ПРОВЕДЕНИЕ РАБОТ ПО ЗАЩИТЕ РЕЧЕВОЙ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В ПОМЕЩЕНИЯХ ДЛЯ СОВЕЩАНИЙ КОМПАНИИ

1. Решение о необходимости использования для мероприятий конфиденциального характера определенного ПС (определенных ПС) принимается руководителем   
   СП ПАО «НК «Роснефть»/руководителем ОГ.
2. Для проведения экспертной оценки того, что помещение может быть использовано для проведения мероприятий конфиденциального характера руководителем   
   СП ПАО «НК «Роснефть»/руководителем ОГ формируется экспертная группа в составе: в СП ПАО «НК «Роснефть» – работников СП ПАО «НК «Роснефть» и работника СБ/в ОГ – работника ПЭБ и работников ОГ.
3. Проводится экспертная оценка возможности использования данного помещения в качестве ПС с отражением ее результатов в экспертном заключении (форма экспертного заключения приведена в [Приложении 3](#_Toc14430509) к настоящим Методическим указаниям).
4. В экспертном заключении, которое оформляется и хранится   
   в СП ПАО «НК «Роснефть»/ОГ, должна содержаться следующая информация:

* о соответствии помещения необходимым требованиям;
* об условиях проведения мероприятий конфиденциального характера в помещении и организационных мерах, способствующих минимизации рисков утечки речевой информации по техническим каналам;
* о расширении КЗ вокруг помещения, при необходимости, путем реализации организационных мер.

Экспертное заключение должно быть подписано членами экспертной группы СП ПАО «НК «Роснефть»/ОГ и утверждено руководителем СП ПАО «НК «Роснефть»/ОГ.

1. Помещение разрешается использовать в качестве ПС, если выполняются следующие условия:

* экспертное заключение содержит решение о возможности использования помещения для проведения мероприятий конфиденциального характера;
* руководителем СП ПАО «НК «Роснефть»/руководителем ОГ назначено лицо, ответственное за эксплуатацию ПС;
* оформлен технический паспорт на ПС (форма технического паспорта на ПС приведена в [Приложении 4](#_Toc18582057) к настоящим Методическим указаниям). Технический паспорт на ПС разрабатывается лицом, ответственным за эксплуатацию ПС;
* разработана инструкция о порядке проведения мероприятий конфиденциального характера в ПС. Инструкция разрабатывается лицом, ответственным за эксплуатацию ПС.

1. С целью своевременного выявления технических каналов утечки речевой информации и предотвращения ее утечки по техническим каналам необходимо проводить периодическую (не реже одного раза в 2 года) инструментальную проверку ПС и контрольные мероприятия, которые осуществляются СБ/ПЭБ и предназначены для:

* выявления возможно установленных в ПС закладочных устройств;
* оценки знаний и выполнения лицами, ответственными за эксплуатацию ПС, своих функциональных обязанностей в части защиты циркулирующей в ПС речевой информации.

Для обеспечения инструментального контроля СБ/ПЭБ обеспечиваются соответствующими техническими средствами ([Приложение 5](#_ПРИЛОЖЕНИЕ_4._РЕКОМЕНДУЕМАЯ_1) к настоящим Методическим указаниям).

1. ТРЕБОВАНИЯ И РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ РЕЧЕВОЙ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ
   1. ОБЩИЕ ПОЛОЖЕНИЯ
2. Требования и рекомендации настоящего раздела направлены на исключение (существенное затруднение) возможности перехвата речевой информации, циркулирующей в ЗП, в ПС, в СЗУ и СЗСВ ЗП.
3. Требования настоящего раздела являются обязательными на всех стадиях создания системы защиты информации, эксплуатации ЗП и размещенных в них ОТСС и ВТСС, эксплуатации ПС, для СЗУ и СЗСВ ЗП.
   1. ОСНОВНЫЕ ТРЕБОВАНИЯ И РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ, ЦИРКУЛИРУЮЩЕЙ В ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЯХ
4. Перечень ЗП и лиц, ответственных за их эксплуатацию, определяется распорядительным документом ПАО «НК «Роснефть»/ОГ. Руководитель СП ПАО «НК «Роснефть»/ОГ письменно (служебной запиской) уведомляет руководителя СБ/ПЭБ о назначении лица, ответственного за эксплуатацию ЗП (с указанием номера помещения и адреса его расположения).
5. ЗП должны размещаться в пределах КЗ офисов ПАО «НК «Роснефть»/ОГ. При этом рекомендуется размещать их на максимальном удалении от ее границ. Не рекомендуется располагать ЗП на первых этажах зданий, а также чтобы ограждающие конструкции ЗП (стены, полы, потолки) были смежными с помещениями других организаций. Рекомендуется, чтобы окна ЗП выходили во внутреннюю, закрытую от несанкционированного доступа территорию и закрывались шторами (жалюзи).
6. ЗП по указанию специализированной организации оснащаются сертифицированными по требованиям безопасности информации СЗИ. Эксплуатация ОТСС, ВТСС и СЗИ должна осуществляться в соответствии с эксплуатационной документацией на них.
7. Для ЗП, в которых установлены средства оргтехники, должны быть зарезервированы прошедшие специальные исследования средства оргтехники и их комплектующие элементы, предназначенные для оперативной замены вышедших из строя или выработавших свой ресурс средств оргтехники.

