

Персональные данные в НКО: руководство по безопасной обработке и защите

Все организации обязаны строго следовать установленным правилам для защиты персональных данных сотрудников и клиентов, обеспечивая безопасность и конфиденциальность сведений.

Памятка составлена по материалам вебинара «Персональные данные в НКО: основы и риски».

Спикер: Виктория Павлюк, генеральный директор Ассоциации экспертов гражданского общества Краснодарского края, руководитель РЦ АНО поддержки социальных инициатив "Третий сектор".

Содержание:

Что такое персональные данные?.....	1
Категории персональных данных.....	3
Кто является оператором персональных данных?.....	4
Зачем обрабатывать персональные данные?.....	5
Основания для обработки персональных данных.....	6
Виды согласий на обработку персональных данных.....	7
Согласие на обработку персональных данных.....	7
Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения.....	9
Обработка персональных данных третьими лицами.....	10
Охрана изображений человека.....	11
Локальная документация и меры по защите персональных данных.....	12
Обязательные документы.....	13
Рекомендованные меры безопасности.....	13
Ответственность за обработку персональных данных и подготовка к проверкам	14
Как подготовить сайт к проверке?.....	16

Что такое персональные данные?

Персональные данные — это любые сведения, относящиеся к прямому или косвенному определению физического лица [субъекта персональных данных]. Они позволяют идентифицировать конкретное лицо и являются основой для реализации конституционного права на неприкосновенность личной жизни и тайны.

Основные термины

- **Субъект персональных данных** - физическое лицо, которому принадлежат персональные данные.
- **Обработка персональных данных** - любое действие или совокупность действий, совершаемых с персональными данными, включая сбор, хранение, передачу и уничтожение.
- **Оператор обработки персональных данных** - организация или индивидуальный предприниматель, осуществляющие обработку персональных данных.

Законодательная база

Работа с персональными данными регулируется рядом нормативных актов:

- **Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных»**
Основной документ, определяющий понятие персональных данных, порядок их хранения и обработки, а также обязанности операторов обработки.
- **Постановление Правительства РФ от 15.09.2008 N 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации»**
Регламентирует работу с персональными данными без использования средств автоматизации [бумажные носители].
- **Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»**
Определяет порядок автоматизированной обработки данных, включая использование оборудования и компьютеров.

Приказы Роскомнадзора

определяющие требования к оформлению согласий на обработку данных и оценки потенциального ущерба при возможных утечках:

- Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 24.02.2021 N 18 «[Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения](#)»
- Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 24.12.2021 N 253 «[Об утверждении формы проверочного листа \[списка контрольных вопросов, ответы на которые свидетельствуют о соблюдении или несоблюдении контролируемым лицом обязательных требований\], применяемого при осуществлении федерального государственного контроля \[надзора\] за обработкой персональных данных Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций и ее территориальными органами](#)»
- Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 27.10.2022 N 178 «[Об утверждении требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения ФЗ “О персональных данных”](#)»
- Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28.10.2022 N 179 «[Об утверждении требований к подтверждению уничтожения персональных данных](#)»

Приказ Федеральной службы по техническому и экспортному контролю [ФСТЭК]

предусматривающий меры технической защиты персональных данных

- Приказ Федеральной службы по техническому и экспортному контролю от 18.02.2013 N 21 «[Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных](#)»

Контроль и регулирование

За соблюдение норм и правил работы с персональными данными отвечают следующие органы:

- **Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций [Роскомнадзор]**
контроль и надзор за обработкой персональных данных.
- **Федеральная служба по техническому и экспортному контролю [ФСТЭК]**
технические аспекты защиты информации.
- **Государственная инспекция труда**
защита прав работников в сфере персональных данных.
- **Прокуратура**
общий надзор за исполнением закона.

Категории персональных данных

Персональные данные подразделяются на различные категории в зависимости от уровня чувствительности и риска нарушения конфиденциальности. Разделение персональных данных на три группы [общие, специальные, биометрические] носит условно-принятый характер и служит исключительно для удобства восприятия и понимания особенностей каждой категории. Такое деление помогает чётко осознавать уровень ответственности и рисков, связанных с обработкой различных типов данных.

