Утвержден

постановлением

Правительства Новосибирской области

от \_\_\_\_\_\_\_\_\_\_\_ № \_\_\_\_\_\_\_\_\_\_\_\_\_

ПОРЯДОК

ВЗАИМОДЕЙСТВИЯ ОБЛАСТНЫХ ИСПОЛНИТЕЛЬНЫХ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ НОВОСИБИРСКОЙ ОБЛАСТИ,

ГОСУДАРСТВЕННЫХ ОРГАНОВ НОВОСИБИРСКОЙ ОБЛАСТИ В ЦЕЛЯХ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ

**Оглавление**

[Общие положения 3](#_Toc510005997)

[Основные понятия, термины и сокращения 3](#_Toc510005998)

[Защищаемая информация 6](#_Toc510005999)

[Система защиты информации Правительства Новосибирской области 7](#_Toc510006000)

[Губернатор Новосибирской области 7](#_Toc510006001)

[Коллегиальный орган 8](#_Toc510006002)

[Уполномоченный орган 8](#_Toc510006003)

[Руководители Органов 9](#_Toc510006004)

[Ответственные за организацию защиты информации в Органах 10](#_Toc510006005)

[Сотрудники Органов 11](#_Toc510006006)

[Угрозы безопасности информации 13](#_Toc510006007)

[Защита информации 14](#_Toc510006008)

[Организационные меры и средства защиты информации 15](#_Toc510006009)

[Определение прав доступа к информации 16](#_Toc510006010)

[Защита помещений и технических средств 17](#_Toc510006011)

[Правила обмена служебной информацией 19](#_Toc510006012)

[Использование информационных систем общего назначения Правительства Новосибирской области 21](#_Toc510006013)

[Использование технологий беспроводного доступа 23](#_Toc510006014)

[Доступ внешних пользователей 24](#_Toc510006015)

[Обращение с носителями защищаемой информации 25](#_Toc510006016)

[Технические меры защиты информации 26](#_Toc510006017)

[Антивирусная защита 26](#_Toc510006018)

[Защита от несанкционированного доступа 27](#_Toc510006019)

[Меры по ограничению программной среды 29](#_Toc510006020)

[Резервное копирование 30](#_Toc510006021)

[Обнаружение вторжений и межсетевое экранирование 30](#_Toc510006022)

[Аттестация ГИС и ИСПДн 31](#_Toc510006023)

[Внутренняя телефонная сеть 31](#_Toc510006024)

[Инциденты информационной безопасности 31](#_Toc510006025)

[Контроль 32](#_Toc510006026)

[Обучение, инструктаж, повышение квалификации 34](#_Toc510006027)

# Общие положения

Настоящий Порядок взаимодействия областных исполнительных органов государственной власти Новосибирской области, государственных органов Новосибирской области в целях обеспечения защиты информации (далее – Порядок) разработан в соответствии с Федеральными законами от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 № 152-ФЗ «О персональных данных», Законом Новосибирской области от 15.10.2007 № 138-ОЗ «О государственных информационных системах, государственных информационных ресурсах, территориальной информационной системе Новосибирской области» и другими нормативными правовыми актами, регулирующими вопросы безопасности информации, а также методическими документами федеральных органов исполнительной власти, осуществляющих функции по выработке государственной политики и нормативно-правовому регулированию в сфере защиты информации.

Порядок определяет политику информационной безопасности Правительства Новосибирской области, обязанности и ответственность по обеспечению защиты информации в государственных органах Новосибирской области, в областных исполнительных органах государственной власти Новосибирской области, в их территориальных органах и в подведомственных им учреждениях (далее – Органы).

Областные исполнительные органы государственной власти Новосибирской области, государственные органы Новосибирской области, указанные в настоящем Порядке ответственными за подготовку и согласование регламентирующих или методических документов, обеспечивают подготовку, утверждение, доведение до сведения заинтересованных Органов соответствующих регламентирующих и методических документов и их актуализацию в связи с изменением действующего законодательства, появлением новых угроз безопасности информации, внедрением новых информационных технологий и другими обстоятельствами.

# Основные понятия, термины и сокращения

В настоящем Порядке используются следующие основные понятия, термины и сокращения:

ГИС НСО – государственные информационные системы Новосибирской области. Межведомственными называются ГИС НСО, эксплуатируемые более чем в одном Органе.

ГИР НСО – государственные информационные ресурсы Новосибирской области.

Информационные системы Органа – информационные системы, не являющиеся ГИС НСО и владельцем (оператором) которых является Орган.

ИСПДн – информационные системы персональных данных.

Сеть Интернет – информационно-телекоммуникационная сеть международного информационного обмена "Интернет".

Сеть Правительства НСО – единая информационно-коммуникационная сеть Правительства Новосибирской области.

ГИСПД НСО – государственная инфокоммуникационная сеть передачи данных Новосибирской области, обеспечивающая для Органов, органов местного самоуправления Новосибирской области и подведомственных им учреждений доступ к ГИС НСО и ГИР НСО, защищенный доступ в сеть Интернет.

ЦОД Правительства НСО – основной и резервный центры обработки данных Правительства Новосибирской области, отказоустойчивый программно-аппаратный комплекс, обеспечивающий бесперебойное функционирование информационных систем и сервисов Сети Правительства НСО.

ЕСАЗ НСО – единая система антивирусной защиты Правительства Новосибирской области, представляющая собой совокупность централизованно управляемых программных и программно-аппаратных средств обнаружения и предотвращения вредоносной программной активности уровня сети, серверов и конечных устройств.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Уполномоченный орган – областной исполнительный орган государственной власти Новосибирской области, осуществляющий государственное управление и нормативное правовое регулирование в сфере информационных технологий, телекоммуникаций, связи, уполномоченный на создание государственных информационных систем и формирование государственных информационных ресурсов Новосибирской области, обеспечивающий совместно с подведомственными Уполномоченному органу учреждениями функционирование и защиту информации сети Правительства НСО, функционирование сетей передачи данных и инженерных систем и защиту информации ЦОД Правительства НСО, организацию защиты информации ГИС НСО и ГИР НСО, отдельных государственных органов, оказание методической помощи по обеспечению безопасности информации и осуществляет контроль состояния защиты конфиденциальной и иной охраняемой законом информации на объектах информатизации Органов.

Надзорные органы – территориальные органы федеральных органов исполнительной власти, федеральные службы, уполномоченные в сфере защиты информации и осуществляющие государственный контроль (надзор) в сфере защиты информации.

Пользователь Правительства НСО, пользователь – сотрудник Органа, имеющий права доступа к сети Правительства НСО, к ГИС НСО, ГИР НСО, к локальной вычислительной сети Органа, к информационным системам Органа.

АРМ пользователя – автоматизированное (компьютерное) рабочее место, предоставленное пользователю для исполнения его должностных (служебных) обязанностей.

Средства вычислительной техники - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Сетевое оборудование – технологическое оборудование, необходимое для построения локальных компьютерных сетей и глобальных сетей удаленного доступа.

Объекты информатизации – сеть Правительства НСО, ГИС НСО, ГИР НСО, информационные системы Органов, локальные компьютерные сети Органов, АРМ пользователей, комплексы технологического оборудования и средств вычислительной техники.

Внешний пользователь – сотрудник организации, права доступа которого к сети Правительства НСО, либо к ГИС НСО, ГИР НСО, либо к локальной вычислительной сети Органа, либо к информационным системам Органа определяет Орган, состоящий с указанной организацией в контрактных либо в договорных отношениях.

Учетная запись пользователя в информационной системе – сведения о пользователе в информационной системе, включая права доступа пользователя и идентифицирующую пользователя информацию. Учетная запись позволяет пользователю пройти процедуры идентификации (предъявления идентификатора, логина пользователя), аутентификации (проверки подлинности пользователя) и авторизации (предоставления пользователю доступа в соответствии с установленными для него правами доступа) в информационной системе.

Служба поддержки пользователей – система обслуживания пользователей Правительства Новосибирской области в сфере информационных технологий, включающая подразделения Уполномоченного органа, подведомственных Уполномоченному органу учреждений, технические средства и программное обеспечение.

Служба инцидентов ИБ – коллегиальный орган из сотрудников подразделений Уполномоченного органа и подведомственных Уполномоченному органу учреждений, деятельность которого предполагает выявление инцидентов информационной безопасности, сбор сведений о них, расследование причин и условий появления инцидентов информационной безопасности, организацию ликвидации последствий инцидентов информационной безопасности, разработку предложений по предупреждению возникновения инцидентов информационной безопасности, направление сведений о произошедших инцидентах информационной безопасности.

Администраторы сети Правительства НСО – сотрудники Уполномоченного органа, подведомственных Уполномоченному органу учреждений, в должностные обязанности которых входит управление учетными записями пользователей в сети Правительства Новосибирской области, распределение доступа пользователей и управление настройками программных и технических средств сети Правительства НСО.

Администраторы ГИС НСО, информационных систем Органов – сотрудники Уполномоченного органа, подведомственных Уполномоченному органу учреждений или Органов, в должностные обязанности которых входит управление учетными записями пользователей в ГИС НСО, в информационных системах Органов, распределение доступа пользователей к ГИС НСО, к информационным системам Органов и управление настройками программных и технических средств ГИС НСО или информационных систем Органов.

Администраторы безопасности – ответственные сотрудники Уполномоченного органа, подведомственных Уполномоченному органу учреждений или Органов, в должностные обязанности которых входит обеспечение безопасности определенных объектов (выделенных помещений, объектов информатизации, автоматизированных систем, систем защиты информации и пр.).

Локальный администратор (роль) – роль, которая назначается учетной записи пользователя и позволяет администрировать АРМ пользователя.

Выделенные помещения – помещения Органов, предназначенные для проведения мероприятий, связанных с обсуждением информации, содержащей сведения, составляющие государственную тайну.

Организация-лицензиат ФСТЭК России – юридическое лицо (индивидуальный предприниматель), имеющее действующую лицензию на осуществление деятельности по технической защите конфиденциальной информации, выданную Федеральной службой по техническому и экспортному контролю в соответствии с Федеральным законом от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности» и Постановлением Правительства РФ от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации».