Проведение специальных исследований резервных средств оргтехники и их комплектующих элементов рекомендуется осуществлять одновременно с проведением специальных исследований других технических средств в период подготовки ЗП к аттестации по требованиям безопасности информации.

В случае установки, взамен вышедшего из строя или выработавшего свой ресурс, резервного средства оргтехники или комплектующего элемента – для него должны быть проведены специальные исследования. Объем работ по специальным исследованиям технических средств должен быть определен по согласованию с СБ/ПЭБ и специализированной организацией, с учетом имеющихся для конкретного ЗП технических каналов утечки информации.

Владельцем ЗП по согласованию с СБ/ПЭБ должно быть организовано извещение специализированной организации, выдавшей «Аттестат соответствия» о всех изменениях в информационных технологиях, составе и размещении средств и систем информатики, условиях их эксплуатации, которые могут повлиять на эффективность мер и средств защиты информации (перечень характеристик, определяющих безопасность информации, об изменениях которых требуется обязательно извещать специализированную организацию, приводится в «Аттестате соответствия»). По результатам указанного извещения, специализированной организацией принимается решение о необходимости проведения дополнительной проверки эффективности системы защиты информации ЗП.

1. На размещаемых в ЗП средствах вычислительной техники программное обеспечение устанавливается в соответствии с требованиями ЛНД Компании.
2. Во время проведения мероприятий конфиденциального характера запрещается проносить в ЗП лицами, участвующими в мероприятиях конфиденциального характера, радиотелефоны, смартфоны, планшетные компьютеры, оконечные устройства сотовой связи, диктофоны, средства аудио- и видеозаписи, а также другие стационарные и переносимые устройства, оборудованные WIFI и/или bluetooth, имеющие функции записи (либо ретрансляции) информации.
3. Для исключения возможности утечки информации за счет акустоэлектрического преобразования необходимо оконечные устройства телефонной связи, имеющие прямой выход в городскую АТС, оборудовать сертифицированными СЗИ от утечки за счет акустоэлектрического преобразования либо временно (на период проведения мероприятий конфиденциального характера) отключать указанные оконечные устройства от телефонной сети.
4. Для исключения возможности скрытного подключения к телефонной сети и прослушивания ведущихся в ЗП разговоров не рекомендуется устанавливать в них цифровые телефонные аппараты цифровых АТС, имеющих прямой выход в городскую АТС и (или) абонентов из сторонних организаций.

В противном случае, необходимо использовать сертифицированные по требованиям безопасности информации цифровые АТС либо устанавливать в эти ЗП аппараты с вмонтированными в них сертифицированными средствами защиты, либо временно отключать телефонные аппараты от телефонной сети.

1. Системы пожарной и охранной сигнализации ЗП должны строиться только по проводной схеме сбора информации (связи с пультом) и, как правило, размещаться в пределах одной с ЗП контролируемой зоне.
2. Звукоизоляция ограждающих конструкций ЗП, их систем вентиляции и кондиционирования в местах возможного перехвата информации должна исключать возможность прослушивания ведущихся в нем разговоров из-за пределов ЗП.

Для обеспечения необходимого уровня звукоизоляции помещений рекомендуется оборудование дверных проемов тамбурами с двойными дверями, установка дополнительных рам в оконных проемах, уплотнительных прокладок в дверных и оконных притворах и применение шумопоглотителей на выходах вентиляционных каналов.

Если предложенными выше методами не удается обеспечить необходимую акустическую защиту, следует применять организационные меры (установка временной КЗ), ограничивая на период проведения мероприятий конфиденциального характера доступ посторонних лиц в места возможного прослушивания разговоров, ведущихся в ЗП.

1. Для снижения вероятности перехвата информации по виброакустическому каналу рекомендуется организационными мерами исключить возможность установки посторонних (внештатных) предметов на внешней стороне ограждающих конструкций ЗП и выходящих из них инженерных коммуникаций (систем отопления, вентиляции, кондиционирования).