- **Общие персональные данные**
включают стандартные сведения, такие как фамилия, имя, отчество, адрес проживания, контактные данные и др.
- **Специальные категории персональных данных**
относятся к наиболее чувствительным данным, таким как раса, национальность, политические взгляды, религиозные убеждения, состояние здоровья, наличие судимости и интимная жизнь.
- **Биометрические персональные данные**
информация, характеризующая физические и биологические характеристики человека, позволяющие однозначно определить его личность [например, отпечатки пальцев, голосовая запись, фотография с целью распознавания лиц].

Специальные категории персональных данных

Эти данные требуют особого внимания и защиты, поскольку нарушение их конфиденциальности может привести к серьёзным последствиям для субъектов данных. К специальным категориям относятся:

- Расовая принадлежность

- Национальность
- Политические предпочтения
- Религиозные или философские убеждения
- Медицинская информация [диагнозы, лечение]
- Судимость
- Интимная жизнь

Для некоммерческих организаций особенно важны медицинские данные, так как многие благотворительные проекты работают с социально уязвимыми группами населения. Обработка специальных категорий требует обязательного письменного согласия субъекта данных или его законного представителя.

Биометрические персональные данные

Это особая категория данных, включающая информацию, которая уникально определяет физическую индивидуальность человека. Примеры биометрических данных:

- Отпечатки пальцев
- Голосовые записи
- Изображения сетчатки глаза
- Фотографии и видеозаписи, используемые для идентификации личности

Важно отметить, что сами по себе фотографии и видеоролики не становятся автоматически биометрическими данными. Они приобретают статус биометрической информации лишь тогда, когда предназначены для целей автоматической идентификации личности.

Кто является оператором персональных данных?

Организация становится оператором персональных данных с момента её создания и начала деятельности. Этот статус распространяется абсолютно на всех юридических лиц, независимо от вида деятельности и размера организации. Исключить себя из статуса оператора невозможно, так как практически каждая организация сталкивается с необходимостью обработки персональных данных в ходе своей обычной деятельности.

Оператором персональных данных считается любая организация, которая совершает любые действия с персональными данными физических лиц, включая:

- Сбор
- Запись

- Систематизацию
- Накопление
- Хранение
- Уточнение
- Обновление
- Изменение
- Обезличивание

Процесс обработки персональных данных охватывает как автоматизированные методы [использование программного обеспечения, баз данных], так и традиционные способы ведения делопроизводства [документация на бумаге].

Обязанности оператора персональных данных

- Соблюдать установленные законом процедуры обработки персональных данных.
- Получить согласие субъекта данных перед началом обработки специальной или биометрической информации.
- Применять необходимые меры для защиты данных от несанкционированного доступа.
- Информировать субъекты данных о целях и способах обработки их информации.

Зачем обрабатывать персональные данные?

Цель обработки персональных данных должна быть четко определенной и ограниченной заранее установленными сроками. Закон предписывает прекратить обработку данных сразу же после достижения поставленной цели, кроме случаев, предусмотренных законодательством. После завершения обработки персональные данные подлежат уничтожению или обезличиванию.

Ключевые принципы обработки персональных данных

- **Четкость целей**
Любые операции с персональными данными должны соответствовать конкретной цели и иметь временные рамки.
- **Минимизация объема данных**
Организации не вправе собирать избыточные персональные данные сверх необходимого минимума для выполнения поставленных задач.
Например:
- *Работники: объем необходимых данных определяется Трудовым кодексом РФ.*

- Исполнители услуг по договорам ГПХ: достаточно знать имя и реквизиты банковского счёта.

- Добровольцы: требуются только ФИО.

- **Соблюдение сроков хранения**

Лишняя информация подлежит удалению или обезличиванию после окончания периода, необходимого для выполнения целей обработки.

- **Запрет бессрочного хранения**

Получение бессрочных согласий на обработку и хранение персональных данных противоречит закону.

- **Соответствие целям**

Вся обработка персональных данных должна основываться на конкретных законных целях.

