Для общего пользования

Методические указания по внедрению ОРД для организаций, обрабатывающих персональные данные в АИС «Навигатор»

Версия 1.1
Апрель 2021 года

Содержание

Список терминов и сокращений

АИС – Автоматизированная информационная система. Например, АИС «Навигатор».
ИБ – Информационная безопасность.
ИСПДн – Информационная система персональных данных. Т.е. информационная система, в которой обрабатываются персональные данные.
ОРД – Организационно-распорядительные документы. Приказы, перечни, инструкции и регламенты, которые должны быть приняты в Организации, которая обрабатывает персональные данные.
ПДн – Персональные данные.
СЗИ – Средства защиты информации.
СКЗИ – Средства криптографической защиты информации.
СМНИ – Съемные машинные носители. Например, карта памяти типа «флэшка».
ФСТЭК РФ – Федеральная служба по техническому и экспортному контролю. Организация, которая наряду с ФСБ РФ определяет и контролирует правила обработки персональных данных.

Введение

Что такое Организационно-распорядительные документы по работе с персональными данными, и для чего они нужны?

Согласно законодательству РФ, любая организация, ведущая обработку персональных данных граждан, автоматически попадает под категорию «Оператор персональных данных». Обрабатываемые персональные данные могут относиться к любым категориям лиц – это могут быть сотрудники организации, приглашённые педагоги, обучающиеся, их родители или любые другие граждане, с которыми организация имеет договорные отношения. Обработка персональных данных является очень серьезным и ответственным процессом, важнейшим её условием является безопасность. Поэтому законодательством РФ выработаны строгие и вполне определённые требования к обработке персональных данных; этим требованиям должен строго следовать каждый оператор персональных данных. Законодательство РФ обязывает каждую организацию-оператора персональных данных составить и принять комплект организационно-распорядительных документов (ОРД), регламентирующих общие для всех сотрудников правила обработки персональных данных внутри Организации. К составу, содержанию и порядку оформления этих документов предъявляются строгие требования. Если Организация начинает обрабатывать какие-то новые персональные данные или начинает обрабатывать их каким-то иным образом (например, не в бумажном виде, а в информационной системе), в ОРД обязательно должны быть внесены изменения.

Подводя итог, сделаем вывод, что ответственность по заполнению организационно-распорядительных документов возникает у Организации НЕ с началом работы в АИС «Навигатор» или с момента аттестации «Навигатора», а с момента начала обработки любых персональных данных – т.е. фактически с момента начала работы Организации.

Почему образцовый комплект ОРД касается не только «Навигатора», а всех видов обработки персональных в Организации?

Разделение ОРД на документы «только для АИС “Навигатор”» и документы «только для остальных работ с ПДн» невозможно из-за того, что по законодательству комплект ОРД является единым и неделимым – в силу своего структурного построения и правил заполнения.

Направленный вам комплект ОРД включает только один документ, однозначно связанный только с АИС «Навигатор» – Акт определения уровня защищённости (п. 1.1.). В остальном же комплект ОРД является образцовым, не связанным с одной только АИС «Навигатор». Таким образом, комплект, кроме прочего, решает более широкую консультативную задачу, разъясняет все особенности учёта и регламентирования работ с любыми персональными данными (ПДн) в организации.

Отметим также, что указание в ОРД требований к операциям (а не самих операций) с ПДн, которые в организации на данный конкретный момент не осуществляются, не противоречит нормам законодательства РФ. К примеру, в Организации могут быть определены требования к резервному копированию информации баз данных с ПДн при том, что такие базы в Организации отсутствуют. Если в какой-то момент они появятся в Организации (например, в связи с установкой новой ИСПДн), вносить специальные изменения в данную конкретную часть ОРД уже не потребуется.

Предварительный итог

По изложенным выше причинам, Организации, которая начала эксплуатацию АИС «Навигатор», не требуется принимать с дословной точностью все присланные образцы организационно-распорядительных документов – чаще всего требуется внести изменения в уже принятые документы. Если какие-то ОРД из образцового комплекта в Организации полностью отсутствуют, они, безусловно, должны быть приняты – однако при этом дополнены или скорректированы в соответствии с реалиями функционирования Организации.

Ниже приводятся краткие разъяснительные комментарии по каждому документу из образцового комплекта ОРД. Также отметим, что дополнительные комментарии можно найти в самих doc-файлах образцовых ОРД.

В **Приложении 1** этого документа вы найдете ответы на часто задаваемые вопросы, связанные с ОРД, а в **Приложении 2** – чёткие ссылки на нормы законодательства РФ, в соответствии с которыми эти документы должны быть утверждены и оформлены.

Методические указания

1. Приказ о создании комиссии

Комиссия выполняет работы и принимает решения, связанные с обработкой ПДн в Организации. Обязанности комиссии и нормативные акты, которыми она должна руководствоваться в своей работе, перечислены в Приказе. Председателем комиссии является сотрудник Организации, назначенный Ответственным за обработку ПДн. Членами комиссии должны выступать сотрудники, допущенные к работе с ПДн «Навигатора». Минимальный состав комиссии - 1 председатель, 1 член комиссии.

1.1. Акт определения уровня защищённости

Акт утверждается комиссией (см. п.1). Методика определения уровня защищенности стандартизована – он определяется однозначно на основании категорий ПДн, обрабатываемых в «Навигаторе» и актуальных угроз. Указанные в образцовом акте категории ПДн, актуальные угрозы и выведенный на их основе уровень защищенности, определен при помощи экспертов организации, которая проводила аттестацию АИС «Навигатор», по результатам изучения особенностей этой АИС. По этой причине настоятельно рекомендуется в утверждаемом Организацией акте сохранять данные, указанные в образцовом документе.