Для снижения уровня виброакустического сигнала рекомендуется расположенные в ЗП элементы инженерно-технических систем отопления, вентиляции оборудовать звукоизолирующими экранами.

1. Если при проведении технического контроля обнаружено, что указанные выше меры защиты информации от утечки по акустическому и виброакустическому каналам недостаточны или нецелесообразны, то рекомендуется применять метод активного акустического или виброакустического маскирующего зашумления.

Для этой цели должны применяться сертифицированные средства активной защиты.

1. При эксплуатации ЗП необходимо предусматривать организационные меры, направленные на исключение несанкционированного доступа в помещение:

* двери ЗП в период между мероприятиями конфиденциального характера, а также в нерабочее время, должны запираться на ключ;
* выдача ключей от ЗП должна производиться только лицам, работающим в нем или ответственным за это помещение;
* установка и замена оборудования, мебели, ремонт ЗП должны производиться только по согласованию и под контролем лица, ответственного за его эксплуатацию (в СП ПАО «НК «Роснефть»/ОГ).
  1. ОСНОВНЫЕ ТРЕБОВАНИЯ И РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ, ЦИРКУЛИРУЮЩЕЙ В ПОМЕЩЕНИЯХ ДЛЯ СОВЕЩАНИЙ

1. В ПАО «НК «Роснефть»/ОГ СБ/ПЭБ организует учет введенных в эксплуатацию   
   ПС и лиц, ответственных за эксплуатацию ПС. Руководитель СП ПАО «НК «Роснефть»/ОГ письменно (служебной запиской) уведомляет руководителя СБ/ПЭБ о вводе в эксплуатацию ПС (с указанием номера помещения, адреса его расположения) и о лице, ответственном за его эксплуатацию.
2. ПС должно обладать определенными параметрами: его ограждающие конструкции, инженерные коммуникации (системы отопления, вентиляции, кондиционирования), его расположение относительно других помещений и КЗ, - которые должны обеспечивать высокую степень защищенности этого помещения.
3. ПС должны размещаться в пределах КЗ офисов Компании на максимальном удалении от ее границ. Ограждающие конструкции ПС (стены, полы, потолки) не должны быть смежными с помещениями других организаций. Окна ПС должны быть оборудованы шторами (жалюзи), которые должны быть закрыты во время проведения мероприятий конфиденциального характера.
4. Во время проведения мероприятий конфиденциального характера запрещается проносить в ПС лицами, участвующими в мероприятиях, радиотелефоны, смартфоны, планшетные компьютеры, оконечные устройства сотовой связи, диктофоны, средства аудио- и видеозаписи, а также другие стационарные и переносимые устройства, оборудованные WIFI и/или bluetooth, имеющие функции записи (либо ретрансляции) информации.
5. Для исключения возможности утечки информации за счет акустоэлектрического преобразования необходимо исключить использование в ПС оконечных устройств телефонной связи, имеющих прямой выход в городскую АТС, либо временно (на период проведения мероприятий конфиденциального характера) отключать указанные оконечные устройства от телефонной сети.
6. Для снижения вероятности перехвата информации по виброакустическому каналу рекомендуется организационными мерами исключить возможность установки посторонних (внештатных) предметов на внешней стороне ограждающих конструкций ПС и выходящих из них инженерных коммуникаций (систем отопления, вентиляции, кондиционирования).
7. При эксплуатации ПС необходимо предусматривать организационные меры, направленные на исключение несанкционированного доступа в помещение:

* двери ПС в период между мероприятиями конфиденциального характера, а также в нерабочее время, должны запираться на ключ;
* выдача ключей должна производиться только лицам, работающим в нем или ответственным за это помещение;
* установка и замена оборудования, мебели, ремонт ПС должны производиться только по согласованию и под контролем лица, ответственного за его эксплуатацию (в СП ПАО «НК «Роснефть»/ОГ).
  1. ЗАЩИТА ИНФОРМАЦИИ, ЦИРКУЛИРУЮЩЕЙ В СИСТЕМАХ ЗВУКОУСИЛЕНИЯ И ЗВУКОВОГО СОПРОВОЖДЕНИЯ ВИДЕОИНФОРМАЦИИ

1. В качестве оборудования СЗУ, предназначенных для обслуживания проводимых в ЗП мероприятий конфиденциального характера, и СЗСВ (в ЗП), содержащих конфиденциальные сведения, необходимо использовать оборудование, удовлетворяющее требованиям стандартов Российской Федерации по электромагнитной совместимости   
   (например, ГОСТ 22505-97).