Дорожная карта

1. Определите конкретные цели обработки персональных данных.
2. Составьте список необходимой информации для каждой цели.
3. По завершении обработки уничтожайте или обезличивайте неиспользуемые данные.

Советы по снижению административных рисков:

- Не храните копии паспортов работников. Данные из паспорта можно перенести в специальную форму, а сам документ вернуть владельцу.
- Чтобы сохранить копию документа, получите отдельное письменное согласие сотрудника.

Основания для обработки персональных данных

Закон предусматривает ряд оснований, разрешающих обработку персональных данных. Рассмотрим три ключевых основания, применимых для некоммерческих организаций:

1. Согласие субъекта персональных данных

Согласие обязательно получать, если обработка осуществляется без наличия иных правовых оснований.

Оно должно быть дано добровольно, осознанно и конкретно сформулировано относительно цели обработки.

2. Исполнение договоров

Когда персональные данные необходимы для исполнения обязательств по заключенным договорам [например, оказание услуг, выполнение работ].

Субъектом данных может выступать работник, исполнитель услуг или клиент.

3. Необходимость исполнения закона

Осуществляется, если обработка необходима для выполнения обязанностей, возложенных на организацию законодательством [например, предоставление отчётности государственным органам].

Кроме указанных оснований, существуют ситуации, когда обработка возможна без прямого согласия субъекта данных:

- Осуществление прав и законных интересов оператора или третьих лиц, если это не нарушает права и свободы субъекта данных.
- Общественно значимые цели, при соблюдении баланса интересов сторон.

Примеры ситуаций

- *Если работодатель производит удержания из заработной платы сотрудника на уплату алиментов, то помимо заявления о переводе алиментов необходимо получение согласия обоих участников процесса.*
- *При размещении фотографий сотрудников на официальном сайте организации необходимо дополнительное согласие, если такая возможность не предусмотрена условиями трудового договора.*

Виды согласий на обработку персональных данных

В соответствии с действующим законодательством можно выделить два отдельных согласия:

1. **Согласие на обработку персональных данных**
статья 9 Федерального закона «О персональных данных»
2. **Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения**
статья 11.1 Федерального закона «О персональных данных»

В российском законодательстве предусмотрены две ключевые формы согласий на обработку персональных данных:

Согласие на обработку персональных данных

Получение согласия на обработку персональных данных является обязательным условием для правомерной обработки данных организацией.

Согласие на обработку персональных данных может быть дано субъектом данных или его представителем в любой форме, позволяющей подтвердить факт его получения, если иное не предусмотрено федеральными законами.

Ограничения и исключения

- **Дееспособность субъекта**

Если субъект данных признан недееспособным, согласие даёт его законный представитель.

- **Наследники**

После смерти субъекта данных согласие предоставляют его наследники.

- **Получение данных от третьих лиц**

Если данные поступают от третьих лиц, необходимо убедиться в легальности их получения.

Важно учитывать следующее:

- Форма согласия может быть устной, письменной или электронно-цифровой.
Особые случаи:
 - Для обработки особо чувствительных данных [биометрия, здоровье и т.д.] требуется специальное письменное согласие.
 - Передача данных за границу также требует отдельного письменного согласия.
- Ответственность за подтверждение получения согласия лежит на операторе.
- Согласия хранятся в специальном разделе сервера организации.

Правила оформления согласия

- **Подтверждение согласия**

Вы можете зафиксировать согласие любыми доступными способами, однако важно, чтобы была возможность доказать факт получения согласия.

- **Электронное согласие**

Допускается использование электронной цифровой подписи [ЭЦП], которая доступна через портал государственных услуг ["Госуслуги"].

- **Отзыв согласия**

Субъект данных имеет право отозвать своё согласие в любой момент. Оператор продолжает обработку только при наличии соответствующих оснований, предусмотренных законодательством.

Как подтвердить получение согласия при анкетировании?

Чтобы подтвердить факт дачи согласия на обработку персональных данных при электронном анкетировании, рекомендуется предусмотреть дополнительные механизмы:

- **Автоматическая обратная связь**

Включите в систему анкетирования автоматический механизм отправки подтверждения о согласии. Пользователь получает уведомление о том, что он подтвердил свое согласие на обработку данных.