1.2. Акт определения потенциального вреда

Данный акт касается всех персональных данных, которые обрабатывает организация. Акт утверждается комиссией (см. п.1). В настоящее время строго утверждённой методики определения потенциального вреда не существует, поэтому указанный в образцовом документе уровень потенциального вреда предложен экспертами аттестующей организации. Организация может выбрать и указать в данном документе иной уровень потенциального вреда, это не повлечёт за собой изменения в других документах.

2. Приказ о назначении ответственных

Аттестующая организация крайне не рекомендует совмещение одним сотрудником должности Ответственного за организацию обработки ПДн и Ответственного за обеспечение безопасности ПДн. Это условие не содержится в НПА законодательства РФ, но неоднократно озвучивалось контролирующими органами-регуляторами на специализированных конференциях. Ответственный за организацию обработки ПДн – в большей степени административный сотрудник, знакомый с нормами законодательства по ПДн, а ответственный за обеспечение безопасности – сотрудник технического профиля.

3. Перечень ПДн ИСПДн и допущенных

Перечень ПДн, обрабатываемых в организации

Поскольку Перечень является универсальным по всей организации, в нём должны фиксироваться все ПДн, обрабатываемые в организации, а не только ПДн, обрабатываемые в АИС «Навигатор». В качестве примера в перечень включены

персональные данные сотрудников, обрабатываемые бухгалтерией и отделом кадров. Организация, безусловно, может и должна редактировать эти данные в соответствии со своими реалиями. Предполагается, что подобный перечень уже имеется среди ОРД, утверждённых в организации, он просто должен быть дополнен за счет данных по АИС «Навигатор». В отличие от упомянутых выше образцовых данных, состав ПДн, обрабатываемых в АИС «Навигатор», указанный в Перечне, чётко соответствует действительности и должен быть внесён в документы Организации именно в таком виде.

Аналогичная логика касается и **Перечня ИСПдн Организации**. Если в Организации уже используются какие-либо ИСПДн, они уже должны быть зафиксированы и утверждены в виде аналогичного списка. Перечень должен быть дополнен за счет информации об АИС «Навигатор». Приведенная информация об этой АИС, указанная в образцовом Перечне, является верной и должна быть внесена в документы Организации именно в таком виде.

В **Перечне должностей сотрудников, допущенных к обработке ПДн**, должны быть перечислены все должности, имеющие доступ хотя бы к какой-либо из категорий ПДн (не только к категориям, указанным в образцовом Перечне). Допустимо вместо перечня должностей указать в документе перечень конкретных сотрудников – однако изменения в этом перечне также должны фиксироваться внутренними актами.

Отметим, что в обработка ПДн в АИС «Навигатор» является автоматизированной. Организация имеет право распечатывать ПДн из АИС «Навигатор» или другим способом переносить их на бумажные носители сугубо для служебного, внутреннего использования, однако такой (неавтоматизированный) вид обработки обязательно должен быть соответствующим образом быть зафиксирован в ОРД. При обработке ПДн на бумажных носителях во всех случаях должны соблюдаться все требования законодательства РФ к обработке персональных данных.

В листе ознакомления к данному документу должны расписаться все сотрудники Организации, допущенные к работе с ПДн.

4. Приказ об организации режима безопасности помещений

Приказ утверждает Перечень помещений, в которых ведётся обработка ПДн. Необходимо перечислить все эти помещения, указать режим прохода в здание, где ведется обработка ПДн, указать все меры защиты, которые принимаются (ЧОП, камеры наблюдения, пропускной режим, кодовые замки и т.д.).

Организация доступа в помещения

Этот раздел необходимо скорректировать в соответствии с режимом доступа в помещения Организации. Если организованы журналы получения-сдачи ключей, установлены временные рамки доступа в помещения и проч., эта информация должна быть отражена в документе.

В листе ознакомления к данному документу должны расписаться все сотрудники Организации.

5. Приказ об утверждении инструкций по защите ПДн

Инструкция пользователя информационных систем персональных данных

Инструкция является общей для всех ИСПДн, которые используются в Организации, и определяет универсальные правила эксплуатации всех ИСПДн. Многие пункты этой инструкции применяются в тех случаях, в которых они могут быть применимы.

Инструкция содержит пункт, касающийся организации работы со съемными машинными носителями (СМНИ). АИС «Навигатор» работает через веб-интерфейс и, следовательно, может функционировать без СМНИ, однако на СМНИ могут сохраняться отчеты или любые другие данные, выгруженные или другим образом скопированные из АИС «Навигатор». В случае если организация работает со СМНИ, данный пункт обязательно случае должен присутствовать в Инструкции.

Инструкция пользователя информационных систем персональных данных

Инструкция включает указание необходимости передачи ПДн по каналам связи с обязательным применением средств криптографической защиты. Криптографическая защита информации в АИС «Навигатор» является встроенной, она реализована посредством криптографического протокола TLS, с использованием которого осуществляется передача всех данных АИС «Навигатор» по внешним каналам связи. Этот протокол выступает в качестве средства шифрования при передаче ПДн АИС «Навигатор» по сетям общего доступа.

Требования по установке программных обновлений являются универсальными для всех видов п/о, используемых в Организации.