По указанию специализированной организации, для повышения уровня защищенности используется оборудование, сертифицированное по требованиям безопасности информации, предъявляемым к СЗУ.

1. СЗУ должны выполняться по проводной схеме передачи информации экранированными проводами и располагаться в пределах ЗП.

С целью уменьшения побочных электромагнитных излучений целесообразно использовать СЗУ с рассредоточенной системой звукоизлучателей, т.е. следует отдавать предпочтение системам с большим количеством оконечных устройств малой мощности перед системами с малым количеством оконечных устройств большой мощности.

Допускается использовать выпускаемые в обычном исполнении громкоговорители с экранированными магнитными цепями или укомплектованные ими звуковые колонки.

1. В СЗУ рекомендуется применять аппаратуру с симметричными входными и выходными цепями. В случае использования аппаратуры с несимметричным выходом, линии оконечных устройств следует подключать к оконечным усилителям через симметрирующие трансформаторы, устанавливаемые в непосредственной близости от оконечных усилителей.
2. В качестве усилительного оборудования рекомендуется использовать усилители в металлических экранах с возможностью их заземления.
3. Коммутационное и распределительное оборудование (распределительные, входные и выходные щитки подключения) следует размещать в металлических шкафах (коробках). На корпусах шкафов (коробок) необходимо предусмотреть клеммы (винты) для их заземления и приспособления для опечатывания.
4. Усилительное и оконечное оборудование СЗУ, СЗСВ следует размещать на возможно большем расстоянии относительно границы КЗ.
5. Система электропитания и заземления должна соответствовать требованиям «Правил устройства электроустановок».

Рекомендуется электропитание аппаратуры СЗУ и СЗСВ осуществлять от подстанции, а заземление от контура, расположенных в пределах КЗ.

Сопротивление заземления в любой точке системы не должно превышать 4 Ом. На контур заземления должны быть посажены третий провод трехпроводной линии электропитания и экранирующие оболочки сетевых линий. На щитках электропитания необходимо выводить «землю» отдельной клеммой.

* 1. ЗАЩИТА ИНФОРМАЦИИ ПРИ ПРОВЕДЕНИИ АУДИО- И ВИДЕОЗАПИСИ

1. Запись и воспроизведение конфиденциальной информации с помощью аппаратуры звуко- и видеозаписи разрешается производить только в ЗП и ПС.
2. Для записи, воспроизведения и хранения информации должны применяться устройства, соответствующие требованиям Инструкции Компании «Порядок использования мобильных технических средств» № П3-11.01 И-0009.
3. Носители информации (аудио- и видеокассеты, карты памяти и др.) должны учитываться и храниться в структурных подразделениях ПАО «НК «Роснефть»/ОГ в порядке, установленном Стандартом Компании «Охрана сведений конфиденциального характера» № П3-11.03 С-0006, Стандартом Компании «Политики информационной безопасности ПАО «НК «Роснефть» и Обществ Группы» № П3-11.01 С-0054.

В СП ПАО «НК «Роснефть» и ОГ должны быть назначены лица, ответственные за хранение и использование аппаратуры звуко- и видеозаписи информации, предназначенной для записи и воспроизведения конфиденциальной информации, и обеспечено хранение и использование этой аппаратуры, исключающее несанкционированный доступ к ней.

1. ССЫЛКИ
2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
3. ГОСТ РО 0043-003-2012 Защита информации. Аттестация объектов информатизации. Общие положения.
4. ГОСТ РО 0043-004-2013 Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний.
5. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
6. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения.
7. ГОСТ 22505-97 Совместимость технических средств электромагнитная. Радиопомехи индустриальные от радиовещательных приемников, телевизоров и другой бытовой радиоэлектронной аппаратуры. Нормы и методы испытаний.
8. Нормативно-методический документ «Специальные требования и рекомендации по технической защите конфиденциальной информации», утвержденный приказом Гостехкомиссии России от 30.08.2002 № 282.
9. Рекомендации по стандартизации. Техническая защита информации. Основные термины и определения. № Р 50.1.056-2005, утвержденные приказом Ростехрегулирования от 29.12.2005 № 479-ст.
10. Правила устройства электроустановок издание 7, утвержденные приказом Минэнерго России от 08.07.2002 № 204.
11. Стандарт Компании «Политики информационной безопасности ПАО «НК» Роснефть и Обществ Группы» № П3-11.01 С-0054 версия 1.00,утвержденный решением Правления ПАО «НК «Роснефть» (протокол от 10.02.2017 №Пр-ИС-03П), введенный в действие приказом ПАО «НК «Роснефть» от 28.03.2017 № 161.
12. Стандарт Компании «Охрана сведений конфиденциального характера»   
    № П3-11.03 С-0006 версия 5.00, утвержденный решением Правления   
    ПАО «НК «Роснефть» (протокол от 04.09.2017 № Пр-ИС-32п, введенный в действие приказом ПАО «НК «Роснефть» от 25.09.2017 № 551.
13. Инструкция Компании «Порядок использования мобильных технических средств»  
    № П3-11.01 И-0009 версия 1.00, утвержденная приказом ПАО «НК «Роснефть»   
    от 03.09.2018 № 523, введенная в действие 05.10.2018.