Организация-лицензиат ФСБ России и ФСТЭК России – юридическое лицо, имеющее действующую лицензию на деятельность предприятий, учреждений и организаций на проведение работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны, выданную Федеральной службой безопасности в соответствии с Законом РФ от 21.07.1993 № 5485-1 «О государственной тайне», а также действующую лицензию на осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны (в части технической защиты информации), выданную Федеральной службой по техническому и экспортному контролю в соответствии с Постановлением Правительства РФ от 15.04.1995 № 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны».

Термины, не указанные в настоящем разделе, используются в определениях Федеральных законов от 27.07.2006 № 149-ФЗ, от 27.07.2006 № 152-ФЗ, от 26.07.2017 № ФЗ-187, Указа Президента РФ от 17.03.2008 № 351, постановлений Правительства Российской Федерации от 01.11.2012 № 1119, от 03.02.2012 № 79, от 03.11.1994 № 1233, Закона Новосибирской области от 15.10.2007 № 138-ОЗ, нормативно-методического документа Гостехкомиссии при Президенте Российской Федерации «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)», приказов ФСТЭК России от 11.02.2013 № 17, от 18.02.2013 № 21, национальных стандартов ГОСТ Р 57628-2017, ГОСТ Р ИСО/МЭК 27002-2012, ГОСТ Р ИСО/МЭК 15408-1-2012, ГОСТ Р ИСО/МЭК 27002-2012, ГОСТ Р 50922-2006, ГОСТ Р 51275-2006, ГОСТ Р ИСО/МЭК 27001-2006, Р 50.1.053-2005, Р 50.1.056-2005, ГОСТ Р ИСО/ТО 13569-2007 и других.

# Защищаемая информация

Информация, использующаяся в служебной деятельности Органов, подлежит защите.

Для общедоступной информации (информации о деятельности Органа, размещенной на официальном сайте Органа, сведений о порядке оказания государственных услуг и другой информации, доступ к которой не может быть ограничен в соответствии с действующим законодательством) должны быть обеспечены её доступность и целостность. Для информации, доступ к которой ограничен федеральными законами, и служебной информации ограниченного доступа кроме доступности и целостности должна быть обеспечена конфиденциальность.

Информация, доступ к которой ограничен федеральными законами, является информацией ограниченного доступа. Информация ограниченного доступа подразделяется на информацию, содержащую сведения, составляющие государственную тайну, и на информацию конфиденциального характера, т.е. информацию ограниченного доступа, не содержащую сведений, составляющих государственную тайну.

Виды информации конфиденциального характера определяются Федеральными законами, указами Президента Российской Федерации. К информации конфиденциального характера относится также служебная информация ограниченного распространения (информация, касающаяся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью), за исключением информации, доступ к которой не может быть ограничен в соответствии с действующим законодательством. Перечень информации конфиденциального характера (в том числе персональных данных), обрабатываемой в Органе, утверждается руководителем Органа или организационно-распорядительным документом Органа.

Информация может быть представлена в форме информационных систем, в звуковой форме (речевая информация), на материальных носителях (при обработке информации без использования средств автоматизации либо при сохранении на съемные машинные носители информации). В информационных системах объектами защиты являются информация, содержащаяся в информационной системе, технические средства (в том числе средства вычислительной техники, средства и системы связи и передачи данных), программное обеспечение, информационные технологии, а также средства защиты информации.

# Система защиты информации Правительства Новосибирской области

Систему защиты информации Правительства Новосибирской области возглавляет Губернатор Новосибирской области. В структуру системы защиты информации Правительства Новосибирской области входят:

- Коллегиальный орган Новосибирской области по информационной безопасности;

- Уполномоченный орган, подведомственные Уполномоченному органу учреждения;

- руководители всех Органов;

- ответственные за организацию защиты информации в Органах;

- сотрудники Органов.

## Губернатор Новосибирской области

Губернатор Новосибирской области как высшее должностное лицо Новосибирской области возглавляет систему защиты информации Правительства Новосибирской области и отвечает за состояние защиты информации в Правительстве Новосибирской области и в Органах.

## Коллегиальный орган

Коллегиальный орган Новосибирской области по информационной безопасности (далее – Коллегиальный орган по информационной безопасности) обеспечивает взаимодействие и согласованные действия областных исполнительных органов государственной власти Новосибирской области, территориальных органов федеральных органов исполнительной власти в Новосибирской области, организаций различных форм собственности при решении задач в сфере обеспечения информационной безопасности в Новосибирской области.

В задачи Коллегиального органа по информационной безопасности входят выработка рекомендаций по повышению эффективности информационной безопасности в Новосибирской области; мониторинг состояния информационной безопасности в Новосибирской области; обеспечение согласованных действий по разработке концептуальных подходов к обеспечению информационной безопасности; анализ состояния защиты информации ограниченного доступа в государственных органах Новосибирской области, в областных исполнительных органах государственной власти Новосибирской области, их территориальных органах и подведомственных им учреждениях; подготовка предложений по совершенствованию правового, нормативно-методического, научно-технического и организационного обеспечения информационной безопасности Новосибирской области; анализ состояния защиты информации, обработка которой осуществляется автоматизированными системами управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды Новосибирской области; другие задачи в сфере обеспечения информационной безопасности в Новосибирской области.

Коллегиальный орган по информационной безопасности является совещательным органом при Губернаторе Новосибирской области. Возглавляет Коллегиальный орган по информационной безопасности Губернатор Новосибирской области либо заместитель Губернатора Новосибирской области, курирующий вопросы защиты информации. Организационно-техническое обеспечение деятельности Коллегиального органа по информационной безопасности обеспечивает Уполномоченный орган.

## Уполномоченный орган

Уполномоченный орган в целях обеспечения защиты информации в пределах своих полномочий обеспечивает и осуществляет:

1) принятие мер по защите информации о деятельности областных исполнительных органов государственной власти Новосибирской области в соответствии с законодательством Российской Федерации, а именно:

- организация работы по защите информации конфиденциального характера в сети Правительства НСО в части координации деятельности по обеспечению безопасности информации в сети Правительства НСО, ГИС НСО и ГИР НСО, оказание методической помощи по обеспечению безопасности информации и осуществление контроля состояния защиты информации конфиденциального характера на объектах информатизации администрации Губернатора Новосибирской области и Правительства Новосибирской области и областных исполнительных органов государственной власти Новосибирской области, а также проведение аудита состояния защиты информации в подведомственных им учреждениях;

- в соответствии с законодательством Российской Федерации в области защиты государственной тайны организация защиты информации, содержащей сведения, составляющие государственную тайну, на объектах информатизации структурных подразделений администрации Губернатора Новосибирской области и Правительства Новосибирской области, координация деятельности Органов по вопросам обеспечения защиты государственной тайны, оказание методической помощи и осуществление контроля за организацией и состоянием защиты информации.

2) доступ к ресурсам сети Правительства НСО сотрудникам Органов; доступ к ГИСПД НСО сотрудникам органов местного самоуправления в Новосибирской области; обеспечение услугами фиксированной телефонной связи, внедрение IP-телефонии в администрации Губернатора Новосибирской области и Правительства Новосибирской области, исполнительных органах государственной власти Новосибирской области;

3) техническое администрирование, поддержку серверного и коммуникационного оборудования единой информационно-коммуникационной сети Правительства Новосибирской области, планирование технических, программных и информационных ресурсов единой информационно-коммуникационной сети Правительства Новосибирской области, локальных компьютерных сетей в здании Правительства Новосибирской области.

## Руководители Органов

Ответственность за обеспечение защиты информации в соответствии с требованиями действующего законодательства в Органе возлагается на его руководителя.

Руководитель Органа определяет персональную ответственность сотрудников Органа за выполнение требований Порядка, за правильность эксплуатации предоставленных сотрудникам для исполнения служебных обязанностей технических средств и установленных на них средств защиты информации; определяет полномочия сотрудников Органа по обработке защищаемой информации; организует повышение квалификации сотрудников Органа в сфере защиты информации; организует контроль выполнения мер по защите информации в Органе; утверждает организационно-распорядительные, инструктивные и проектные документы Органа по защите информации, в том числе перечень информации конфиденциального характера, обрабатываемой в Органе, перечень сотрудников (должностей сотрудников), допущенных к обработке защищаемой информации, модель угроз безопасности информации и другие; исполняет иные обязанности руководителя в области защиты информации.

Руководитель Органа назначает ответственного за организацию защиты информации в Органе (штатный сотрудник или структурное подразделение Органа) для организации и ведения деятельности по защите информации в Органе. Ответственный за организацию защиты информации в Органе назначается распорядительным документом Органа.

В случае, если в Органе имеются выделенные помещения или автоматизированные системы, предназначенные для обработки информации, содержащей сведения, составляющие государственную тайну, кроме назначения ответственного за организацию защиты информации в Органе назначаются ответственные за осуществление мероприятий по защите информации в ходе выполнения работ с использованием сведений, отнесенных к государственной тайне (администраторы информационной безопасности) для каждого выделенного помещения и автоматизированной системы[[1]](#footnote-1). В обязательном порядке создаётся постоянно действующая техническая комиссия по защите государственной тайны[[2]](#footnote-2).

Руководители областных исполнительных органов государственной власти Новосибирской области курируют защиту информации в подведомственных им государственных организациях (учреждениях и предприятиях). Руководители Органов могут создавать коллегиальные органы по вопросам защиты информации, в том числе с участием представителей подведомственных Органам организаций.

## Ответственные за организацию защиты информации в Органах

Ответственным за организацию защиты информации в Органе назначается сотрудник (должностное лицо) Органа или структурное подразделение по защите информации в Органе, исходя из условий функционирования Органа (количество сотрудников, обрабатывающих защищаемую информацию, количество и расположение помещений, в которых обрабатывается защищаемая информация и пр.) Органа и класса (уровня защищенности, категории) информационных систем, оператором которых является Орган. Ответственный за организацию защиты информации в Органе назначается распорядительным документом Органа; в случае, если ответственный за организацию защиты информации в Органе не назначен, ответственным за организацию защиты информации является руководитель Органа.

