



едурегионлаб

БЕСПЛАТНЫЙ ВЕБИНАР

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

НОВЫЕ ТРЕБОВАНИЯ 2026 ГОДА,
ДОКУМЕНТЫ И ЗАЩИТА
ОТ КИБЕРУГРОЗ



Эксперт

ГЕРАСИМЕНКО НАТАЛЬЯ СЕРГЕЕВНА

- Кандидат юридических наук
- Эксперт по охране и экономике труда
- Эксперт по проведению НОК в области охраны труда (г. Москва)
- Помощник по вопросам охраны труда уполномоченного по защите прав предпринимателей в Волгоградской области

Информационная безопасность и защита информации



Обучение
информационной
безопасности



Что такое информационная безопасность



Информационная безопасность (ИБ) — практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации

Это **комплекс мероприятий, направленных на защиту от утечки или взлома программ, компьютерных систем и данных**

Информация — сведения (сообщения, данные) независимо от формы их представления, это любые сведения, которые можно сохранить, преобразовать и передать

Виды информации:

- акустическая (речевая) информация;
- информация, получаемая в виде изображений объектов или документов;
- информация, обрабатываемая (циркулирующая) в информационной системе в виде электрических, электромагнитных, оптических сигналов;
- информация, обрабатываемая в ИС, представленная в виде бит, байт, файлов.

Информационная система — совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Обучение
информационной
безопасности



Что такое информационная безопасность



Информационные технологии — процессы и методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов

Информационно-телекоммуникационная сеть — технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники

Событие в системе информационной безопасности — выявленный случай в системе, услуге по доступу к информации или состоянию сети, указывающий на возможное нарушение информационной безопасности, политики, нарушение или отказ средств управления или прежде неизвестная ситуация, которая может иметь значение для безопасности информации

Инцидент информационной безопасности — одно событие или серия нежелательных или нетипичных событий в системе обработки информационной безопасности, которые имеют большой шанс подвергнуть риску деловые операции и поставить под угрозу информационную безопасность информации.

Обучение
информационной
безопасности



Что такое информационная безопасность



Конфиденциальность — состояние защищенности информации, которое характеризуется способностью АС обеспечивать сохранение в тайне информации от субъектов, не имеющих полномочий на ознакомление с ней. Это свойство информации быть недоступной и закрытой для неавторизованных лиц, субъектов или процессов

К конфиденциальным сведениям относятся **персональные данные сотрудников организации и их родственников, служебная информация**. Не относятся к конфиденциальной информации данные, внесенные в свидетельство о регистрации юридического лица, лицензию или учредительные документы, относящиеся к кадровой политике и способам оплаты труда, сведения о наличии вредных производственных факторов, информация о проведении на предприятиях тендеров и конкурсов с целью подписания контрактов и набора новых сотрудников, данные о финансовой деятельности некоммерческих организаций

Нарушение конфиденциальности — состояние, когда информация становится известной лицу, не располагающему полномочиями доступа к ней

Угрозы конфиденциальности — несанкционированный доступ неких лиц к базам данных или иным хранилищам

Перехват — получение несанкционированного доступа к ресурсу. Подключение к каналу связи с целью перехвата данных

Обучение
информационной
безопасности



Что такое информационная безопасность



Разглашение конфиденциальной информации — действие или бездействие, в результате которых информация, составляющая тайну, становится известной третьим лицам без согласия обладателя такой информации

Целостность — состояние защищенности информации, которое характеризуется способностью системы или сервиса обеспечивать сохранность и неизменность конфиденциальной информации при попытках несанкционированных или случайных воздействий на нее в процессе обработки и хранения. Это свойство сохранения правильности и полноты информационных ресурсов

Нарушение целостности — повреждение информации. Вирус, злоумышленник или физический процесс, проникший в систему, стирает или видоизменяет данные, что нарушает систему обработки информации или сведения, содержащиеся в ней, или делает невозможной ее работу