Инструкция по антивирусной защите

В дополнение к образцовой инструкции напоминаем, что антивирусные средства, используемые на рабочих местах АИС «Навигатор», должны быть не только лицензионными, но и сертифицированными. Информация об этом содержится в документах «Перечень мер для РМЦ» и «Перечень мер для региональных организаций». В списке объектов антивирусного контроля перечислены все типы объектов, которые, в соответствии с требованиями законодательства РФ, должны проверяться на отсутствие вирусов посредством антивирусных программ. Перечень является универсальным, и если какой-то тип объектов отсутствует в организации, это не означает, что присутствие этого типа в утверждённом списке объектов антивирусной защиты Организации является нарушением законодательства. Если Организация считает это необходимым, она может удалить отсутствующие типы объектов из перечня. Периодичность антивирусных проверок может быть реализована на усмотрение Организации.

Инструкция по организации резервирования и восстановления

Упомянутое в данном документе резервное копирование и восстановление работоспособности касается **всех** технических средств и программного обеспечения, баз данных и средств защиты информации в тех ИСПДн, обслуживание которых находится в ведении Организации. АИС «Навигатор» не входит в их число - резервное копирование данных АИС «Навигатор» осуществляется на стороне компании-разработчика АИС. В общем случае, наличие в организации внутренних требований по такому копированию помогает снять лишние вопросы контролирующих и, кроме того, не противоречит требованиям законодательства РФ.

Требования к резервированию в ИСПДн определены в Приказе ФСТЭК №21, а также детализированы в методических рекомендациях ФСТЭК. При подготовке ОРД эти требования могут и очень часто формулируются как универсальные для всех операций данного рода, проводимых в организации. Если в организации производится резервирование ПДн, к примеру, из базы данных программ семейства «1С» или базы данных отдела кадров, это резервирование также должно отвечать общим требованиям, указанным в ОРД. В случае если на момент утверждения в ОРД в организации не осуществляется резервное копирование, наличие требований к такому копированию не нарушает нормы законодательства РФ.

Пункт, касающийся архивного копирования резервируемой информации, является рекомендованным. Для этих целей организация может использовать специализированные средства копирования или осуществлять копирование иным выбранным способом. Желательно зафиксировать этот способ в ОРД.

Периодичность резервного копирования открытой информации может быть выбрана Организацией на своё усмотрение – в образцовом документе указана рекомендованная периодичность. Открытая информация – это информация, зафиксированная и документированная любым способом на любой носитель информации и не являющаяся при этом конфиденциальной информацией. Организации могут осуществлять резервное копирование открытой информации для разнообразных целей, например, для сохранения целостности данных. Это распространённая процедура, поэтому её документирование в ОРД может помочь организациям регламентировать её, дисциплинировать работу с данными, снизить риск потери ценной информации. Периодичность резервирования может быть определена организацией на своё усмотрение, указанная периодичность является рекомендованной – как и сама процедура, указанная в образцовом комплекте ОРД.

5.1. Журнал учёта съемных машинных носителей

В образцовом документе показан пример заполнения журнала.

В листе ознакомления к данному документу должны расписаться все сотрудники Организации.

6. Инструкция по обращению с СКЗИ

Документы, связанные с СКЗИ, могут отсутствовать в комплекте ОРД, если в организации не используются средства криптографической защиты (СКЗИ). Если в Организации используются СКЗИ (для работы с АИС «Навигатор» или для любых других целей), такие документы в обязательном порядке должны быть утверждены.

В листе ознакомления к данному документу должны расписаться все сотрудники Организации, использующие СКЗИ.

7. Регламент реагирования на инциденты ИБ

Согласно законодательству, Организация должна сама определить (и зафиксировать во внутреннем нормативном акте), какие события относятся инцидентам безопасности. Список может быть расширен, однако некоторые виды инцидентов из образцового документа должны фиксироваться обязательно – это требование законодательства.

Порядок регистрации событий информационной безопасности

Пункты 4, 5, 6 (Реагирование на сбои, Мониторинг результатов, Генерирование временных меток) являются рекомендованными, но не обязательными. Аналогичным образом, пункты этого документа, которые далее детализируют данные действия, тоже являются рекомендованными.

Основные этапы процесса реагирования на инциденты

Данный раздел определяет *необходимость* определения, является ли произошедшее событие инцидентом, или нет. Далее указывается *возможность* использования для этой цели специализированных средств. Упомянутыми в документе лицами, занимающимся реагированием на инциденты, являются ответственный за обеспечение безопасности информационной системы, администратор информационной системы.

В листе ознакомления к данному документу должны расписаться сотрудники Организации, осуществляющие защиту ПДн.

8. Положение о разрешительной системе доступа

Согласно законодательству РФ, юридическое утверждение (приказами) в Организации должностей Администратора (информационной системы) и Администратора безопасности не является обязательным. Допускается объединить описанные в документе уровни доступа в рамках одной роли «Администратор».

В листе ознакомления к данному документу должны расписаться все сотрудники Организации.

9. Положение о неавтоматизированной обработке ПДн

Как уже было указано выше, обработка персональных данных в АИС «Навигатор» является полностью автоматизированной. Но если в Организации происходит любая неавтоматизированная персональных данных, т.е. персональных данных на бумажных носителях (например, при приёме новых сотрудников на работу), то данное Положение в обязательном порядке должно быть утверждено.

В листе ознакомления к данному документу должны расписаться все сотрудники Организации, производящие неавтоматизированную обработку ПДн.