На ответственного за организацию защиты информации в Органе возлагаются следующие функциональные обязанности, включаемые в должностную инструкцию:

- доведение до сведения сотрудников Органа положений законодательства Российской Федерации в сфере защиты информации;

- ознакомление сотрудников Органа с настоящим Порядком, с указанными в настоящем Порядке регламентирующими и методическими документами, с организационно-распорядительными и инструктивными документами Органа по защите информации путём проведения периодического инструктажа всех сотрудников и обязательного первичного инструктажа вновь принятых сотрудников; ведение журнала проведения инструктажа сотрудников Органа;

- подготовка проектов организационно-распорядительных и инструктивных документов Органа по защите информации; подготовка проектов и обновление (актуализация) принятых в соответствии с требованиями действующего законодательства документов Органа по защите информации: перечня информации конфиденциального характера, обрабатываемой в Органе; перечня сотрудников (должностей сотрудников), допущенных к обработке защищаемой информации; перечня информационных систем, эксплуатируемых в Органе, и других;

- проведение организационных мер защиты информации в Органе;

- подготовка предложений по финансированию работ по технической защите информации в Органе; участие в рассмотрении проектов технических заданий и описания объектов закупок по технической защите информации; сопровождение исполнения контрактов по технической защите информации в Органе, по аттестации информационных систем Органа по требованиям безопасности информации;

- в пределах своих полномочий осуществление контроля исполнения требований настоящего Порядка, организационно-распорядительных и инструктивных документов Органа по защите информации; участие в проведении внутреннего контроля соблюдения положений организационно-распорядительных, инструктивных и методических документов по защите информации, правильности эксплуатации средств защиты информации в Органе;

- в пределах своих полномочий осуществление контроля применения и обслуживания средств защиты информации, установленных в Органе; оказание в своей зоне ответственности помощи пользователям в работе с эксплуатируемыми техническими и программными средствами защиты информации;

- своевременное извещение Службы инцидентов ИБ о произошедших в Органе инцидентах информационной безопасности на основании сообщений сотрудников Органа и собственных наблюдений; участие в расследовании инцидентов ИБ, произошедших в Органе;

- подготовка докладов руководителю Органа о нарушениях требований настоящего Порядка, организационно-распорядительных и инструктивных документов Органа по защите информации сотрудниками Органа; подготовка представлений руководителю Органа о привлечении виновных сотрудников к дисциплинарной ответственности;

- сопровождение мероприятий по контролю выполнения мер по защите информации, проводимых Уполномоченным органом; сопровождение проверок по вопросам защиты информации, проводимых надзорными органами;

- разработка проектов планов работ Органа по обеспечению защиты информации, подготовка отчетов о проведенной работе по обеспечению защиты информации;

- взаимодействие с Уполномоченным органом и с подведомственными Уполномоченному органу учреждениями по вопросам организации защиты информации;

- систематическое повышение своей квалификации в сфере защиты информации.

## Сотрудники Органов

Сотрудники Органов должны быть ознакомлены с настоящим Порядком и с указанными в настоящем Порядке регламентирующими и методическими документами, а также с организационно-распорядительными и инструктивными документами Органа по защите информации. Инструктаж по вопросам защиты информации в Органе проводит ответственный за организацию защиты информации в Органе либо организует руководитель Органа. После прохождения инструктажа по вопросам защиты информации сотрудники Органа должны расписаться в журнале проведения инструктажа.

Сотрудник Органа обязан соблюдать правила, предписанные указанными выше документами; об известных ему нарушениях правил сообщать ответственному за организацию защиты информации в Органе, в его отсутствие – непосредственному руководителю; содействовать в поддержании режима конфиденциальности информации; об известных ему инцидентах информационной безопасности своевременно сообщать ответственному за организацию защиты информации в Органе и в Службу инцидентов ИБ.

Сотрудники Органов обязаны:

- при работе с документами и иными материальными носителями, содержащими защищаемую информацию, неуклонно следовать положениям инструкций, регламентирующих обращение с указанными документами и материальными носителями;

- использовать находящиеся в их пользовании средства вычислительной техники и программного обеспечения в соответствии со своими должностными (служебными) обязанностями;

- при обнаружении неисправностей в работе средств вычислительной техники, программного обеспечения, ГИС НСО и ГИР НСО сообщать о них в Службу поддержки пользователей;

- соблюдать правила работы со средствами защиты информации; самовольно не отключать установленные на АРМ пользователя и в помещении средства защиты информации;

- не разглашать используемые пароли доступа в сети Правительства НСО, в ГИС НСО, в информационных системах Органов, электронной почты третьим лицам и не предоставлять другим сотрудникам Органа;

- не использовать для работы учетные записи других сотрудников Органа;

- не предоставлять доступа под своей либо иной учетной записью сторонним лицам (незарегистрированным пользователям);

- блокировать экран АРМ пользователя (путём блокирования компьютера или использования защищенных паролем экранных заставок) на время своего отсутствия на рабочем месте;

- использовать только разрешенное к эксплуатации (предустановленное на АРМ пользователя либо устанавливаемое специалистами Службы поддержки пользователей) программное обеспечение; не вносить изменений в аппаратную и программную конфигурацию АРМ пользователя;

- не подключать к АРМ пользователей неучтенные машинные носители информации;

- не подключать к АРМ пользователей, к сети Правительства НСО, к локальным компьютерным сетям Органов личные мобильные устройства (за исключением подключения к WiFi-сетям Органов для централизованного выхода в сеть Интернет, указанным в разделе «Использование технологий беспроводного доступа»);

- использовать на рабочем месте доступ к сети Интернет исключительно для выполнения должностных (служебных) обязанностей;

- при работе в сети Интернет следует избегать посещения сайтов, содержимое которых нарушает законодательство РФ, и анонимайзеров (средств для скрытия информации о компьютере или пользователе в сети Интернет).

Сотрудник Органа допускается к обработке защищаемой информации на основании организационно-распорядительного документа Органа (приказа, утвержденного руководителем Органа перечня сотрудников (должностей сотрудников), допущенных к обработке защищаемой информации, должностного регламента или должностной инструкции сотрудника и т.д.). Орган заключает с сотрудниками, допущенными к обработке информации конфиденциального характера, соглашения о неразглашении конфиденциальной информации на основании типового соглашения, разрабатываемого Уполномоченным органом.

Сотрудник Органа, допущенный к обработке защищаемой информации, обязан соблюдать конфиденциальность информации, к обработке которой он допущен, а также иной служебной информации, ставшей ему известной при исполнении служебных обязанностей, т.е. не передавать защищаемую информацию третьим лицам без согласия ее обладателя и не использовать её в неслужебных целях. Нарушение конфиденциальности информации сотрудником влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Ответственность сотрудников Органов за нарушение требований настоящего Порядка и указанных в настоящем Порядке регламентирующих и методических документов, зафиксированное актом внутреннего контроля Органа либо Службой инцидентов ИБ:

- в случае однократного нарушения непосредственный руководитель виновного сотрудника делает замечание;

- в случае неоднократного нарушения, по представлению ответственного за организацию защиты информации в Органе, Уполномоченного органа либо Службы инцидентов ИБ, руководством Органа проводится служебная проверка, по итогам которой выносится соответствующее решение о применении дисциплинарного взыскания; сведения о наложенном дисциплинарном взыскании Орган передает в Службу инцидентов ИБ;

- в случае неоднократного нарушения после дисциплинарного взыскания доступ виновного сотрудника к ресурсам сети Правительства НСО, к отдельным ГИС НСО и ГИР НСО, информационным системам Органов может быть прекращён Уполномоченным органом, подведомственным Уполномоченному органу учреждением, Органом-владельцем (оператором) информационной системы; сведения об ограничении или прекращении доступа доводятся до сведения руководителя Органа; руководством Органа может быть поставлен вопрос о служебном соответствии виновного сотрудника.

# Угрозы безопасности информации

Под актуальными угрозами безопасности информации понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к защищаемой информации при ее обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, неправомерноераспространение защищаемой информации, а также иные неправомерные действия и негативные воздействия. Для определения актуальных угроз безопасности обрабатываемой информации используются положения действующего федерального законодательства, Банк данных угроз безопасности информации и уязвимостей (www.bdu.fstec.ru) Федеральной службы по техническому и экспортному контролю, нормативные правовые акты Новосибирской области[[3]](#footnote-3).

Перечень актуальных угроз должен использоваться при построении частных моделей угроз безопасности информации (персональных данных, государственных информационных систем, иной защищаемой информации) (далее – модель угроз) и моделей нарушителя информационных систем персональных данных и государственных информационных систем Новосибирской области (далее – модель нарушителя), эксплуатируемых в Органах. Построение указанных моделей Орган может проводить самостоятельно или привлекать организацию-лицензиат ФСТЭК России.

В целях выполнения требований о защите информации в информационных системах, собственником или оператором которых является Орган, при содействии Уполномоченного органа, подведомственных Уполномоченному органу учреждений либо с привлечением организации-лицензиата ФСТЭК России Орган:

- проводит классификацию (категорирование) информационных систем, в которых обрабатывается защищаемая информация, в соответствии с требованиями о защите информации, утверждает акты классификации (категорирования) информационных систем;

- на основе модели угроз и модели нарушителя определяет требования к системе защиты информации, содержащейся в системе, которые оформляются в виде технического задания (технического проекта) на создание системы защиты информации (далее – техническое задание). Модель угроз и техническое задание для ГИС НСО Орган согласует с Управлением ФСТЭК России по Сибирскому федеральному округу, в части выполнения установленных требований о защите информации. Согласованная модель угроз, модель нарушителя и техническое задание утверждаются руководителем Органа.

- организует проведение мероприятий по созданию системы защиты информации и по аттестации информационных систем по требованиям безопасности информации.

# Защита информации

Защита информации – это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, обеспечивающая безопасность информации, ее конфиденциальность, доступность и целостность. Меры по защите информации применяются для нейтрализации актуальных угроз безопасности информации.

Методы защиты информации определяются Федеральными законами, нормативными правовыми актами Правительства Российской Федерации, методическими и руководящими документами уполномоченных федеральных органов исполнительной власти.

Техническую защиту информации, содержащей сведения, составляющие государственную тайну, на объектах информатизации администрации Губернатора Новосибирской области и Правительства Новосибирской области организует Уполномоченный орган, подведомственные Уполномоченному органу учреждения с привлечением организаций-лицензиатов ФСБ России и ФСТЭК России. На объектах информатизации иных Органов защиту информации, содержащей сведения, составляющие государственную тайну, организуют Органы с привлечением организаций-лицензиатов ФСБ России и ФСТЭК России.