# ПРИЛОЖЕНИЯ

**Таблица 1**

**Перечень Приложений к Методическим указаниям Компании**

| **НОМЕР ПРИЛОЖЕНИЯ** | **НАИМЕНОВАНИЕ ПРИЛОЖЕНИЯ** | **ПРИМЕЧАНИЕ** |
| --- | --- | --- |
| **1** | **2** | **3** |
| 1 | Форма технического паспорта на защищаемое помещение | Включено в настоящий файл |
| 2 | Форма аттестата соответствия защищаемого помещения | Включено в настоящий файл |
| 3 | Форма экспертного заключения о проведении оценки возможности (невозможности) использования помещения в качестве помещения для совещаний | Включено в настоящий файл |
| 4 | Форма технического паспорта на помещение для совещаний | Включено в настоящий файл |
| 5 | Рекомендуемая техника для проведения инструментальных проверок | Включено в настоящий файл |

## 

**ПРИЛОЖЕНИЕ 1. ФОРМА ТЕХНИЧЕСКОГО ПАСПОРТА НА ЗАЩИЩАЕМОЕ ПОМЕЩЕНИЕ**

УТВЕРЖДАЮ

Руководитель СП

ПАО «НК «Роснефть» или ОГ

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись, инициалы, фамилия )

“\_\_\_” \_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_

(дата)

ТЕХНИЧЕСКИЙ ПАСПОРТ

на защищаемое помещение № \_\_\_\_\_\_

СОСТАВИЛ

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (должность, подпись, инициалы, фамилия

работника СП ПАО «НК «Роснефть» или ОГ)

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_

(дата)

ОЗНАКОМЛЕН

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (должность, подпись, инициалы,

фамилия ответственного за помещение)

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_

(дата)

\_\_\_\_

(Год)

1. **Памятка**

**по обеспечению режима безопасности и эксплуатации**

**оборудования, установленного в защищаемом**

**помещении № \_\_\_\_\_\_\_**

*(Примерный текст)*

1. Ответственность за соблюдение требований по технической защите речевой информации в защищаемом помещении (ЗП) и правильность использования установленных в нем технических средств несет лицо, ответственное за его эксплуатацию.

2. Установка и замена оборудования, мебели, ремонт ЗП должны производиться только по согласованию и под контролем лица, ответственного за его эксплуатацию (в СП ПАО «НК «Роснефть»/ОГ).

3. Двери ЗП в период между мероприятиями, а также в нерабочее время, должны быть заперты на ключ.

4. Выдача ключей от ЗП должна производиться лицам, работающим в нем, или лицу(ам), ответственному(ым) за его эксплуатацию.

5. Для исключения просмотра текстовой и графической конфиденциальной информации через окна помещения рекомендуется оборудовать их шторами (жалюзи).

6. Должны выполняться предписания на эксплуатацию средств связи, вычислительной техники, оргтехники, бытовых приборов и другого оборудования, установленного в помещении.

7. Во время проведения мероприятий конфиденциального характера запрещается проносить в помещение лицами, участвующими в мероприятиях, радиотелефоны, смартфоны, планшетные компьютеры, оконечные устройства сотовой и транкинговой связи, диктофоны, средства аудио- и видеозаписи, а также другие стационарные и переносимые устройства, оборудованные WIFI и/или bluetooth, имеющие функции записи (либо ретрансляции) информации. При установке в ЗП телефонных и факсимильных аппаратов с автоответчиком или спикерфоном, а также телефонных аппаратов с автоматическим определителем номера, их следует отключать из сети на время проведения этих мероприятий или использовать соответствующие средства защиты.

8. Повседневный контроль за выполнением требований по защите помещения осуществляют лица, ответственные за помещение.

9. Периодический (раз в 2 года) контроль эффективности мер защиты помещения организуется СБ/ПЭБ с привлечением специализированных организаций, имеющих соответствующие лицензии.