- **Отметка о согласии**

Позаботьтесь о том, чтобы пользователи могли поставить соответствующую отметку о своём согласии на обработку данных при заполнении анкеты.

Содержание согласия

В соответствии со статьей 9 Федерального закона «О персональных данных», согласие должно содержать следующую информацию:

1. ФИО и адрес субъекта данных.
2. Реквизиты документа, удостоверяющего личность.
3. Полномочия представителя субъекта данных [если согласие даёт представитель].
4. Назначение и адреса оператора.
5. Цель обработки данных.
6. Перечень передаваемых данных.
7. Срок действия согласия и процедура его отзыва.
8. Подпись субъекта данных.

Передача данных третьим лицам

Если ваша организация планирует передать персональные данные третьим лицам [например, партнёрам фонда, аутсорсинговым компаниям или участникам грантовых конкурсов], согласие должно содержать конкретные указания о том, кому именно разрешено передавать данные, а также цель и метод передачи. Недостаточно просто указать общую фразу о возможности передачи третьим лицам. Необходимо точно обозначить каждую сторону, которой разрешается передача данных.

Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения

В марте 2021 вступили в силу важные изменения в Федеральный закон «О персональных данных»:

- **Появился термин «персональные данные, разрешенные для распространения»**
Это персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения.
- **Появился новый документ – согласие на обработку персональных данных, разрешенных для распространения.**
Порядок работы с ним изложен в статье 10.1 Федерального закона «О персональных данных» и Приказе Роскомнадзора от 24.02.2021 N 18.

Распространение персональных данных подразумевает публикацию информации в открытом доступе, позволяя неограниченному числу лиц просматривать и использовать эти данные. Часто возникает путаница между передачей данных определенным лицам и их открытым распространением. Рассмотрим различия и правила оформления согласия на распространение.

Отличие передачи от распространения

- Передача персональных данных заранее указанным третьим лицам [например, подрядчикам или партнерам]. Регулируется стандартным соглашением на обработку персональных данных.
- Распространение данных делает информацию доступной широкой публике, например, публикуя данные на веб-сайте или социальных сетях.

Правила получения согласия на распространение

- Согласие на распространение персональных данных оформляется отдельно от общего согласия на обработку данных.
- Должно быть ясно указано, какие именно данные [ФИО, контакты и т.д.] и на каких ресурсах [сайтах, платформах] будут опубликованы.
- Отсутствие специального согласия означает запрет на распространение данных неограниченному кругу лиц.

Содержание согласия на обработку персональных данных, разрешенных для распространения:

1. ФИО субъекта данных.

2. Контактная информация [телефон, email, почтовый адрес].
3. Сведения об операторе - организации [наименование, адрес из ЕГРЮЛ, ИНН, ОГРН].
4. Сведения об операторе - физическом лице [ФИО, место жительства или пребывания].
5. Сведения об операторе - ИП [ФИО, ИНН, ОГРНИП].
6. Сведения об информационных ресурсах.
7. Цель обработки данных.
8. Категория и перечень персональных данных.
9. Категория и перечень персональных данных, для обработки которых субъект устанавливает условия и запреты, и их перечень [по желанию субъекта].
10. Условия передачи персональных данных по внутренней сети оператора, через интернет, либо без передачи [по желанию субъекта].
11. Срок действия согласия

Обработка персональных данных третьими лицами

Если ваша организация передает обработку персональных данных третьим лицам [например, субподрядчикам, аутсорсинговым компаниям], необходимо заключить специальный договор, содержащий важные условия.

Основные требования к договору

- **Перечень персональных данных**
Договор должен подробно определять, какие именно персональные данные будут переданы третьей стороне для обработки.
- **Описание действий с данными**
Подробно укажите, какие действия третья сторона будет осуществлять с данными [например, хранение, обновление, удаление].
- **Цели обработки**
Чётко зафиксируйте цели, ради которых передается обработка данных.
- **Конфиденциальность**
Обязательно пропишите обязательства по обеспечению конфиденциальности и сохранности данных.
- **Местонахождение данных**
Подчеркните, что все персональные данные должны храниться на территории Российской Федерации.