Защиту общедоступной информации организует Уполномоченный орган и подведомственные Уполномоченному органу учреждения.

Защиту информации конфиденциального характера организует каждый Орган при возможном участии Уполномоченного органа, подведомственных Уполномоченному органу учреждений и с привлечением организаций-лицензиатов ФСТЭК России.

# Организационные меры и средства защиты информации

В целях организации защиты информации конфиденциального характера в каждом Органе должны проводиться организационные меры в соответствии с требованиями действующего законодательства, основные из них:

- назначение ответственного за организацию защиты информации в Органе (сотрудник (должностное лицо) Органа или структурное подразделение по защите информации в Органе);

- определение защищаемой информации, обрабатываемой в Органе, формирование и утверждение перечня информации ограниченного доступа (информации конфиденциального характера, персональных данных, информационных систем с обработкой информации ограниченного доступа, эксплуатируемых в Органе, и т.п.);

- определение сотрудников (должностей), которым необходим доступ к защищаемой информации для выполнения служебных обязанностей; утверждение перечня сотрудников (должностей), допущенных к обработке защищаемой информации;

- формирование и утверждение организационно-распорядительных документов по защите персональных данных и иной защищаемой информации Органа. Примерный перечень и шаблоны указанных документов разрабатывает и размещает на своём официальном сайте Уполномоченный орган;

- проведение ознакомления сотрудников Органа с документами, регламентирующими защиту информации;

- проведение классификации информационных систем или сегментов информационных систем, оператором которых является Орган; утверждение актов классификации информационных систем;

- определение актуальных угроз безопасности информации; формирование, при необходимости согласование с Управлением ФСТЭК России по Сибирскому федеральному округу и утверждение частной модели угроз и модели нарушителя;

- определение актуальных угроз безопасности информации; формирование, согласование с Управлением ФСТЭК России по Сибирскому федеральному округу и утверждение частной модели угроз и модели нарушителя для ГИС НСО, оператором которых является Орган;

- организация создания и внедрения системы защиты информации и аттестации информационных систем по требованиям безопасности информации;

- организация создания и внедрения системы защиты информации и аттестации по требованиям безопасности информации:

а) информационных систем, оператором которых является Орган;

б) сегментов ГИС НСО и АРМ пользователей Органа, подключаемых к информационным системам, оператором которых являются иные Органы;

- организация внутреннего контроля выполнения мер по защите информации.

## Определение прав доступа к информации

Права доступа сотрудников Органов к информации ограниченного доступа должны определяться исходя из должностных обязанностей сотрудников. Сотрудникам должны назначаться минимально необходимые права и привилегии пользователей, администраторов информационных систем, администраторов безопасности; сотруднику, выполняющему различные по уровню доступа функции, должны предоставляться права доступа (роли), разделяющие полномочия пользователя и администратора.

Доступ сотрудников Органа к информации, содержащей сведения, составляющие государственную тайну, осуществляется после оформления допуска сотрудников Органа к государственной тайне в соответствии с действующим законодательством[[4]](#footnote-4) и при наличии у Органа разрешения органа безопасности на работу со сведениями, составляющими государственную тайну, либо лицензии на осуществление работ, связанных с использованием сведений, составляющих государственную тайну.

Доступ сотрудников Органа к информации конфиденциального характера (в том числе к персональным данным) определяется на основании утвержденного руководителем Органа перечня сотрудников (должностей), допущенных к обработке информации конфиденциального характера (в том числе персональных данных).

Права доступа сотрудников Органа к сети Правительства НСО и к информационным системам общего назначения Правительства Новосибирской области устанавливают администраторы сети Правительства НСО на основании официального запроса Органа. Права доступа сотрудников Органа к ГИС НСО устанавливают администраторы ГИС НСО на основании официального запроса Органа.

Права доступа сотрудников Органа к информационным системам Органа устанавливают администраторы информационных систем Органа в соответствии с документированным указанием руководителя Органа. Доступ сотрудников Органа к общим папкам и файлам Органа должен быть ограничен.

Управление правами доступа сотрудников Органа к сети Правительства НСО, к ГИС НСО и ГИР НСО, к информационным системам Органа состоит в назначении минимально необходимых прав доступа; в пересмотре прав доступа при смене должности или обязанностей сотрудника; в прекращении прав доступа (блокировании учетных записей) при увольнении сотрудника. В целях осуществления указанных функций управления Орган должен направлять администраторам сети Правительства НСО, администраторам ГИС НСО, администраторам информационных систем Органа сведения о приёме на работу сотрудников Органа, которым должны быть назначены права доступа, о смене должностных обязанностей и соответствующем изменении прав доступа сотрудников Органа, о временном отсутствии, об увольнении сотрудников Органа в соответствии с регламентом, согласованным с департаментом организации управления и государственной гражданской службы администрации Губернатора Новосибирской области и Правительства Новосибирской области и утвержденным Уполномоченным органом.

Для АРМ пользователей, на которых производится обработка информации, содержащей сведения, составляющие государственную тайну, документально оформляется разрешительная система доступа для каждого АРМ пользователя.

Органы, являющиеся операторами ГИС НСО, информационных систем Органов, ведут перечни пользователей каждой ГИС НСО, информационной системы Органа в соответствии с регламентом, утверждаемым Уполномоченным органом. Перечень пользователей обновляется (актуализируется) ведущим его Органом на постоянной основе.

Перечень пользователей сети Правительства НСО ведется Уполномоченным органом, подведомственными Уполномоченному органу учреждениями в соответствии с распорядительным документом Уполномоченного органа.

Подключение Органов к сети Правительства НСО, подключение Органов, органов местного самоуправления Новосибирской области и муниципальных учреждений к ГИСПД НСО производится Уполномоченным органом, подведомственными Уполномоченному органу учреждениями на основании официального запроса и при выполнении условий подключения, утверждаемых Уполномоченным органом.[[5]](#footnote-5)

Несанкционированный (осуществляемый с нарушением установленных прав доступа) доступ к информации является инцидентом информационной безопасности.

## Защита помещений и технических средств

Меры по защите информации включают контроль и управление физическим доступом к техническим средствам обработки информации, средствам защиты информации, средствам обеспечения функционирования информационных систем (далее – технические средства), а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к указанным техническим средствам, их хищение или нарушение работоспособности, хищение носителей информации. Необходимо также обеспечивать защиту технических средств от внешних воздействий: воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов. Охрана помещений, занимаемых Органами, должна обеспечивать круглосуточный контроль доступа в помещения.

Охрану зданий Правительства Новосибирской области по адресам Красный проспект, д. 18, д. 25, ул. Кирова, д. 3 (далее – здания Правительства НСО) организует Орган, в полномочия которого включены охрана объектов и служебных помещений, занимаемых Правительством Новосибирской области, заместителями Губернатора Новосибирской области, Правительством Новосибирской области, администрацией Губернатора Новосибирской области и Правительства Новосибирской области, Законодательным Собранием Новосибирской области, государственными органами Новосибирской области; соблюдение пропускного режима в зданиях Правительства НСО; обеспечение эксплуатационно-технического обслуживания зданий Правительства НСО[[6]](#footnote-6).

В зданиях Правительства НСО развёрнуты системы охранной и пожарной сигнализации, оповещения и управления эвакуацией, контроля и управления доступом, видеонаблюдения, управления пожарной автоматикой, управления инженерными подсистемами; сигналы тревоги выводятся на пульт централизованного наблюдения, который оборудован на круглосуточном посту охраны. Система контроля и управления доступом позволяет проводить электронную идентификацию для входа в защищаемые помещения с автоматической постановкой/снятием с охраны помещений по факту идентификации сотрудника; обеспечивает реакцию охранной сигнализации на попытки несанкционированного доступа либо взлома. Для обеспечения антитеррористической защищенности имеется кнопка тревожной сигнализации для экстренного вызова полиции.

Охрану помещений, занимаемых Органами по иным адресам, организуют Органы с исполнением указанных выше требований.

Основные обязанности по обеспечению защиты информации в помещениях, предназначенных для проведения мероприятий, связанных с обсуждением информации, содержащей сведения, составляющие государственную тайну (далее – выделенные помещения), и на средствах вычислительной техники при обработке, изготовлении и размножении документов, содержащих сведения, составляющие государственную тайну (далее – объекты информатизации), определяются нормативным правовым актом Губернатора Новосибирской области. Руководители Органов при наличии выделенных помещений или при использовании объектов информатизации назначают ответственных за обеспечение защиты информации и администраторов информационной безопасности в соответствующих выделенных помещениях и на объектах информатизации. Режим доступа в выделенные помещения, аттестованные по требованиям безопасности информации, определяется инструкциями ответственному за соответствующие помещения[[7]](#footnote-7).

Для защиты АРМ пользователей, мест хранения материальных носителей информации от беспрепятственного доступа и наблюдения Органами определяется контролируемая зона Органа, для помещений которой Орган определяет перечень сотрудников (должностей), имеющих право доступа в помещения, и в которой исключает неконтролируемое пребывание посетителей, проникновение посторонних лиц и посторонних технических средств. Орган обеспечивает размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр; предотвращение хищения или порчи, размещенных в контролируемой зоне технических средств; использование систем бесперебойного электропитания технических средств; организацию ремонта технических средств Органа в режиме, исключающем считывание записанной или восстановление стертой информации сторонними лицами.

ЦОД Правительства НСО, центры обработки данных и серверные Органов, иные помещения, в которых располагается телекоммуникационное оборудование, должны находиться под постоянным контролем; доступ в указанные помещения, в том числе перечень сотрудников, имеющих право доступа, должен быть регламентирован Органами, в оперативном управлении которых находятся помещения. Для обеспечения отказоустойчивого функционирования ЦОД Правительства НСО, центров обработки данных Органов должно быть реализовано гарантированное бесперебойное электропитание и оборудование системой кондиционирования и системой пожаротушения.

Уполномоченный орган, подведомственные Уполномоченному органу учреждения организуют устойчивое функционирование ЦОД Правительства НСО, обеспечивают гарантированное бесперебойное электропитание, оборудование системами контроля доступа в помещения, кондиционирования и пожаротушения[[8]](#footnote-8).