10. Регламент проведения внутреннего контроля соответствия обработки ПДн

В предыдущих документах мы определили требования к обработке ПДн и эксплуатации ИСПДн, однако выполнение этих требований безусловно должно проверяться, а результаты проверок – фиксироваться. Не получают ли доступ к ИСПДн сотрудники, которым не положено иметь такого доступа? Работают ли антивирусные программы на рабочих местах пользователя? Защищен ли доступ на компьютер паролем? Не хранятся ли в общем доступе флэшки с перс.данными? Выявленные нарушения фиксируются в журнале. Проверку обязательно проводит, как минимум, Ответственный за организацию обработки ПДн. Проверяется всё, что связано с обработкой ПДн в организации, а не только работа в ИСПДн.

Ответственность за организацию данного вида контроля несет сотрудник, назначенный Ответственным за организацию обработки ПДн.

Порядок проведения внутреннего контроля, приведенный в образцовом комплекте, включает в себя выявление уязвимостей в ИСПДн с использованием специализированных средств инструментального анализа защищенности (САЗ). том числе и сертифицированных. Для определяемого в организациях-пользователях АИС «Навигатор» уровня защищенности 4 использование сертифицированных средств анализа защищенности (САЗ) является рекомендованным. Использование дополнительных мер анализа защищенности поможет повысить уровень безопасности персональных данных. Для этих целей, в частности, можно использовать бесплатную программу ScanOVAL с сайта ФСТЭК.

В листе ознакомления к данному документу должны расписаться сотрудники Организации, осуществляющие защиту ПДн.

11. Положение об обеспечении безопасности ПДн

Этот документ, по сути, сводит воедино тот комплект, который мы разбирали до этого: назначение ответственных, реагирование на инциденты, определение уровня защищенности, разграничение доступа, доступ в помещения, резервирование, парольную защиту, а также использование СКЗИ если они используются. Поскольку Положение обеспечивает цельность остального комплекта документации, оно должно ему соответствовать. К примеру, если организация не использует СКЗИ, соответствующий раздел должен быть исключен из Положения.

Оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию СЗПДн обеспечивается силами специалистов Организации.

Указанная в документе организация резервирования и восстановления работоспособности программного обеспечения, баз данных ПДн и средств защиты информации (СЗИ), относится к любым объектам, находящимся в собственности и ведении Организации. Законодательство РФ не предъявляет требований к данным процедурам, их порядок определяется на усмотрение Организации и фиксируется в соответствующей инструкции. Аналогичное правило касается и организации обновления программного обеспечения и СЗИ.

Указанная в документе установка и настройка СЗИ в ИСПДн касается всех ИСПДн, эксплуатация которых требует такой установки. Примером для АИС «Навигатор» является установка антивирусного программного обеспечения.

Основные мероприятия по обеспечению безопасности персональных данных

В случае, если в организации (для любых целей) используются СКЗИ, их использование также может быть указано и описано в документе, как одно из мероприятий по обеспечению безопасности персональных данных. Если СКЗИ в организации не применяются, соответствующие пункты могут быть исключены из документа.

В листе ознакомления к данному документу должны расписаться сотрудники Организации, осуществляющие защиту ПДн.

12. Положение об организации обработки ПДн

Положение определяет цели, с которыми обрабатываются разные категории ПДн в организации, конкретный состав этих ПДн и определяет порядок этой

обработки. Поэтому разделы Положения и их наполнение должно быть полностью приведены в соответствие с реалиями организации. Важно, чтобы все виды и случаи обработки ПДн были описаны по примеру в образцовом документе.

Перечень нормативных актов, в соответствии с которыми производится обработка ПДн, определяется самой организацией. В случае образовательных организаций, которые обрабатывают ПДн в АИС «Навигатор», такая обработка должна происходить в соответствии и во исполнение Федерального закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации».

Условия и порядок обработки персональных данных работников.

Цели обработки персональных данных работников должны быть скорректированы в соответствии с целями такой обработки в организации.

В АИС «Навигатор» реализуются все перечисленные в образцовом документе действия по работе с ПДн: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Приведенная для примера информация по обработке биометрических данных и трансграничной передаче данных должна быть при необходимости отредактирована в соответствии с реалиями Организации.

Условия и порядок обработки персональных данных кандидатов; физ. лиц, работающих на основании ГПД и пользователей сайта

Разделы, касающиеся условий и порядка обработки ПДн кандидатов на замещение вакантных должностей и физических лиц, работающих на основании гражданско-правовых договоров, и пользователей сайта (сайтов) Организации, не касаются непосредственно работы в АИС «Навигатор» и данном документе присутствуют для примера, поскольку утверждаемое Положение носит универсальный характер и должно касаться всех видов обработки ПДн в Организации.

Условия и порядок обработки персональных данных детей и родителей

В образцовом документе предполагается, что обработка ПДн детей и родителей производится Организацией как с использованием АИС «Навигатор», так и без использования этой АИС. Для регистрации на АИС «Навигатор» родитель в обязательном порядке должен в электронном виде выразить согласие (т.е. поставить отметку «Согласен») с Правилами сайта и политикой конфиденциальности. Данный документ доступен для свободного изучения на сайте «Навигатора» и в качестве одного из пунктов включает в себя согласие на обработку ПДн, учитывающее все особенности и правила обработки ПДн в АИС «Навигатор». В случае, если родитель передаёт Организации свои ПДн и ПДн своего ребёнка для обработки без использования АИС «Навигатор» или без использования другой АИС, включающей аналогичный функционал дачи согласия, он должен в обязательном порядке подписать согласие на обработку ПДн, аналогичное тому, которое включено в виде образца в комплект ОРД.

В листе ознакомления к данному документу должны расписаться все сотрудники Организации.

Приложение 1: ЧаВо (часто задаваемые вопросы) по организационным вопросам внедрения ОРД и защите ПДн

1. **Вопрос:** Кто должен подавать в Роскомнадзор Уведомление об обработке ПДн?
   Ответ: Каждая организация региона, использующая АИС «Навигатор».