**Примечание**: В памятку целесообразно включать и другие сведения, учитывающие особенности установленного в ЗП оборудования; действия персонала в случае срабатывания установленной в помещении сигнализации, порядок эксплуатации средств защиты, организационные меры защиты и т.п.

1. **Перечень оборудования, установленного в помещении**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Вид оборудования | Тип | Учетный  (зав.)  номер | Дата  установки | Класс  ТС  (ОТСС или ВТСС) | Сведения по сертификации, специсследованиям и спецпроверкам |
|  |  |  |  |  |  |

1. **Меры защиты информации**

(Пример)

1. Телефонный аппарат коммутатора директора (инв.№ 7).

Выполнены требования предписания на эксплуатацию.

(Перечень предусмотренных мер защиты согласно предписанию).

2. Телефонный аппарат № 7-17.

На линию установлено защитное устройство «Сигнал-5», зав.№ 017.

3. Пульт коммутатора.

Выполнены требования предписания на эксплуатацию.

4. Часы электронные.

Выполнены требования предписания на эксплуатацию.

5. Вход в помещение оборудован тамбуром, двери двойные, обшиты слоем ваты и дермантина. Дверные притворы имеют резиновые уплотнения.

6. Доступ к вентиляционным каналам, выходящим на чердак здания, посторонних лиц исключен (приводятся предусмотренные для этого меры).

1. **Отметка о проверке средств защиты**

|  |  |  |  |
| --- | --- | --- | --- |
| Вид оборудования | Учетный  номер | Дата  проверки | Результаты проверки и  № отчетного документа |
|  |  |  |  |

1. **Результаты аттестационного и периодического**

**контроля помещения**

|  |  |  |
| --- | --- | --- |
| Дата проведения | Результаты аттестации или периодического контроля, № отчетного документа | Подпись  проверяющего |
|  |  |  |

**ПРИЛОЖЕНИЕ 2. ФОРМА АТТЕСТАТА СООТВЕТСТВИЯ ЗАЩИЩАЕМОГО ПОМЕЩЕНИЯ**

УТВЕРЖДАЮ

Руководитель организации,

проводившей работы по аттестации

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись, инициалы, фамилия )

“\_\_\_” \_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_

(дата)

АТТЕСТАТ СООТВЕТСТВИЯ

**№ \_\_\_\_\_**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

название объекта информатизации

**требованиям безопасности информации**

**Выдан** “\_\_\_\_”\_\_\_\_\_\_\_\_”\_\_\_\_\_г.

**Действителен до** “\_\_\_\_”\_\_\_\_\_\_\_\_”\_\_\_\_\_г.

1. Настоящим АТТЕСТАТОМ удостоверяется, что объект информатизации

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

(полное наименование защищаемого помещения)

расположенный в \_\_\_\_\_\_\_\_\_\_\_\_\_\_ по адресу \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ , с установленным в нем оборудованием соответствует требованиям нормативных документов по безопасности информации и в нем разрешается проведение конфиденциальных мероприятий (совещаний, переговоров и т.п.).

Перечень установленного в защищаемом помещении оборудования, указан в техническом паспорте на защищаемое помещение.

2. Аттестация ЗП выполнена в соответствии с программой и методиками аттестационных испытаний \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

3. Установленный порядок пользования ЗП позволяет осуществлять его эксплуатацию, расположенного в нем оборудования и средств защиты в соответствии с требованиями по защите конфиденциальной информации.

4. Повседневный контроль за выполнением установленных правил эксплуатации ЗП осуществляется ответственным за обеспечение защиты информации в ПАО «НК «Роснефть»/ОГ.

5. В ЗП запрещается проводить ремонтно-строительные работы, замену (установку новых) элементов интерьера, вносить изменения в состав оборудования и средства защиты информации, без согласования с \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(наименование организации, проводившей аттестацию)

6. Лицо, ответственное за эксплуатацию защищаемого помещения, обязано незамедлительно извещать \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_:

(наименование организации, проводившей аттестацию)

1. о предполагаемых ремонтно-строительных работах и изменениях в размещении и монтаже установленного оборудования, технических средств и систем, средств защиты информации, в интерьере помещения;
2. о нарушениях в работе средств защиты информации;
3. о фактах несанкционированного доступа в помещение.

7. Результаты аттестационных испытаний приведены в Заключении № \_\_\_\_\_\_\_ от \_\_\_\_\_\_\_\_\_\_ по результатам аттестационных испытаний и в протоколе аттестационных испытаний № \_\_\_\_\_\_\_ от \_\_\_\_\_\_\_\_\_\_.