Модификация — доступ к информационному ресурсу, приведший к изменению информации

Атака — попытка уничтожения, открытия доступа, внесения изменения, вывода из строя, кражи, получения несанкционированного доступа или несанкционированного использования информационной системы или ресурса

Обучение
информационной
безопасности



Что такое информационная безопасность



Контроль доступа — обеспечение того, чтобы доступ к активам был санкционирован и ограничен в соответствии с требованиями коммерческой тайны и безопасности

Доступность информации — состояние информации и/или системы ее обработки, которое характеризуется способностью обеспечивать доступ к информации субъектов, имеющих на это полномочия

Предоставление доступа к информации — действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц

Распространение информации — действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц

Угрозы доступности — ограниченность или невозможность доступа к базе данных, например, по причине атаки или сбоя в работе системы обработки информации

Обучение
информационной
безопасности



Что такое информационная безопасность



Нарушение доступности информации — блокирование доступа к информации, выведение из строя средств связи, технических средств обработки информации

Угроза — возможная причина нежелательного инцидента, который может закончиться ущербом для системы или организации (атаки на доступность — это DDOS)

Уязвимость — слабость актива или средства управления, на которых может реализоваться угроза

Обучение
информационной
безопасности



Защита информации и информационное общество



Система защиты — комплекс средств и методов, а также деятельность на их основе, направленная на выявление, отражение и ликвидацию различных видов угроз безопасности объекта защиты

Техническая защита информации (ТЗИ) — это комплекс мероприятий, направленных на предотвращение утечки защищаемой информации по техническим каналам, на предотвращение несанкционированного доступа к ней, ее модификации, искажения, копирования, блокирования или уничтожения по техническим каналам (ТКУИ), от несанкционированного доступа (НСД)

Обучение
информационной
безопасности



Технические средства защиты информации



Технические средства защиты информации — это устройства, которые обеспечивают безопасность информации при помощи аппаратных средств, поэтому их еще называют аппаратными средствами защиты

Основные технические средства и системы (ОТСС) — технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации

Вспомогательные технические средства и системы (ВТСС) — технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации, размещаемые совместно с ОТСС или в ЗП **в рамках помещения**

Средства обработки информации — любые системы, службы или инфраструктуры по обработке информации

Обучение
информационной
безопасности



Информационные системы



Информационная система (ИС) — совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств

Автоматизированная система (АС) — система, состоящая из персонала, комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций и сведений о составе и расположении этой системы

Информационная система персональных данных (ИСПДн) — совокупность сведений, содержащихся в базах персональных данных, и обеспечивающих их обработку информационных технологий и технических средств

Государственные информационные системы (ГИС) — федеральные информационные системы и региональные информационные системы, созданные соответственно на основании федеральных законов, законов субъектов Российской Федерации, правовых актов государственных органов

Информационные системы общего пользования (ИСОП) – федеральные государственные ИС, созданные или используемые в целях реализации полномочий федеральных органов исполнительной власти и содержащие сведения о деятельности Правительства РФ и федеральных органов исполнительной власти, обязательные для размещения в информационно-телекоммуникационной сети Интернет, определяемые Правительством РФ

Обучение
информационной
безопасности



Защита информации



Физическая защита информации — защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты

Правовая защита — защита информации правовыми методами, включающая в себя разработку нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением

Обучение
информационной
безопасности



Законодательные и организационные средства



Законодательные средства — законы всех уровней и другие нормативно-правовые акты, с помощью которых регламентируются правила использования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил. Распространяются на всех субъектов информационных отношений. В настоящее время отношения в сфере информационной безопасности регулируются более чем 80 законами и нормативными документами.