2. **Вопрос:** В штате организации нет сотрудника, который занимается информационно-технической поддержкой (т.к. данная должность не предусмотрена в этой организации). Руководитель данной организации не понимает, как правильно поступить в данном случае и какого человека назначить ответственным за обеспечение безопасности персональных данных, а какого человека назначить администратором ? Он должен выбирать сам? Или просить руководство о вводе дополнительно штатной единицы? Может ли один человек быть и ответственным за обеспечение безопасности персональных данных и администратором?
   Ответ: Да, допускается назначение одного сотрудника ответственным за обеспечение безопасности ПДн и администратором системы. Обычно это сотрудник технического профиля, например, системный администратор. Ответственный за организацию обработки ПДн должен быть другим лицом – это скорее административный сотрудник, знакомый со всеми нормами законодательства о безопасности ПДн.

3. **Вопрос:** Если организации можно оставить ведение сопроводительной документации в бумажном виде, то, как мы понимаем, ей не нужно заполнять журнал учета мест хранения носителей персональных данных? И другие документы, касающиеся электронных носителей (например, журнал учета съемных машинных носителей персональных данных).
   Ответ: Если в организации для хранения ПДн не используются электронные носители, то указывать их в документации не нужно.

4. **Вопрос**: Могут ли входить в состав комиссии те же сотрудники организации, кто и будет работать в Навигаторе? Или членами комиссии должны быть иные сотрудники, кто не будет осуществлять работу в Навигаторе?
   Ответ: Да, к участию в комиссии допускаются сотрудники, работающие в Навигаторе, а также любые сотрудники, обрабатывающие ПДн.

5. **Вопрос**: Можно ли убрать какие-либо пункты их функциональных обязанностей ответственных и администратора?
   Ответ: Нет, эти обязанности прописаны в законодательстве РФ.

6. **Вопрос**: Обязательны ли сведения о бывших работниках и о ближайших родственниках?
   Ответ: В данной таблице четко фиксированными являются только данные, связанные с Навигатором. Все остальные данные организация заполняет, исходя из своих реалий.

7. **Вопрос**: Обязателен ли пропускной режим в здании, где ведется Обработка ПДн, или достаточно просто ведения журнала учета посещаемости работниками организации?
   Ответ: Согласно Приказу 21 ФСТЭК в случае эксплуатации ИСПДн обязательно должна обеспечиваться следующая мера: «Контроль и управление физическим

доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены».
Очевидно, что один только журнал посещаемости такую меру не обеспечивает, т.к. позволяет любому постороннему лицу получить доступ в помещения, где ведется обработка персональных данных.

8. **Вопрос**: Положение об организации обработке ПДн: Из Согласия на обработку – обязаны ли родители предоставлять паспортные данные?
Ответ: Согласно законодательству РФ, обработка любых ПДн не допустима без согласия субъекта этих ПДн. Согласие родителя на обработку ПДн необходимо для работы в Навигаторе. Родитель выражает своё согласие на обработку ПДн, ставя галочку при напротив пункта «Я ознакомлен и выражаю согласие с политикой конфиденциальности и пользовательским соглашением». Согласие на обработку ПДн является частью пользовательского соглашения, а перечень обрабатываемых ПДн перечислен в политике конфиденциальности. Однако, обращаем ваше внимание, что любой сотрудник, данные которого обрабатываются в Навигаторе, должен предварительно заполнить Согласие на обработку ПДн, оно дано в приложении к документу 11 («Положение об организации обработки ПДн»), кроме того, любой сотрудник, получающий доступ в админскую часть Навигатора должен также заполнить Обязательство о неразглашении, оно находится в приложении к тому же документу.

9. **Вопрос**: «Персональные данные работников Оператора и бывших работников Оператора обрабатываются в целях: - ведения кадрового, бухгалтерского и воинского учета; - обеспечения пропускного режима, сохранности имущества Оператора, обеспечение личной безопасности; - исполнения Оператором функции работодателя, оформления трудовых отношений и обеспечения установленных законодательством Российской Федерации условий труда; - осуществление видов деятельности, предусмотренных Уставом». Обязательно ли указывать эти цели?
Ответ: Организация редактирует эти данные, исходя из своих реалий.

10. **Вопрос**: Раздел «Условия и порядок обработки персональных данных работников». «Персональные данные работников Оператора и бывших работников Оператора обрабатываются в целях:ведения кадрового, бухгалтерского и воинского учета; обеспечения пропускного режима, сохранности имущества Оператора, обеспечение личной безопасности;исполнения Оператором функции работодателя, оформления трудовых отношений и обеспечения установленных законодательством Российской Федерации условий труда; осуществление видов деятельности, предусмотренных Уставом». Обязательно ли указывать все эти цели?
Ответ: Организация редактирует эти данные, исходя из своих реалий.

11. **Вопрос**: Раздел «Условия и порядок обработки персональных данных кандидатов на замещение вакантных должностей» – обязательно ли включать этот раздел? Что выбрать?

«Основанием обработки персональных данных пользователей Сайта является согласие на обработку персональных данных. Пользователи Сайта дают свое согласие на обработку своих персональных данных в следующих случаях: - при регистрации на Сайте в личном кабинете;- при авторизации через социальные сети;- при заполнении формы обратной связи / заказе обратного звонка на Сайте; - при оформлении подписки на рассылку; - при отправке отзывов; - при отправке резюме».
Ответ: В случае АИС «Навигатора» – первый вариант из списка (регистрация в личном кабинете). В остальных случаях – исходя из реалий организации.