## Правила обмена служебной информацией

Официальными средствами ведения служебной электронной переписки в Органах являются сервисы электронной почты, файлового обмена, обмена электронными сообщениями и другого информационного обмена с помощью электронных сервисов (далее – сервисы обмена), находящиеся в пространстве доменных имен Правительства Новосибирской области (nso.ru и другие зарегистрированные доменные имена Правительства Новосибирской области), а также сервисы обмена, удовлетворяющие условиям использования в служебных целях сервисов обмена, определяемым Уполномоченным органом[[9]](#footnote-9). Доступ к сервисам обмена, не удовлетворяющим указанным условиям, в сети Правительства НСО ограничивается Уполномоченным органом, подведомственными Уполномоченному органу учреждениями.

Сотрудники Органов для переписки в служебных целях используют учетные записи электронной почты nso.ru и на почтовых серверах Органов, включённых в перечень официальных средств ведения служебной переписки. Доступ к почтовым серверам, не включенным в перечень официальных средств ведения служебной переписки, ограничивается Уполномоченным органом, подведомственными Уполномоченному органу учреждениями.

Перечень адресов электронной почты nso.ru ведёт Уполномоченный орган или подведомственное Уполномоченному органу учреждение. Создание индивидуального или группового адреса электронной почты nso.ru осуществляется на основании официального запроса Органа с указанием фамилии, имени, отчества, должности сотрудника (или нескольких сотрудников), служебного телефона, обоснования (для группового адреса). Создание, изменение, удаление адресов, использование электронной почты nso.ru производятся в соответствии с регламентом, утверждаемым Уполномоченным органом.

Объем почтового ящика (хранилища входящих и исходящих сообщений) на почтовом сервере ограничен. Настройка автоматической переадресации входящих писем на адреса сторонних почтовых сервисов запрещена. Настроена автоматическая антивирусная проверка и антиспам-фильтрация входящих сообщений.

Доступ к адресам электронной почты nso.ru через сеть Интернет осуществляется в соответствии с регламентом, утверждаемым Уполномоченным органом, при этом авторизация на почтовом сервисе производится по учетной записи в сети Правительства НСО.

Передача информации конфиденциального характера производится в соответствии с регламентированными процедурами (административными регламентами оказания услуг, регламентами функционирования информационных систем и т.д.), по запросам территориальных органов федеральных органов исполнительной власти, иных органов государственной власти, имеющих соответствующие полномочия в соответствии с действующим законодательством, по официальному обращению, содержащему обоснованное требование о предоставлении информации конфиденциального характера (от субъекта персональных данных и т.д.).

Передача информации конфиденциального характера в электронном виде производится только по защищенным каналам связи (из ГИС НСО через систему электронного межведомственного взаимодействия, по Деловой почте ViPNet и т.д.). В вербальной (речевой) форме информация конфиденциального характера может обсуждаться без использования технических средств в защищаемых, режимных помещениях, иных помещениях контролируемой зоны, определенных распорядительными документами Органа, а также передаваться на сеансах защищенной видеоконференцсвязи, по телефонам специальной связи.

Передача информации, содержащей сведения, составляющие государственную тайну, в электронном виде по каналам связи не производится. Для обсуждения вопросов, связанных с государственной тайной, оборудуются выделенные помещения, которые защищаются и аттестуются по требованиям безопасности информации.

## Использование информационных систем общего назначения Правительства Новосибирской области

В настоящем разделе будут рассмотрены такие информационные системы общего назначения Правительства Новосибирской области, как Система электронного документооборота и делопроизводства Правительства Новосибирской области, типовой официальный сайт исполнительного органа государственной власти Новосибирской области в сети Интернет, Служба поддержки пользователей сети Правительства НСО.

Система электронного документооборота и делопроизводства Правительства Новосибирской области (далее – СЭДД Правительства НСО) обеспечивает подключенным к СЭДД Правительства НСО Органам документооборот и электронное делопроизводство. Электронные документы в СЭДД Правительства НСО, подписанные простой электронной подписью, признаются равнозначными документам на бумажных носителях, подписанным собственноручной подписью[[10]](#footnote-10).

Доступ к СЭДД Правительства НСО осуществляется с рабочих мест в сети Правительства НСО; доступ с мобильных рабочих мест через сеть Интернет осуществляется по защищенному каналу связи с использованием технологии ViPNet Custom.

Перечень пользователей СЭДД Правительства НСО ведёт Уполномоченный орган или подведомственное Уполномоченному органу учреждение. Учетные записи пользователей в СЭДД Правительства НСО создаются, редактируются, удаляются по официальным запросам Органов уровня государственного органа Новосибирской области, областного исполнительного органа государственной власти Новосибирской области; для территориальных органов областных исполнительных органов государственной власти Новосибирской области и для подведомственных им государственных учреждений учетные записи в СЭДД Правительства НСО создаются, редактируются, удаляются по официальному запросу вышестоящего им Органа.

СЭДД Правительства НСО подключен к системе межведомственного электронного документооборота федеральных органов исполнительной власти Российской Федерации (МЭДО).

Официальный сайт Губернатора Новосибирской области и Правительства Новосибирской области в сети Интернет (далее – Портал Правительства НСО), официальные сайты областных исполнительных органов государственной власти Новосибирской области в сети Интернет (далее – официальные сайты Органов), тематические сайты Правительства Новосибирской области размещены в ЦОД Правительства НСО, построены на базе программного обеспечения типового официального сайта исполнительного органа государственной власти Новосибирской области в сети Интернет (далее – типовой сайт) и опубликованы в пространстве доменных имён Правительства Новосибирской области (nso.ru и другие зарегистрированные доменные имена Правительства Новосибирской области).

Правительство Новосибирской области утверждает требования к Порталу Правительства НСО, официальным сайтам Органов и к тематическим сайтам Правительства Новосибирской области в сети Интернет[[11]](#footnote-11). Информационная структура Портала Правительства НСО и Органы, ответственные за подготовку и публикацию материалов, по каждому разделу Портала Правительства НСО утверждаются Правительством Новосибирской области[[12]](#footnote-12).

Уполномоченный орган обеспечивает функционирование и развитие Портала Правительства НСО, предоставляет Органам программное, информационное и методическое обеспечение типового сайта, обеспечивает функционирование технических средств типовых сайтов Органов; устанавливает требования к регламентам функционирования официальных сайтов Органов[[13]](#footnote-13).

По запросу государственных учреждений, органов местного самоуправления для создания официальных сайтов государственных учреждений, органов местного самоуправления в сети Интернет Уполномоченный орган может предоставлять программное, информационное и методическое обеспечение типового сайта, размещать указанные официальные сайты в ЦОД Правительства НСО и публиковать их в пространстве доменных имён Правительства Новосибирской области.

Информационное наполнение официальных сайтов Органов обеспечивается Органами. Для официальных сайтов Органов, созданных на основе типового официального сайта, права административного доступа сотрудникам Органа на официальный сайт Органа предоставляет Уполномоченный орган или подведомственное Уполномоченному органу учреждение по официальному запросу Органа; административный доступ возможен из сети Правительства НСО либо через сеть Интернет по защищенным каналам связи с использованием средств двухфакторной аутентификации.

В целях обеспечения поддержки и предоставления качественного обслуживания пользователей Правительства Новосибирской области в сфере информационных технологий внедрена Служба поддержки пользователей Правительства Новосибирской области, регламент функционирования которой утверждает Уполномоченный орган[[14]](#footnote-14). Портал Службы поддержки пользователей, предназначенный для создания заявок на получение технической поддержки, информирования о состоянии исполнения заявок, размещения методических и информационных материалов, является веб-интерфейсом. Авторизация пользователей на указанном Портале производится по учетной записи в сети Правительства НСО.

## Использование технологий беспроводного доступа

АРМ пользователей Органов подключаются к сети Правительства НСО с использованием технологии проводного доступа через предусмотренные для этих целей точки подключения (розетки).

С АРМ пользователей, подключенных к сети Правительства НСО с использованием технологии проводного доступа, запрещается одновременное подключение к сети Интернет и другим сетям информационного обмена по технологии беспроводной передачи данных по радиоканалам, в том числе с использованием WiFi-маршрутизаторов, модемов сотовой связи 3G, 4G или иных устройств.

В зданиях и помещениях, занимаемых Органами, за исключением выделенных помещений, разрешено использование сотовой связи с помощью личных или служебных устройств и подключение мобильных устройств к WiFi-сетям ограниченного доступа (далее – WiFi-сеть для централизованного выхода в сеть Интернет).

Требования к WiFi-сетям для централизованного выхода в сеть Интернет утверждаются Уполномоченным органом.

Для обеспечения потребностей посетителей мероприятий в зданиях Правительства Новосибирской области WiFi-сеть для централизованного выхода в сеть Интернет организуется Уполномоченным органом, подведомственными Уполномоченному органу учреждениями.

При необходимости использования собственной WiFi-сети Орган обязан согласовать ее создание и использование с Уполномоченным органом, предоставив в Уполномоченный орган подтверждение выполнения утвержденных требований в WiFi-сети для централизованного выхода в сеть Интернет, владельцем которой является Орган.

## Доступ внешних пользователей

Доступ граждан к информационным системам Органов и ГИС НСО общего доступа[[15]](#footnote-15) организуется Органом, являющимся оператором информационной системы, ГИС НСО, либо Уполномоченным органом, подведомственным Уполномоченному органу учреждением по заявке Органа, являющегося оператором информационной системы, ГИС НСО (в случае размещения информационной системы Органа, ГИС НСО в ЦОД Правительства НСО).

Доступ сотрудников органов местного самоуправления, подведомственных им муниципальных учреждений к информационным системам ограниченного доступа ГИС НСО, ГИР НСО, информационным системам Органов предоставляется на основании нормативных правовых актов Правительства Новосибирской области, Губернатора Новосибирской области[[16]](#footnote-16) либо по официальной заявке Органа, являющегося оператором ГИС НСО, информационной системы.

Доступ внешних пользователей – сотрудников, информационных систем организаций, с которыми Органы состоят в контрактных либо в договорных отношениях (далее – заинтересованные Органы), – к сети Правительства НСО, к инфраструктуре ГИС НСО, ГИР НСО, информационных систем Органов, размещенных в ЦОД Правительства НСО, может быть предоставлен в случае служебной необходимости (выполнение служебных обязанностей, исполнение государственных контрактов и т.п.).