Организационные средства — организационно-технические и организационно-правовые мероприятия, осуществляемые в течение всего жизненного цикла защищаемой информационной системы: строительство помещений, проектирование информационных систем, монтаж и наладка оборудования, испытания и эксплуатация информационных систем. Другими словами, это средства уровня организации, регламентирующие перечень лиц, оборудования, материалов и т.д., имеющих отношение к информационным системам, а также режимов их работы и использования. К организационным мерам также относят сертификацию информационных систем или их элементов, аттестацию объектов и субъектов на выполнение требований обеспечения безопасности, реализацию требований по сертификации и оценке соответствия требованиям по обработке и/или защите информации

Морально-этические нормы — сложившиеся в обществе или в данном коллективе моральные нормы или этические правила, соблюдение которых способствует защите информации, а нарушение приравнивается к несоблюдению правил поведения в обществе или коллективе, ведет к потере престижа и авторитета

Обучение
информационной
безопасности



Законодательные и организационные средства



Законодательные средства — законы всех уровней и другие нормативно-правовые акты, с помощью которых регламентируются правила использования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил. Распространяются на всех субъектов информационных отношений.

Организационные средства — организационно-технические и организационно-правовые мероприятия, осуществляемые в течение всего жизненного цикла защищаемой информационной системы: строительство помещений, проектирование информационных систем, монтаж и наладка оборудования, испытания и эксплуатация информационных систем. Другими словами, это средства уровня организации, регламентирующие перечень лиц, оборудования, материалов и т.д., имеющих отношение к информационным системам, а также режимов их работы и использования. К организационным мерам также относят сертификацию информационных систем или их элементов, аттестацию объектов и субъектов на выполнение требований обеспечения безопасности, реализацию требований по сертификации и оценке соответствия требованиями по обработке и/или защите информации

Морально-этические нормы — сложившиеся в обществе или в данном коллективе моральные нормы или этические правила, соблюдение которых способствует защите информации, а нарушение приравнивается к несоблюдению правил поведения в обществе или коллективе, ведет к потере престижа и авторитета

Обучение
информационной
безопасности



ФЗ, указы и ПП в сфере информационной безопасности



Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».

Федеральный закон от 29.06.2015 № 162-ФЗ «О стандартизации в Российской Федерации»

Федеральный закон от 24.06.2025 № 156-ФЗ "О создании многофункционального сервиса обмена информацией и о внесении изменений в отдельные законодательные акты Российской Федерации"

изменил правила оформления согласия на обработку ПД.

С 1 сентября 2025 года согласие на обработку ПД должно оформляться **отдельно от иных документов и информации**, которые субъект подтверждает или подписывает

Обучение
информационной
безопасности



ФЗ, указы и ПП в сфере информационной безопасности



Указ Президента РФ от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера»

В перечень входят, в частности, персональные данные — сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность

Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»

Стратегический документ. Не является непосредственным основанием для разработки локального положения о ПД, например, ОО

Указ Президента РФ от 22.05.2015 № 260 «О некоторых вопросах информационной безопасности Российской Федерации»

Обучение
информационной
безопасности



ФЗ, указы и ПП в сфере информационной безопасности



Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

Это особенно полезно для ОО, потому что неавтоматизированная обработка — это бумажные анкеты; заявления; личные дела; бумажные списки; журналы; карточки; документы на бумаге

Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации...»

Он применяется именно тогда, когда используются средства криптографической защиты информации

Обучение
информационной
безопасности



ФЗ, указы и ПП в сфере информационной безопасности



Приказ Роскомнадзора от 28.10.2022 № 180

Он утверждает формы:

- уведомления о намерении осуществлять обработку ПД;
- уведомления об изменении сведений;
- уведомления о прекращении обработки.

Приказ Роскомнадзора от 28.10.2022 № 179

Причём при автоматизированной обработке подтверждением являются:

- акт об уничтожении;
- выгрузка из журнала регистрации событий.