12. **Вопрос**: С кем его заключать гражданско-правовой договор? С кем заключать договор на оказание услуг? Обязательно ли?
Ответ: Данные договоры указываются при необходимости, в случае, если они заключаются в организации.

13. **Вопрос**: Является ли ИСПДн собственная база данных организации, в которой хранятся персональные данные? А набор файлов Word, в которых хранятся такие данные?
Ответ: Согласно п.10 ст.3 ФЗ от 27.07.2006 N 152-ФЗ «О персональных данных»: информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств. По этой формулировке собственная база данных организации, если она работает вместе с системой управления базой данных (т.е., техническим средством) является ИСПДн, а набор файлов Word – не является.

14. **Вопрос**: Если в организации используется несколько ИСПДн, обязательно ли для каждой из них назначать отдельного сотрудника администратором ИСПДН?
Ответ: Согласно законодательству РФ, юридическое утверждение (приказами) в Организации должностей Администратора (информационной системы) и Администратора безопасности не является обязательным. Допускается объединить описанные в документе уровни доступа в рамках одной роли «Администратор». Аналогичным образом законодательство не запрещает совмещение одним сотрудником обязанностей по администрированию сразу нескольких ИСПДн.

15. **Вопрос:** В образце документа «Положение об организации обработки ПДн» содержится пункт: «Срок хранения персональных данных работников Оператора и бывших работников Оператора в электронной форме и на бумажных носителях составляет 5 лет после расторжения трудового договора». Чем обусловлен данный срок?
Ответ: Организация может выставить и, соответственно, реализовывать срок на своё усмотрение.

16. **Вопрос:** Можно ли работать в АИС «Навигатор» при отсутствии аттестованных рабочих мест?
Ответ: В случае, если АИС «Навигатор» официально не придан статус ГИС, она имеет статус простой ИСПДн, и требования к безопасности обработки персональных данных в нём определяются Приказом 21 ФСТЭК от 18.02.2013. Согласно п. 6 данного Приказа, оценка эффективности реализованных мер защиты может проводиться оператором самостоятельно. Это значит, что

официальная аттестация компанией-лицензиатом ФСТЭК рабочих мест «Навигатора» не является обязательной.

17. **Вопрос:** Нужен брандмауэр или другой вид сетевого экрана, как его установить?
Ответ: Брандмауэр входит в состав стандартного функционала ОС Windows. При желании брандмауэр (межсетевой экран) можно приобрести в качестве отдельного программного или аппаратного средства защиты. На рынке представлены решения разного уровня. В случае АИС «Навигатор», не имеющей статуса ГИС, специальных требований к этим средствам не выдвигается.

18. **Вопрос:** Мы работаем в АИС «Навигатор» с 2018 года и не подавали уведомление в Роскомнадзор! Что же нам теперь делать?!
Ответ: Подать уведомление в Роскомнадзор. Запоздалая подача не повлечет за собой санкций. А вот отсутствие организации-пользователя АИС «Навигатор» в реестре операторов персональных данных – вполне может.

19. **Вопрос:** Вопрос касается документа «Положение об организации обработки ПДн». Как должны соотноситься срок или условие уничтожения ПДн (пункт 7.8) с описанием порядка уничтожения ПДн, приведенного в пункт 13.1 («Оператор прекращает обработку персональных данных и уничтожает носители персональных данных и удаляет их из информационных систем персональных данных в случаях: - достижения целей обработки персональных данных или максимальных сроков хранения – в течение 30 дней»)?
Ответ: Пункт 7.8 устанавливает, по сути, условие, после которого данные прекращают обрабатываться. Пункт 13.1 устанавливает срок, в течение которого после наступления условия данные прекращают обрабатываться. В «Навигаторе» не предусмотрено массовое/автоматическое уничтожение ПДн, но компания «Государство Детей» всегда уничтожает ПДн конкретного субъекта по его запросу. Поэтому мы считаем, что если в п. 7.8 условием уничтожения указать «По запросу от родителя», а в п. 13.1 оставить без изменений, то это не войдет в противоречие ни с законом, ни с реалиями «Навигатора».

20. **Вопрос:** Можно ли производить обработку персональных данных, работая в АИС «Навигатор» из дома?
Ответ: Установленные законом требования к обработке персональных данных в информационных системах включают в себя технические, физические и организационные меры. Технические меры включают в себя программные и аппаратные средства защиты – антивирусы, брандмауэры, средства блокировки компьютера и проч. Физические меры обычно реализуются с использованием постов охраны, камер наблюдения, физического ограничения доступа в помещения, где обрабатываются персональные данные. Организационные меры касаются внутреннего режима в помещениях. Технические меры в принципе возможно организовать на любом рабочем месте. Однако мы затрудняемся ответить, каким образом физические и организационные меры могут быть организованы в домашних условиях, особенно если в том же помещении проживают домочадцы, не имеющие доступа к ПДн.

Приложение 2: Перечень документов, регламентирующих порядок защиты информации ограниченного доступа

Данный перечень подготовлен в соответствии со следующими нормативными документами:

1. Федеральный закон от 27 июля 2006г. №152-ФЗ «О персональных данных»;
2. Постановление Правительства РФ от 1 ноября 2012г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
3. «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» Приказ ФСТЭК России от 18.02.2013г №21;
4. «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», утв. приказом ФСБ России от 10 июля 2014г. №378;
5. Приказ ФСБ России от 9 февраля 2005г. №66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;
6. «Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утв. приказом ФАПСИ от 13 июня 2001г. №152;
7. «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности», утвержденные руководством 8 Центра ФСБ России (№149/7/2/6-432 от 31 марта 2015г.).