Доступ внешних пользователей организуется Уполномоченным органом, подведомственными Уполномоченному органу учреждениями по официальной заявке заинтересованного Органа, в которой указываются следующие параметры доступа: цель предоставления доступа; кому предлагается предоставить доступ (для сотрудников организаций – ФИО, должности, телефоны; для информационных систем – наименование и владелец информационной системы); период предоставления доступа; информационная система или ресурс, к которым предлагается предоставить доступ; виды информации ограниченного доступа, конфиденциальность которой может быть нарушена при предоставлении доступа; технические параметры доступа; обоснование необходимости предоставления доступа.

Указанные заинтересованным Органом параметры доступа документируются в официальной заявке в соответствии с порядком, утверждаемым Уполномоченным органом[[17]](#footnote-17).

Заинтересованный Орган несёт ответственность за сведения, указанные в официальной заявке о предоставлении доступа, и за соблюдение конфиденциальности, целостности, доступности информации, к которой внешний пользователь получает доступ в соответствии с его заявкой.

Решение о предоставлении доступа к функционалу и данным ГИС НСО, ГИР НСО, информационной системы Органа и о параметрах доступа (уровне полномочий внешнего пользователя) принимает руководитель Органа, являющегося оператором соответствующей ГИС НСО, ГИР НСО, информационной системы Органа, исходя из положений действующего законодательства Российской Федерации.

## Обращение с носителями защищаемой информации

Должны обеспечиваться учет и надёжное хранение бумажных и машинных носителей защищаемой информации и их обращение, исключающее хищение, подмену и уничтожение. Ведение учета руководитель Органа поручает ответственному за организацию защиты информации в Органе либо иному сотруднику (сотрудникам) Органа.

Перед использованием съемные машинные носители защищаемой информации маркируются индивидуальным номером носителя и отметкой о категории информации, для которой будет носитель использоваться. На бумажный носитель защищаемой информации наносится служебная отметка о категории содержащейся информации.

Носители защищаемой информации подлежат учёту в Органе (подразделении Органа), обрабатывающем защищаемую информацию. В целях учета машинных носителей (магнитных, оптических дисков, карт памяти и пр.) защищаемой информации в Органе ведутся журналы учёта. Учёт бумажных носителей защищаемой информации ведётся в соответствующих журналах учёта, в картотеках либо описях. Указанные журналы учёта, картотеки, описи могут формироваться как в бумажном виде, так и в электронном.

Храниться носители защищаемой информации должны в местах, недоступных для посторонних лиц (в помещениях, замки которых оборудуются для опечатывания, в запираемых шкафах, сейфах). Для программно-аппаратных комплексов хранения ключевой информации, иных носителей ключевой информации используются опечатываемые колбы.

В Органе должен быть утверждён порядок учета, хранения и уничтожения носителей защищаемой информации, определяющий виды носителей защищаемой информации, способ их учета, ответственных за ведение учёта, места хранения, порядок уничтожения.

# Технические меры защиты информации

Технические меры защиты информации обеспечивают безопасность информации, подлежащей защите, с применением технических, программных и программно-технических средств защиты информации. Для обеспечения безопасности информации ограниченного доступа должны применяться средства защиты информации, прошедшие в установленном порядке процедуру оценки соответствия (сертификацию федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации).

## Антивирусная защита

Антивирусная защита должна обеспечивать обнаружение компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

Реализация антивирусной защиты должна удовлетворять следующим требованиям и предусматривать:

- применение средств антивирусной защиты на автоматизированных рабочих местах, серверах, средствах защиты информации уровня периметра (средствах межсетевого экранирования, прокси-серверах, почтовых шлюзах и других средствах защиты информации при наличии технической возможности), мобильных технических средствах и иных точках доступа в информационную систему, подверженных внедрению (заражению) вредоносными компьютерными программами (вирусами) через съемные машинные носители информации или сетевые подключения, в том числе к сетям общего пользования (вложения электронной почты, веб- и другие сетевые сервисы);

- установку, централизованное конфигурирование и управление средствами антивирусной защиты;

- предоставление доступа средствам антивирусной защиты к объектам информационной системы, которые должны быть подвергнуты проверке средством антивирусной защиты;

- проведение периодических проверок компонентов информационной системы (автоматизированных рабочих мест, серверов, других средств вычислительной техники) на наличие вредоносных компьютерных программ (вирусов);

- проверку в масштабе времени, близком к реальному, объектов (файлов) из внешних источников (съемных машинных носителей информации, сетевых подключений, в том числе к сетям общего пользования, и других внешних источников) при загрузке, открытии или исполнении таких файлов;

- оповещение администраторов безопасности в масштабе времени, близком к реальному, об обнаружении вредоносных компьютерных программ (вирусов);

- определение и выполнение действий по реагированию на обнаружение в информационной системе объектов, подвергшихся заражению вредоносными компьютерными программами (вирусами).

- обновление базы данных признаков вредоносных компьютерных программ (вирусов) средств антивирусной защиты информационных систем, имеющих подключение к сетям общего пользования, – не реже одного раза в сутки, информационных систем, не подключенных к сетям общего пользования, – не реже одного раза в месяц.

- обновление базы данных признаков вредоносных компьютерных программ (вирусов) должно предусматривать: получение из доверенных источников обновлений базы данных признаков вредоносных компьютерных программ (вирусов) контроль целостности перед применением.

Антивирусная защита ГИС НСО, ГИР НСО, информационных систем Органов, размещенных в ЦОД Правительства НСО, и АРМ пользователей, включенных в сеть Правительства НСО, обеспечивается посредством подключения к единой системе антивирусной защиты Правительства Новосибирской области, представляющей собой совокупность централизованно управляемых программных и программно-аппаратных средств обнаружения и предотвращения вредоносной программной активности уровня сети, серверов и конечных устройств (ЕСАЗ НСО). Эксплуатацию ЕСАЗ НСО и подключение к ней осуществляют Уполномоченный орган и подведомственные Уполномоченному органу учреждения совместно с Органами, являющимися операторами информационных систем, в соответствии с регламентом функционирования ЕСАЗ НСО, утверждаемым Уполномоченным органом.

Правила и процедуры антивирусной защиты ГИС НСО, ГИР НСО и информационных систем регламентируются типовым регламентом антивирусной защиты, утверждаемым Уполномоченным органом, и организационно-распорядительными документами Органов, созданными на основе указанного типового регламента.

## Защита от несанкционированного доступа

Для доступа пользователей к сети Правительства НСО, к ГИС НСО, ГИР НСО, к локальным компьютерным сетям Органов, к информационным системам Органов используются механизмы идентификации (присвоение пользователям уникального признака-идентификатора) и аутентификации (подтверждение подлинности, проверку принадлежности пользователю предъявленного им идентификатора) в виде ввода логина и пароля пользователя либо двухфакторной аутентификации (использование аппаратных средств идентификации и пароля). В соответствии с правами доступа, определенными Органом, пользователю создаются учетные записи, при этом пользователю присваивается уникальное имя (логин) и формируется индивидуальный или временный пароль.

Идентификация, аутентификация и авторизация пользователей в сети Правительства НСО, в локальных вычислительных сетях Органов проводится средствами операционной системы либо средствами защиты от несанкционированного доступа, если они установлены на АРМ пользователя; при этом должен быть обеспечен автоматизированный контроль правил генерации и смены паролей пользователей, а также принудительной периодической смены паролей и смены временного пароля при первой аутентификации.

Идентификация и аутентификация пользователей в ГИС НСО, в информационных системах Органов проводится в соответствующих информационных системах либо средствами федеральной государственной информационной системы «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме»[[18]](#footnote-18).

Программные средства защиты, установленные на АРМ пользователей, могут иметь сквозную авторизацию с операционной системой либо требовать отдельной идентификации и аутентификации пользователей.

Наименование сетевого узла (логин) и индивидуальный пароль пользователя в защищенной сети Правительства Новосибирской области и в защищенных сетях Органов первоначально создаются администратором защищенной сети, передаются пользователю при установке средств криптографической защиты информации на АРМ пользователя; индивидуальный пароль может быть изменен пользователем на сетевом узле защищенной сети.

Технологические пароли устанавливаются штатными специалистами Органов, осуществляющими техническую поддержку средств вычислительной техники объектов информатизации. Технологические пароли должны быть задокументированы; они могут быть неиндивидуальными, общими для групп устройств, если это разрешено распорядительными документами Органа. Пароли, предустановленные производителем, должны сменяться до начала эксплуатации средств вычислительной техники.

Общие требования к аутентификации в сети Правительства НСО, в локальных компьютерных сетях Органов, в ГИС НСО, в информационных системах Органов (ограничение неуспешных попыток аутентификации (ввода неправильного пароля) до автоматического блокирования учётной записи пользователя; продолжительность автоматического блокирования; блокирование открытого сеанса доступа пользователя после установленного времени бездействия (неактивности) пользователя или по его запросу; ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя; период изменения пароля; хранение истории предыдущих паролей пользователя и предотвращение их повторного использования; степень отличия нового пароля от хранимых в истории предыдущих паролей и т.д.) в зависимости от типа, категории, класса и уровня защищенности объекта информатизации регламентируются парольной политикой Правительства Новосибирской области, которую разрабатывает, утверждает и доводит до сведения Органов Уполномоченный орган.

Требования к сложности паролей при их создании и изменении (минимальная длина пароля, алфавит пароля, способ формирования пароля) в зависимости от типа, категории, класса и уровня защищенности объекта информатизации регламентируются парольной политикой Правительства Новосибирской области, которую разрабатывает, утверждает и доводит до сведения Органов Уполномоченный орган.

Для выбора качественного пароля, который легко запомнить, не подвержен легкому угадыванию или вычислению с использованием персональной информации, связанной с владельцем пароля, можно использовать парольные фразы – грамматически правильно построенные предложения, которые составлены из слов, несколько начальных букв которых составляют пароль либо значительную его часть. Запрещается записывать пароли, если только не обеспечено безопасное хранение записей; пароли в открытом виде не должны содержаться в компьютерных файлах.