8. Аттестат соответствия выдан на 3 года, в течение которых должна быть обеспечена неизменность условий функционирования ЗП и технологии защиты информации.

Руководитель аттестационной комиссии

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(должность и название организации)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

подпись, инициалы, фамилия

“\_\_\_\_”\_\_\_\_\_\_\_\_”\_\_\_\_ г.

============================================================

**Отметки органа надзора:**

**[ПРИЛОЖЕНИЕ](#_ПРИЛОЖЕНИЕ_4._РЕКОМЕНДУЕМАЯ_1) 3. ФОРМА ЭКСПЕРТНОГО ЗАКЛЮЧЕНИЯ О ПРОВЕДЕНИИ ОЦЕНКИ ВОЗМОЖНОСТИ (НЕВОЗМОЖНОСТИ) ИСПОЛЬЗОВАНИЯ ПОМЕЩЕНИЯ В КАЧЕСТВЕ ПОМЕЩЕНИЯ ДЛЯ СОВЕЩАНИЙ**

УТВЕРЖДАЮ

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(руководитель СП ПАО «НК «Роснефть»/ОГ)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ 222 (подпись) (инициалы, фамилия)

“\_\_\_” \_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

ЭКСПЕРТНОЕ ЗАКЛЮЧЕНИЕ

о проведении экспертной оценки возможности использования

помещения \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ в качестве помещения для совещаний

(наименование или № пом.)

В результате проведенного визуального обследования помещения на соответствие требованиям пункта 4.3.3. раздела 4.3. Методических указаний Компании «Требования и рекомендации по технической защите речевой конфиденциальной информации» (МУ), предъявляемым помещениям для совещаний, установлено, что помещение \_\_\_\_\_\_\_соответствует\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ указанным требованиям.

(соответствует / не соответствует)

Экспертная группа считает, что проведение мероприятий конфиденциального характера (совещаний, обсуждений, переговоров и т.п.) в данном помещении возможно при соблюдении следующих условий (при необходимости):

1.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(указываются условия проведения мероприятий конфиденциального характера, способствующие минимизации рисков утечки

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ речевой информации по техническим каналам. Например, путем использования организационных мер (выставле-

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

нием работника охраны на период проведения мероприятий конфиденциального характера для ограничения доступа

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;

посторонних лиц в места возможного прослушивания разговоров, ведущихся в помещении для совещаний)

2. В соответствии с пунктом 4.3.7. МУ должны быть предусмотрены организационные меры по исключению несанкционированного доступа в помещение (двери помещения в период между мероприятиями конфиденциального характера, а также в нерабочее время должны запираются на ключ, выдача ключей от помещений должна осуществляется только лицам, работающим в помещении или ответственным за помещение).

1. В ПАО «НК «Роснефть» руководитель СБ/в ОГ - руководитель ПЭБ должен быть извещен о назначении лиц(а), ответственных(ого) за эксплуатацию данного помещения.

Члены группы:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

(должность работника СП (ОГ)) (подпись) (фамилия, инициалы)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

(должность работника СП (ОГ)) (подпись) (фамилия, инициалы)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

(должность работника СП (ОГ)) (подпись) (фамилия, инициалы)

**ПРИЛОЖЕНИЕ 4. ФОРМА ТЕХНИЧЕСКОГО ПАСПОРТА НА ПОМЕЩЕНИЕ ДЛЯ СОВЕЩАНИЙ**

УТВЕРЖДАЮ

Руководитель СП

ПАО «НК «Роснефть» или ОГ

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись, инициалы, фамилия )

“\_\_\_” \_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_

(дата)

ТЕХНИЧЕСКИЙ ПАСПОРТ

на помещение для совещаний № \_\_\_\_\_\_

СОСТАВИЛ

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (должность, подпись, инициалы,

фамилия ответственного за помещение)

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_

(дата)

\_\_\_\_

(Год)

* 1. **Памятка**

**по обеспечению режима безопасности и эксплуатации**

**оборудования, установленного в помещении для совещаний № \_\_\_\_\_\_\_**

*(Примерный текст)*

1. Ответственность за соблюдение требований по технической защите речевой информации в помещении для совещаний (ПС) и правильность использования установленных в нем технических средств несет лицо, которое постоянно в нем работает, или лицо, ответственное за его эксплуатацию.

2. Установка и замена оборудования, мебели, ремонт ПС должны производиться только по согласованию и под контролем лица, ответственного за его эксплуатацию (в СП ПАО «НК «Роснефть»/ОГ).

3. Двери ПС в период между мероприятиями, а также в нерабочее время, должны быть заперты на ключ.