№ п/п	Наименование документа	Основание	Наличие	Примечание
1.	Приказ о создании комиссии по защите информации ограниченного доступа, обрабатываемой в ИС	Пункт 8 «Требований к защите ПДн ...» (№1119). Статья 18.1 пункт 1 подпункт 5 Федерального закона «О персональных данных» (№152-ФЗ)	Предоставлен шаблон документа «1 Приказ о создании комиссии».	**Данные документы разработаны для всех информационных систем персональных данных Организации. Они могут дополняться, исправляться в соответствии с особенностями обработки персональных данных в Организации.** **Данные документы необходимы, чтобы пройти проверку Роскомнадзора.**
2.	Акт определения уровня защищенности персональных данных, при их обработке в информационной системе	Пункт 8 «Требований к защите ПДн ...» (№1119). Статья 19, пункт 2, подпункт 9 Федерального закона «О персональных данных» (№152-ФЗ): *«Обеспечение безопасности достигается, в частности… контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных».*	Предоставлен шаблон документа «1.1 Акт определения уровня защищенности»	
3.	Акт оценки потенциального вреда субъектам персональных данных	Статья 18.1 пункт 1 подпункт 5 Федерального закона «О персональных данных» (№152-ФЗ): *«…оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения настоящего Федерального закона, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом»;*	Предоставлен шаблон документа «1.2 Акт определения потенциального вреда»	
4.	Приказ о назначении ответственных	Статья 18.1 пункт 1 подпункт 1 Федерального закона «О персональных данных» (№152-ФЗ): *«…назначение оператором, являющимся юридическим лицом, ответственного за организацию обработки персональных данных»;*	Предоставлен шаблон документа «2 О назначении ответственных»	

№ п/п	Наименование документа	Основание	Наличие	Примечание
	Инструкция ответственного за организацию обработки персональных данных	Статья 22.1 Федерального закона «О персональных данных» (№152-ФЗ): *«Оператор, являющийся юридическим лицом, назначает лицо, ответственное за организацию обработки персональных данных».*	Предоставлен шаблон документа «2 О назначении ответственных» Приложение 1	
	Инструкция ответственного за защиту информации в ИС	Рекомендуется аттестующей организацией для разделения полномочий и обязанностей по защите персональных данных	Предоставлен шаблон документа «2 О назначении ответственных» Приложение 2	
	Инструкция администратора ИС	Рекомендуется аттестующей организацией для разделения полномочий и обязанностей по защите персональных данных	Предоставлен шаблон документа «2 О назначении ответственных» Приложение 3	
5.	Приказ о утверждении перечня персональных данных, информационных систем персональных данных и допущенных работников		Предоставлен шаблон документа «3 Перечень ПДн ИСПДн и допущенных» Приложение 1	
	Перечень ПДн, обрабатываемых на объекте информатизации	Рекомендуется аттестующей организацией. По опыту проверок, Роскомнадзор такой документ запрашивает.		
	Перечень информационных систем персональных данных	Рекомендуется аттестующей организацией. По опыту проверок, Роскомнадзор такой документ запрашивает.	Предоставлен шаблон документа «3 Перечень ПДн ИСПДн и допущенных» Приложение 2	

№ п/п	Наименование документа	Основание	Наличие	Примечание
	Перечень должностей работников, допущенных к обработке персональных данных	Пункт 13в «Требований к защите ПДн ...» (№1119): *«…утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей»*	Предоставлен шаблон документа «3 Перечень ПДн ИСПДн и допущенных» Приложение 3	
6.	Правила доступа в помещения	Пункт 13.а «Требований к защите ПДн ...» (№1119): *«Организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения».* ЗТС.3 «Состава и содержания организационных …» (№21) *«…контроль и управление физическим доступом к техническим средствам, СЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, СЗИ и средствам обеспечения функционирования ИС, в помещения и сооружения, в которых они установлены».*	Предоставлен шаблон документа «4 Приказ об орг режима обеспеч безоп помещений».	
7.	Приказ об утверждении инструкций по защите персональных данных.		Представлен шаблон документа «5 Приказ об утв интрукций по защите ПДн»	

№ п/п	Наименование документа	Основание	Наличие	Примечание
	Инструкция пользователя информационных систем персональных данных	Статья 18.1, часть 1, пункт 6 Федерального закона «О персональных данных» (№152-ФЗ). Статья 19, часть 2, пункт 8 Федерального закона «О персональных данных» (№152-ФЗ) АВЗ.1, АВЗ.2, УПД.15, ЗТС3, ЗТС4 «Требований о защите информации ...» (№21).	Представлен шаблон документа «5 Приказ об утв интрукций по защите ПДн» Приложение 1	
	Инструкция по парольной защите информации	ИАФ1, ИАФ3, ИАФ4, ИАФ5, ИАФ6 «Требований о защите информации ...» (№21) ИАФ.4: *«Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации»*	Представлен шаблон документа «5 Приказ об утв интрукций по защите ПДн» Приложение 2	
	Инструкция по организации антивирусной защиты	АВЗ.1, АВЗ.2, «Требований о защите информации ...» (№21). АВЗ.1: *«Реализация антивирусной защиты»*	Представлен шаблон документа «5 Приказ об утв интрукций по защите ПДн» Приложение 3	