При обнаружении фактов, указывающих на компрометацию (разглашение) пароля, изменение пароля обязательно.

Сотрудники Органов не должны использовать в сети Интернет пароли, повторяющие те, которыми они пользуются при исполнении служебных обязанностей; не должны использовать повторяющиеся пароли для доступа к разным информационным системам.

При создании учетной записи пользователя в сети Правительства НСО, в локальных компьютерных сетях Органов, в ГИС НСО, в информационных системах Органов формируется временный (с обязательным изменением при первой аутентификации пользователя) либо уникальный пароль, который доводится до сведения пользователя. Способы передачи паролей пользователю регламентируются парольной политикой Правительства Новосибирской области.  Пользователи должны подтверждать получение паролей. Смена пароля осуществляется пользователем лично в условиях конфиденциальности

Сотрудникам Органов запрещено предоставлять идентификационные данные другим сотрудникам или сторонним лицам. Сотрудники Органа несут ответственность за все действия в информационной системе, совершенные с использованием их учетных записей. В случае компрометации или утери пароля сотрудник обязан оповестить об этом ответственного за организацию защиты информации в Органе, в случае его отсутствия – сотрудников Службы инцидентов ИБ.

## Меры по ограничению программной среды

В целях ограничения программной среды на АРМ пользователей запрещается запуск программного обеспечения, не разрешенного к использованию, и исключена возможность самостоятельной установки пользователем дополнительного программного обеспечения. Установка программного обеспечения производится специалистами Службы поддержки пользователей.

Пользователи не должны иметь прав локальных администраторов АРМ пользователя, за исключением случаев, когда наличие прав локальных администраторов требуется для функционирования используемого программного обеспечения. Экспертиза о необходимости наличия прав локальных администраторов производится специалистами Службы поддержки пользователей.

## Резервное копирование

Резервное копирование ГИС НСО, ГИР НСО, информационных систем Органов, размещённых в ЦОД Правительства НСО на ресурсах (вычислительных мощностях), принадлежащих Уполномоченному органу или подведомственным Уполномоченному органу учреждениям, обеспечивает Уполномоченный орган, подведомственные Уполномоченному органу учреждения в соответствии с планами резервного копирования и восстановления, утверждаемыми руководителем Уполномоченного органа или руководителем подведомственного Уполномоченному органу учреждения для каждой информационной системы (группы информационных систем) на основании подготовленных Органами-операторами соответствующих ГИС НСО, информационных систем Органов планов резервного копирования. Резервные копии размещаются на отдельной от ЦОД Правительства НСО площадке. Восстановление информационной системы из резервной копии производится в соответствии с указанными выше регламентами по запросу Органа, являющегося оператором информационной системы.

Резервное копирование информационных систем и информационных ресурсов, размещенных вне ЦОД Правительства НСО либо размещенных в ЦОД Правительства НСО на ресурсах (вычислительных мощностях), принадлежащих Органам, обеспечивают Органы, являющиеся операторами информационных систем, на основании регламентов резервного копирования и восстановления, согласованных Уполномоченным органом и утвержденных соответствующими Органами. Периодичность проведения резервного копирования определяется исходя из особенностей ГИС НСО, ГИР НСО, информационных систем Органов, но не реже 1 раза в месяц.

Уполномоченный орган, подведомственные Уполномоченному органу учреждения обеспечивают резервное копирование настроек (конфигураций) сетевого и серверного оборудования, инфраструктуры сети Правительства и ЦОД Правительства, среды виртуализации, систем хранения данных, размещенных в ЦОД Правительства НСО.

## Обнаружение вторжений и межсетевое экранирование

Уполномоченный орган организует работу по обеспечению каналами связи, доступа к сети Интернет администрации Губернатора Новосибирской области и Правительства Новосибирской области и исполнительных органов государственной власти Новосибирской области. На базе ЦОД Правительства НСО создан отказоустойчивый мультипровайдерный центр с высокой пропускной способностью, который обеспечивает выход в сеть Интернет рабочих мест, подключенных к ГИСПД НСО. Уполномоченный орган, подведомственные Уполномоченному органу учреждения обеспечивают функционирование системы обнаружения вторжений, межсетевого экранирования на границе сети Правительства НСО с сетью Интернет, регулярное обновление баз решающих правил для системы обнаружения вторжений и для систем межсетевого экранирования.

Сеть Правительства НСО подключена к государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Уполномоченный орган обеспечивает подключение сети Правительства НСО к российскому государственному сегменту информационно-телекоммуникационной сети Интернет (RSNet).

Органы, имеющие независимые от сети Правительства НСО подключения к сети Интернет, обеспечивают обнаружение вторжений и межсетевое экранирование в соответствии с требованиями действующего законодательства самостоятельно, при этом состав средств защиты Органы согласовывают с Уполномоченным органом.

## Аттестация ГИС и ИСПДн

Комплекс мероприятий по созданию системы защиты информации, в результате которых подтверждается соответствие информационной системы требованиям стандартов или иных нормативно-технических документов по безопасности информации. Подтверждением такого соответствия является специальный документ – аттестат соответствия, срок его действия не может превышать 5 лет. По окончании срока действия аттестата соответствия, изменения класса защищенности информационной (уровня защищенности информации) системы необходимо проводить повторную аттестацию информационной системы. При изменении состава угроз безопасности информации или изменения проектных решений, реализованных при создании системы защиты информации информационной системы, проводятся дополнительные аттестационные испытания в рамках действующего аттестата соответствия.

Аттестацию на соответствие требованиям по защите информации имеют право проводить только организации-лицензиаты ФСТЭК России.

С целью своевременного выявления новых угроз безопасности информации и предотвращения утечки информации, Орган может проводить ежегодный контроль соответствия системы защиты информации требованиям безопасности информации с привлечением организаций-лицензиатов ФСТЭК России.

## Внутренняя телефонная сеть

Уполномоченный орган организует работу по обеспечению услугами фиксированной телефонной связи, внедрению IP-телефонии в администрации Губернатора Новосибирской области и Правительства Новосибирской области, исполнительных органах государственной власти Новосибирской области.

Справочник телефонных номеров сотрудников Органов ведет Уполномоченный орган или подведомственное Уполномоченному органу учреждение; сведения в указанный справочник заносятся при поступлении официальной заявки Органа о выделении телефонного номера сотруднику Органа или заявки в Службу технической поддержки при принятии или увольнении сотрудника Органа.

Защита речевой информации при использовании внутренней телефонной сети обеспечивается выделением отдельных подсетей в сети Правительства НСО.

# Инциденты информационной безопасности

Инцидент информационной безопасности (далее – инцидент ИБ) – это событие или группа событий, возникшие в результате нарушения установленных требований по защите информации, отказа технических средств, иной непредвиденной ситуации по информационной безопасности, которые приводят или могут привести к нарушению или прекращению функционирования сети Правительства НСО, локальных вычислительных сетей Органов, ГИС НСО, ГИР НСО, информационных систем Органов и (или) к возникновению угроз безопасности информации.

В целях выявления инцидентов ИБ и реагирования на них Уполномоченный орган определяет группу сотрудников подразделений Уполномоченного органа и подведомственных Уполномоченному органу учреждений как коллегиальный орган, ответственный за выявление инцидентов ИБ, сбор сведений о них, расследование причин и условий появления инцидентов ИБ, организацию ликвидации последствий инцидентов ИБ, разработку предложений по предупреждению возникновения инцидентов ИБ, направление сведений о произошедших инцидентах ИБ (далее – Служба инцидентов ИБ).

Деятельность Службы инцидентов ИБ по выявлению и устранению инцидентов ИБ регламентируется Уполномоченным органом. В целях выявления инцидентов ИБ используется оперативная информация, полученная в ходе текущего контроля и анализа защищенности, от сотрудников Органов, от территориальных органов федеральных органов исполнительной власти, из других источников, и сведения автоматизированного контроля и регистрации событий безопасности.

Сотрудники Уполномоченного органа, Органов обязаны своевременно сообщать в Службу инцидентов ИБ об известных им инцидентах ИБ. Порядок извещения Службы инцидентов ИБ, включая телефон, адрес электронной почты, утверждает и доводит до сведения Органов Уполномоченный орган.

Служба инцидентов ИБ представляет информацию о компьютерных инцидентах ИБ в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации в соответствии с нормативными правовыми актами Российской Федерации[[19]](#footnote-19).

# Контроль

В целях обеспечения безопасности информации и выполнения требований по защите информации в ходе эксплуатации объектов информатизации проводится контроль выполнения мер по защите информации. Контроль проводится в различных формах.

Уполномоченный орган проводит в Органах мероприятия по контролю в соответствии с ежегодно утверждаемыми заместителем Губернатора Новосибирской области планами:

- План мероприятий по контролю выполнения мер по защите информации содержащей сведения, составляющие государственную тайну, на объектах информатизации администрации Губернатора Новосибирской области и Правительства Новосибирской области и областных исполнительных органов государственной власти Новосибирской области;

- План мероприятий по контролю выполнения мер по защите информации не содержащей сведений, составляющих государственную тайну, на объектах информатизации администрации Губернатора Новосибирской области и Правительства Новосибирской области и областных исполнительных органов государственной власти Новосибирской области;

- План мероприятий по контролю устранения недостатков, выявленных в ходе проводимых Уполномоченным органом в предыдущем году проверок исполнительных органов государственной власти Новосибирской области, и реализации рекомендаций.

По результатам проведенного в Органе мероприятия по контролю Уполномоченным органом формируется акт проверки, экземпляр которого направляется в Орган. В случае выявления нарушений или недостатков Орган принимает меры по их устранению и сообщает о результатах в Уполномоченный орган.

Справка о результатах проведенных мероприятий по контролю, выявленные типовые нарушения и недостатки могут быть рассмотрены на заседании Коллегиального органа по информационной безопасности.