Последствия несоблюдения требований

Если договор не соответствует приведённым условиям, он может быть признан недействительным. Поэтому крайне важно уделить внимание деталям и обеспечить полное соответствие документу требованиям российского законодательства.

Охрана изображений человека

Фотографические и видеок cadры с изображением людей часто воспринимаются как обычные материалы, однако в ряде случаев они классифицируются как биометрические персональные данные. Согласно российскому законодательству, подобные данные требуют особого подхода при обработке и хранении.

Что такое биометрические персональные данные?

Биометрические персональные данные – это информация, связанная с физическими характеристиками человека, позволяющими однозначно идентифицировать его личность. Такие данные считаются высокочувствительными и подлежат особой охране.

Признаки биометрических данных:

- Фотография, позволяющая четко идентифицировать лицо.
- Идентификация голоса, глаз, отпечатков пальцев и т.д.

Обычные изображения и биометрия:

- Простые фотографии или коллективные снимки, на которых трудно выделить одного человека, не попадают под категорию биометрических данных.
- Если фотография или видео позволяют легко идентифицировать конкретное лицо, они квалифицируются как биометрические.

Необходимость получения согласия

В большинстве случаев понадобится два разных согласия:

1. **Согласие на обработку биометрических данных**

Любая некоммерческая организация [НКО] обязана получить предварительное письменное согласие субъекта данных на обработку биометрических данных. Формат согласия должен соответствовать нормам действующего законодательства.

2. **Согласие на распространение данных**

Если планируется публикация фото или видеоизображений в

общедоступных источниках [например, на сайте или в соцсетях], необходимо получить ещё одно отдельное согласие на распространение персональных данных.

Исключение из правил

Гражданский кодекс РФ выделяет несколько исключений, когда не требуется предварительного согласия на использование изображений:

- **Использование в общественных или государственных интересах**
публикация изображений, раскрывающих угрозу общественному порядку или экологической обстановке.
- **Фотографирование на публичных мероприятиях**
съёмка массовых мероприятий, концертов, собраний, соревнований и аналогичных событий, если изображение не является главным объектом съёмки.

Рекомендации по обращению с изображениями

- Оформлять отдельные соглашения на обработку и распространение данных.
- Проверять качество и специфику изображения перед отнесением его к биометрическим данным.
- Избегать публикаций изображений без надлежащего обоснованного согласия.

Локальная документация и меры по защите персональных данных

Обеспечение должного уровня защиты персональных данных предполагает разработку ряда внутренних документов и внедрение комплексных мер по безопасности. Определенного перечня разработанных или утвержденных бланков нет, и каждый оператор должен это делать самостоятельно с учетом специфики своей деятельности. Есть определенный перечень бланков, документов, который можно назвать обязательным.

Обязательные документы

- **Приказ о назначении ответственного за обработку персональных данных**
Назначенный ответственный сотрудник контролирует выполнение

всех норм и правил обработки персональных данных. Если штат сотрудников небольшой, эта роль может быть возложена на руководителя организации.

- **Положение об обработке и защите персональных данных**

Этот внутренний документ детально описывает процедуру сбора, хранения, обработки и защиты персональных данных в организации. В положении рекомендуется отразить:

1. Категорию субъектов персональных данных [например, работники, посетители сайта, партнеры].
2. Перечень обрабатываемых данных.
3. Цели обработки данных.
4. Меры защиты данных.
5. Процедура уничтожения данных.
6. Порядок блокировки данных при нарушении правил обработки.
7. Локальные акты, принимаемые во исполнение положения.

Утвержденное положение доводится до сотрудников под подпись теми, кто непосредственно работает с персональными данными.

- **Политика оператора в отношении обработки персональных данных**

Политика оператора – это публичный документ, доступный широкому кругу заинтересованных лиц. Он размещается на сайте организации и доступен для просмотра пользователями интернета. В документе отражаются:

1. Информационная открытость деятельности оператора.
2. Методы обработки и защиты данных.
3. Публичные обязательства оператора по отношению к пользователям.