№ п/п	Наименование документа	Основание	Наличие	Примечание
	Инструкцию по организации резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных	Статья 19, часть 2, пункт 7 Федерального закона «О персональных данных» (№152-ФЗ): *«Обеспечение безопасности ПДн достигается, в частности… восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним»;*	Представлен шаблон документа «5 Приказ об утв интрукций по защите ПДн» Приложение 4	
	Порядок обращения со съемными машинными носителями персональных данных	Статья 19, часть 2, пункт 5 Федерального закона «О персональных данных» (№152-ФЗ): *«Обеспечение безопасности ПДн достигается, в частности… учетом машинных носителей персональных данных»;* Пункт 13.б «Требований к защите ПДн ...» (№1119).	Представлен шаблон документа «5 Приказ об утв интрукций по защите ПДн» Приложение 5 + форма журнала учет съемных машинных носителей и форма акта об уничтожении съемных машинных носителей	
8.	Приказ об обращении со средствами криптографической защиты информации <u>Приложение 1</u>: Инструкция по обращению с	Пункт 30, пункт 51, Раздел 2, раздел 3 «Инструкции об организации...» (№152). Пункт 13.а «Требований к защите ПДн ...» (№1119). ЗТС.3, ЗИС.3 «Требований о защите информации ...» (№21).	Предоставлен шаблон документа «6 Инструкция по обращению с СКЗИ» + журнал учета СКЗИ + журнал учета ключей от режимных помещений + заключение о	**Данный документ необходим только в том случае, если Организация использует средства криптографической**

№ п/п	Наименование документа	Основание	Наличие	Примечание
	криптографическими средствами защиты информации; Приложение 2: Перечень помещений, выделенных для установки средств криптографической защиты информации и хранения ключевых документов к ним; Приложение 3: Приказ о хранилищах		допуске к работе с СКЗИ	**защиты (СКЗИ)**
9.	Регламент реагирования на инциденты информационной безопасности	Статья 19, часть 2, пункт 6 Федерального закона «О персональных данных» (№152-ФЗ). РСБ.1, РСБ.2, РСБ.3, РСБ.7 «Требований о защите информации ...» (№21): *«Определение событий безопасности, подлежащих регистрации, и сроков их хранения…Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения»*	Предоставлен шаблон документа «7 Регламент реагирования на инциденты ИБ» + журнал учета нештатных ситуаций.	**Частично несет и рекомендательный характер по пунктам РСБ.4, РСБ.5, РСБ.6 «Требований о защите информации ...» (№21).**
10.	Приказ о разрешительной системе доступа: Приложение 1: Положение о разрешительной системе доступа;	Статья 19, часть 2, пункт 8 Федерального закона «О персональных данных» (№152-ФЗ). ИАФ.1, ИАФ.3, ИАФ.4, ИАФ.5, ИАФ.6, УПД.1, УПД.2, УПД.3, УПД.4, УПД.5, УПД.6, УПД.15, РСБ.7, «Требований о защите информации ...» (№21). УПД: *«Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей,*	Предоставлен шаблон документа «8 Положение о разрешительной системе доступа».	**Данные документы разработаны для всех информационных систем персональных данных**

№ п/п	Наименование документа	Основание	Наличие	Примечание
	<u>Приложение 2:</u> Матрица субъектов доступа.	*в том числе внешних пользователей… Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей»* Пункт 19 «Инструкции об организации…» (№152).		**Учреждения. Они могут дополняться, исправляться в соответствии с особенностями обработки персональных данных в Учреждении.** **Данные документы необходимы, чтобы пройти проверку Роскомнадзора.**
11.	Приказ об утверждении положения об организации обработки персональных данных без использования средств автоматизации	ПП РФ от 15 сентября 2008 г. №687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации"	Представлен шаблон документа «9 Положение об неавтоматизированной обработке ПДн» + журнал учета мест хранения носителей ПДн + акт об уничтожении бумажных носителей ПДн	
12.	Регламент проведения внутреннего контроля соответствия обработки информации ограниченного доступа требованиям к защите информации ограниченного доступа	Статья 18.1, часть 1, пункт 4 Федерального закона «О персональных данных» (№152-ФЗ): *«…осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных настоящему Федеральному закону и принятым в соответствии с ним нормативным правовым актам».* Статья 19, часть 2, пункт 6 Федерального закона «О персональных данных» (№152-ФЗ). Пункт 17 «Требований к защите ПДн ...» (№1119). *«Контроль за выполнением настоящих требований организуется и проводится оператором (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих*	Предоставлен шаблон документа «10 Регламент проведения внутр контроля соотв обработки ПДн».	

№ п/п	Наименование документа	Основание	Наличие	Примечание
		лицензию…» РСБ.1, РСБ.2, РСБ.3, АНЗ.2, «Требований о защите информации ...» (№21). Пункт 73 «Инструкции об организации…» (№152).		
13.	Приказ об утверждении положения об обеспечении безопасности персональных данных	Рекомендуется	Предоставлен шаблон документа «11 Положение об обеспечении безопасности ПДн».	
14.	Приказ об утверждении положения об организации обработки персональных данных	Статья 6 пункт 3 Федерального закона «О персональных данных» (№152-ФЗ) Статья 7 Федерального закона «О персональных данных» (№152-ФЗ) Статья 18 Федерального закона «О персональных данных» (№152-ФЗ) Статья 18.1 пункт1 подпункт 2 Федерального закона «О персональных данных» (№152-ФЗ) Статья 9 Федерального закона «О персональных данных» (№152-ФЗ) Статья 21 Федерального закона «О персональных данных» (№152-ФЗ)	Предоставлен шаблон документа «12 Положение об организации обработки ПДн» + обязательство о неразглашении + форма договора на поручении ПДн.	