Периодический автоматизированный контроль проводит Уполномоченный орган, подведомственные Уполномоченному органу учреждения с использованием средств анализа защищённости, средств антивирусной защиты информации, иных программных и технических средств. Результатами автоматизированного контроля являются сведения о выявленных уязвимостях и ошибках конфигурирования операционных систем, служб, систем управления базами данных, прикладных систем и средств защиты информации, используемых в сети Правительства НСО и в ЦОД Правительства НСО, сведения об установке обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации, о работоспособности и правильности функционирования средств защиты информации, о соответствии стандартам и другие. По результатам автоматизированного контроля Уполномоченный орган, подведомственные Уполномоченному органу учреждения проводят мероприятия по повышению защищённости сети Правительства НСО, ГИС НСО и ГИР НСО. Результаты автоматизированного контроля могут быть рассмотрены на заседании Коллегиального органа по информационной безопасности.

В целях осуществления внутреннего контроля соблюдения положений организационно-распорядительных, инструктивных и методических документов по защите информации, правильности (соответствия технической документации на средства защиты информации) эксплуатации средств защиты информации. Органы проводят периодические внутренние проверки выполнения мероприятий по обеспечению защиты информации (далее – внутренние проверки). Внутренние проверки осуществляются ответственным за организацию защиты информации в Органе либо комиссией, образуемой руководителем Органа. Внутренние проверки проводятся в соответствии с регламентом внутренних проверок Органа, сформированным на основании типового регламента проведения внутренних проверок, утверждаемого Уполномоченным органом. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений и недостатков, руководителю Органа докладывает ответственный за организацию защиты информации в Органе либо председатель комиссии.

Уполномоченным органом, подведомственными Уполномоченному органу учреждениями, привлекаемыми Уполномоченным органом на договорной основе организациями-лицензиатами ФСТЭК России могут проводиться проверки на уязвимость ГИС НСО, ГИР НСО, сегментов сети Правительства НСО, информационных систем Органов.

Результаты проверки доводятся до сведения руководителя Уполномоченного органа и курирующего заместителя Губернатора Новосибирской области, а также до руководителей Органов в части, их касающейся. В случае необходимости выработки решения, принятия общей рекомендации результаты проведенной проверки рассматриваются на заседании Коллегиального органа по информационной безопасности. Уполномоченный орган, подведомственные Уполномоченному органу учреждения организуют проведение мероприятий по оперативному устранению вновь выявленных уязвимостей сети Правительства НСО, ГИС НСО и ГИР НСО, информационных систем Органов.

Надзорные органы (территориальные органы федеральных органов исполнительной власти, федеральные службы, уполномоченные в сфере защиты информации) осуществляют государственный контроль (надзор) в сфере защиты информации. Надзорными органами являются Федеральная служба по техническому и экспортному контролю, уполномоченная в области противодействия техническим разведкам и технической защиты информации, Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций, уполномоченная по защите прав субъектов персональных данных, Федеральная служба безопасности, осуществляющая обеспечение безопасности Российской Федерации.

Надзорные органы проводят проверки по вопросам защиты информации в соответствии с собственными планами.

По результатам проведения проверки Уполномоченный орган формирует план устранения нарушений и недостатков, выявленных в ходе проверки, и выполнения полученных рекомендаций. Указанный план согласуется с проверяющим надзорным органом, утверждается заместителем Губернатора Новосибирской области. Уполномоченный орган организует исполнение указанного плана и проводит регулярные отчеты в надзорный орган до полного исполнения плана.

# Обучение, инструктаж, повышение квалификации

Сотрудники Органа, непосредственно обрабатывающие информацию, содержащую сведения, составляющие государственную тайну, либо значимую конфиденциальную информацию (персональные данные высокого уровня защищенности и т.д.), должны регулярно повышать квалификацию в сфере защиты информации.

Руководители Органов, в которых обрабатывается информация, содержащая сведения, составляющие государственную тайну, и сотрудники Органов, обрабатывающие указанную информацию, повышают квалификацию по работе со сведениями, составляющими государственную тайну, в учебных заведениях, перечень которых утверждён Межведомственной комиссией по защите государственной тайны.

Руководители Органов организуют повышение квалификации в сфере защиты информации ответственных за организацию защиты информации в Органе (сотрудников подразделения по защите информации в Органе). Повышение квалификации указанных специалистов осуществляется с периодичностью, позволяющей специалистам в условиях нарастания количества угроз безопасности информации, а также с учетом необходимости постоянного совершенствования методов и средств их нейтрализации получать новые знания, умения и навыки, необходимые для профессиональной деятельности, но не реже чем каждые три года.

Ответственный за организацию защиты информации в Органе проводит периодический инструктаж сотрудников Органа, в который входит ознакомление с действующими нормативными правовыми актами и с организационно-распорядительными документами Органа по защите информации, объяснение правил и процедур, принятых в Органе для обеспечения безопасности информации, инструктаж по использованию средств защиты информации на АРМ пользователей, проверка знаний и понимания положений нормативных правовых и организационно-распорядительных документов сотрудниками Органа. Указанный инструктаж в обязательном порядке проводится с новыми сотрудниками Органа. По результатам проведения инструктажа сотрудник Органа расписывается в журнале проведения инструктажа сотрудников Органа.

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

1. Например, постановление Губернатора Новосибирской области от 19.08.2013 № 202 ДСП «Об обеспечении защиты информации, содержащей сведения, составляющие государственную тайну» [↑](#footnote-ref-1)
2. Совместный приказ Гостехкомиссии России и ФСБ России от 28.07.2001 № 309/405 «Об утверждении Положения о постоянно действующих технических комиссиях по защите государственной тайны» [↑](#footnote-ref-2)
3. Постановление Правительства Новосибирской области от 15.02.2017 № 51-п ДСП «Об определении актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, эксплуатируемых в администрации Губернатора Новосибирской области и Правительства Новосибирской области, исполнительных органах государственной власти Новосибирской области и подведомственных им учреждениях и организациях» [↑](#footnote-ref-3)
4. Закон Российской Федерации от 21.07.1993 № 5485-1 «О государственной тайне»;

   Постановление Правительства Российской Федерации от 06.02.2010 № 63 «Об утверждении инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне» [↑](#footnote-ref-4)
5. Приказ ДИиРТТ НСО от 03.03.2016 № 14-Д «Об утверждении условий подключения к государственной инфокоммуникационной сети передачи данных Новосибирской области» [↑](#footnote-ref-5)
6. Постановление Правительства Новосибирской области от 18.04.2017 № 142-п «Об утверждении Положения об управлении делами Губернатора Новосибирской области и Правительства Новосибирской области» [↑](#footnote-ref-6)
7. Постановление Губернатора Новосибирской области от 19.08.2013 № 202 ДСП «Об обеспечении защиты информации, содержащей сведения, составляющие государственную тайну»;

   Приказ администрации Губернатора Новосибирской области и Правительства Новосибирской области от 03.06.2016 № 20дсп «О назначении ответственных за обеспечение защиты информации» [↑](#footnote-ref-7)
8. Постановление Правительства Новосибирской области от 23.11.2016 № 385-п «О департаменте информатизации и развития телекоммуникационных технологий Новосибирской области»;

   Распоряжение Правительства Новосибирской области от 15.07.2013 № 313-рп «О создании государственного бюджетного учреждения «Центр информационных технологий Новосибирской области» [↑](#footnote-ref-8)
9. Распоряжение Губернатора Новосибирской области от 14.07.2014 № 124-р «О правилах ведения служебной электронной переписки»;

   приказ департамента информатизации и развития телекоммуникационных технологий Новосибирской области от 07.06.2016 № 76-Д «Об условиях использования в служебных целях сервисов обмена»;

   приказ департамента информатизации и развития телекоммуникационных технологий Новосибирской области от 09.06.2016 № 79-Д «О ведении перечня официальных средств ведения служебной переписки» [↑](#footnote-ref-9)
10. Постановление Губернатора Новосибирской области от 01.04.2013 № 73 «О признании электронных документов в системе электронного документооборота и делопроизводства в Правительстве Новосибирской области, подписанных простой электронной подписью, равнозначными документам на бумажных носителях, подписанным собственноручной подписью» [↑](#footnote-ref-10)
11. Постановление администрации Новосибирской области от 26.10.2009 № 398-па «Об утверждении требований к технологическим, программным и лингвистическим средствам обеспечения пользования официальными сайтами администрации Новосибирской области, областных исполнительных органов государственной власти Новосибирской области» [↑](#footnote-ref-11)
12. Распоряжение Правительства Новосибирской области от 25.03.2014 № 93-рп «О мерах по обеспечению функционирования официального сайта Губернатора Новосибирской области и Правительства Новосибирской области в информационно-телекоммуникационной сети Интернет» [↑](#footnote-ref-12)
13. Распоряжение Губернатора Новосибирской области от 31.03.2011 № 96-р «Об организации доступа к информации о деятельности исполнительных органов государственной власти Новосибирской области, размещаемой в сети Интернет» [↑](#footnote-ref-13)
14. приказ департамента информатизации и развития телекоммуникационных технологий Новосибирской области от 07.04.2014 № 55-Д «О вводе в эксплуатацию информационной системы «Служба поддержки пользователей Правительства Новосибирской области» [↑](#footnote-ref-14)
15. например, ГИС НСО «Электронная демократия Новосибирской области», официальные сайты областных исполнительных органов государственной власти [↑](#footnote-ref-15)
16. например, постановления Правительства Новосибирской области от 13.02.2013 № 54-п «О межведомственной автоматизированной информационной системе», от 05.06.2014 № 219-п «О государственной информационной системе Новосибирской области "Информационно-аналитический портал Новосибирской области», от 25.06.2014 № 244-п «О подсистемах "Электронный детский сад" и "Учет платных услуг" государственной информационной системы Новосибирской области "Межведомственная автоматизированная информационная система"», от 04.08.2014 № 313-п «О государственной информационной системе "Региональная геоинформационная система Новосибирской области"», от 05.03.2015 № 82-п «О государственной информационной системе Новосибирской области "Мониторинг хода реализации наказов избирателей депутатам Законодательного Собрания Новосибирской области"» и другие [↑](#footnote-ref-16)
17. приказ департамента информатизации и развития телекоммуникационных технологий Новосибирской области от 13.05.2016 № 60-Д «Об утверждении порядка документирования правил доступа к единой информационно-коммуникационной сети Правительства Новосибирской области» [↑](#footnote-ref-17)
18. Постановление Правительства РФ от 10.07.2013 № 584 «Об использовании федеральной государственной информационной системы "Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» [↑](#footnote-ref-18)
19. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [↑](#footnote-ref-19)