Конструктор организационно-распорядительной документации по работе с персональными данными.

Рекомендованные меры безопасности

Оценка рисков и внутренний контроль

Рекомендуется регулярно проводить оценку рисков утечки или незаконного использования персональных данных. Один из вариантов – составление акта оценки возможных угроз или проверка посредством чек-листа. Проводятся профилактические мероприятия по обучению сотрудников основам безопасного обращения с персональными данными.

Управление информационными системами

- Создайте перечень информационных систем, содержащих персональные данные, и разместите его на внутреннем контроле.
- Разработайте инструкции для сотрудников, ответственных за защиту данных.
- Проверьте доступ сотрудников к персональным данным и установите строгие границы доступа.
- Периодически обновляйте программное обеспечение и защитные средства [антивирус, файрволлы].

Обучение персонала

Сотрудники, имеющие доступ к персональным данным, должны подписать обязательство о неразглашении информации. Организуйте обучение персонала по вопросам обработки персональных данных, подчеркивая важность конфиденциальности и безопасности.

Регистрация в реестре операторов

Каждой организации необходимо подать уведомление в Роскомнадзор о ведении деятельности, связанной с обработкой персональных данных. Это защищает компанию от штрафов и претензий со стороны контролирующего органа.

Уведомление подается одним из способов:

- Бумажная форма.
- Электронная форма с использованием электронной цифровой подписи [ЭЦП].
- Через портал "Госуслуги".

Если планируется трансграничная передача данных [за пределы РФ], необходимо подать отдельное уведомление в Роскомнадзор, рассмотрение которого занимает около десяти дней.

Ответственность за обработку персональных данных и подготовка к проверкам

При обработке персональных данных важно соблюдать установленные законодательством требования, чтобы избежать негативных последствий. Давайте рассмотрим ключевые моменты, касающиеся ответственности и подготовки к возможным проверкам.

Органы надзора и типы проверок

Основными органами, осуществляющими контроль за обработкой персональных данных, являются:

- **Роскомнадзор**
проводит проверки, направленные на выявление нарушений законодательства в области обработки персональных данных.
- **Федеральная служба по техническому и экспортному контролю [ФСТЭК]**
следит за соблюдением технических мер защиты данных.
- **ФСБ**
участвует в обеспечении защиты государственной тайны и стратегически важной информации.

Типы проверок, проводимых Роскомнадзором:

- **Инспекционный визит**
обследование без назначения проверяющих органов.
- **Документарная проверка**
изучение документов без выезда на объект.
- **Выездная проверка**
посещение объекта с проведением осмотра и анализа документов.

Критерии проверки

При проведении проверок Роскомнадзор уделяет внимание следующим аспектам:

- Наличие уведомления о регистрации в качестве оператора персональных данных.
- Назначение ответственного за обработку персональных данных.
- Наличие политики и других локальных актов по обработке персональных данных.
- Соответствие порядка обработки и хранения данных установленным требованиям.
- Наличие согласий на обработку персональных данных.
- Реакция на жалобы и запросы субъектов персональных данных.
- Выполнение требований по защите данных в информационных системах.

Проверочный лист на основании которого можно выделить основные моменты, на которые следует обратить внимание при подготовке к проверке.

Как подготовить сайт к проверке?

При подготовке сайта к проверке обратите внимание на следующие моменты:

- Сайт размещен на территории Российской Федерации.
- Наличие файла cookie и метрик [Google Analytics, Яндекс.Метрика и т.д.].
- Доступность публичной политики обработки персональных данных.
- Использование современных методов шифрования [SSL/TLS].
- Удаление устаревших или излишних данных.

Другие меры предосторожности

Дополнительные шаги для повышения уровня безопасности:

- Проведение регулярных тренингов для сотрудников по вопросам обработки персональных данных.
- Установка надежного программного обеспечения для защиты данных.
- Создание резервных копий важных данных.
- Постоянный мониторинг активности сотрудников, имеющих доступ к персональным данным.