4. Выдача ключей от ПС должна производиться лицам, работающим в нем, или лицу(ам), ответственному(ым) за его эксплуатацию.

5. При проведении мероприятий конфиденциального характера бытовая радиоаппаратура, установленная в помещении (телевизоры, радиоприемники и т.п.), должна отключаться от сети электропитания.

6. Для исключения просмотра текстовой и графической конфиденциальной информации через окна помещения рекомендуется оборудовать их шторами (жалюзи).

7. Должны выполняться предписания на эксплуатацию средств связи, вычислительной техники, оргтехники, бытовых приборов и другого оборудования, установленного в помещении.

8. Во время проведения мероприятий конфиденциального характера запрещается проносить в помещение лицами, участвующими в мероприятиях, радиотелефоны, смартфоны, планшетные компьютеры, оконечные устройства сотовой и транкинговой связи, диктофоны, средства аудио- и видеозаписи, а также другие стационарные и переносимые устройства, оборудованные WIFI и/или bluetooth, имеющие функции записи (либо ретрансляции) информации. При установке в помещении телефонных и факсимильных аппаратов с автоответчиком или спикерфоном, а также телефонных аппаратов с автоматическим определителем номера, их следует отключать из сети на время проведения этих мероприятий.

9. Повседневный контроль за выполнением требований по защите помещения осуществляют лица, ответственные за помещение.

10. Периодическая (раз в год) проверка помещения с целью выявления возможно установленных в ПС закладочных устройств осуществляется СБ/ПЭБ.

**Примечание**: В памятку целесообразно включать и другие сведения, учитывающие особенности установленного в ПС оборудования; действия персонала в случае срабатывания установленной в помещении сигнализации, порядок эксплуатации средств защиты, организационные меры защиты и т.п.

* 1. **Перечень оборудования, установленного в помещении**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Вид оборудования | Тип | Учетный  (зав.)  номер | Дата  установки | Класс  ТС  (ОТСС или ВТСС) | Дополнительная информация |
|  |  |  |  |  |  |

* 1. **Меры защиты информации**

(Пример)

1. Телефонный аппарат коммутатора директора (инв.№ 7).

Выполнены требования предписания на эксплуатацию.

(Перечень предусмотренных мер защиты согласно предписанию).

2. Телефонный аппарат № 7-17.

3. Пульт коммутатора.

Выполнены требования предписания на эксплуатацию.

4. Часы электронные.

Выполнены требования предписания на эксплуатацию.

5. Вход в помещение оборудован тамбуром, двери двойные, обшиты слоем ваты и дермантина. Дверные притворы имеют резиновые уплотнения.

6. Доступ к вентиляционным каналам, выходящим на чердак здания, посторонних лиц исключен (приводятся предусмотренные для этого меры).

* 1. **Отметка о проверке средств защиты**

|  |  |  |  |
| --- | --- | --- | --- |
| Вид оборудования | Учетный  номер | Дата  проверки | Результаты проверки и  № отчетного документа |
|  |  |  |  |

* 1. **Результаты периодического контроля помещения**

|  |  |  |
| --- | --- | --- |
| Дата проведения | Результаты периодического контроля, № отчетного документа | Подпись  проверяющего |
|  |  |  |

**[ПРИЛОЖЕНИЕ 5](#_ПРИЛОЖЕНИЕ_4._РЕКОМЕНДУЕМАЯ_1). РЕКОМЕНДУЕМАЯ ТЕХНИКА ДЛЯ ПРОВЕДЕНИЯ ИНСТРУМЕНТАЛЬНЫХ ПРОВЕРОК**

|  |  |
| --- | --- |
| **Наименование** | **Назначение** |
| Аппаратура визуального обследования помещений | Обследование труднодоступных зон помещений (комплекты досмотровых зеркал, видеоэндоскопы, обнаружители скрытых видеокамер). |
| Аппаратура проведения радиомониторинга и поиска электронных устройств съема информации | Аппаратура для проведения радиоконтроля в рабочем диапазоне частот не менее 6 ГГц (анализаторы спектра, измерители частоты и мощности, многофункциональные поисковые приборы (с поиском электронных устройств съема информации, работающих по радиоканалу, использующих для передачи сигналов слаботочные и силовые линии, осуществляющих передачу сигналов в инфракрасном диапазоне излучения). |
| Аппаратура нелинейной локации | Аппаратура для поиска скрытно установленных электронных устройств, имеющих в своем составе полупроводниковые элементы. |

1. Помимо указанных документов специализированная организация может предоставить дополнительные документы. [↑](#footnote-ref-1)