Эти документы должны храниться **3 года с момента уничтожения ПД.**

Обучение
информационной
безопасности



ФЗ, указы и ПП в сфере информационной безопасности



ГОСТ Р ИСО 7498-2-99 — архитектура защиты информации;

ГОСТ Р 50739-95 — защита от НСД;

ГОСТ Р 50922-2006 — термины и определения;

ГОСТ Р 52069.0-2013 — система стандартов защиты информации;

ГОСТ Р 51275-2006 — объект информатизации и факторы воздействия;

ГОСТ Р 59710-2022 — управление компьютерными инцидентами;

ГОСТ Р 58771-2019 — технологии оценки риска;

ГОСТ 34.10-2018 — ЭП;

ГОСТ 34.11-2018 — хэширование;

ГОСТ 34.12-2018 — блочные шифры;

ГОСТ 34.13-2018 — режимы работы блочных шифров

Обучение
информационной
безопасности



Цели информационной защиты



Цель информационной безопасности связана с тремя основными свойствами информации: конфиденциальность, целостность, доступность. Основная цель информационной безопасности — **обеспечение конфиденциальности, целостности и доступности информации.**

Три основных типа контроля

Физический контроль. Обеспечивается мониторинг рабочих мест сотрудников, вычислительной техники, бытового оборудования (кондиционные и отопительные системы, пожарные и дымовые сигнализации, видеонаблюдение, замки, двери и т.д.).

Логический контроль. Используются технические средства контроля, которые формируют условия для защиты доступа к информационным системам. В логический контроль входит множество составляющих элементов: программное обеспечение для защиты информационных систем, пароли на доступ, межсетевые экраны и т.д.

Административный контроль. Реализуется комплекс мер, стандартов, процедур, которые утверждены на предприятии. С их помощью формируются определенные в первую очередь юридические границы, в рамках которых ведется бизнес и управление сотрудниками. К административному контролю информационной безопасности также относятся законодательные и нормативные акты, которые приняты государством и профильными регуляторами, отраслевые стандарты, договоры с контрагентами.

Обучение
информационной
безопасности



Цели информационной защиты



Одной из важных целей информационной безопасности является ликвидация угроз. Угрозы информационной безопасности можно условно разделить на несколько отдельных групп:

Техногенные. Угрозы, которые формируются из-за проблем в техническом обеспечении и средствах защиты. Их прогнозирование является крайне проблематичным и сложным.

Антропогенные. Угрозы, возникающие из-за человеческих ошибок, действий или бездействия. В эту категорию включены как намеренные, так и ненамеренные ошибки, допущенные человеком. К непреднамеренным относят случайные ошибки, например отключение антивирусных программ по незнанию. Антропогенные проблемы могут быть спрогнозированы. Также иногда есть возможность быстро устранить вызванные ими последствия. Намеренные действия по нарушению работы систем и сервисов — это информационные преступления.

Стихийные. Угрозы, вызванные стихийными источниками, обладают малой вероятностью прогнозирования, потому что их предотвращение видится невозможным (пожары, землетрясения, наводнения, отключение электричества из-за стихийных бедствий и т.д.).

Вся работа систем безопасности сведена к формированию безопасных каналов связи, защите серверов, обеспечению безопасности внешних носителей и рабочих мест сотрудников.

Обучение
информационной
безопасности



Задачи информационной безопасности



Задачи информационной безопасности:

- обеспечение защищенного хранения информации на носителях;
- защита данных, передаваемых по каналам связи;
- создание резервных копий, послеаварийное восстановление и т.д.

Задачи отдела, который занимается информационной безопасностью:

- разработка комплексной системы безопасности, включающей использование разнообразных методов и способов защиты конфиденциальной информации от намеренного и ненамеренного разглашения, утери, искажения, кражи;
- введение режима конфиденциальности и контроль за его соблюдением, разграничение доступа к данным и информационным системам. Выдача минимально достаточных прав пользователям, аудит всех действий, связанных с правами и доступами учетных записей, корректировка прав доступа при смене должности, увольнении, переводе и т.д.;
- взаимодействие с контрагентами в части информационной безопасности, обеспечение конфиденциальности передачи данных и информации, сообщаемой партнерам, клиентам и государственным органам в процессе переговоров;
- разработка документов, предписывающих соблюдение режима конфиденциальности штатными сотрудниками организации и прикомандированными работниками;
- мониторинг действий сотрудников: фиксация рабочих сессий, анализ активности, использования и перемещения данных, предотвращение подозрительных операций и др.

Обучение
информационной
безопасности



Важность информационной безопасности



Сейчас резко возросло число кибератак. Часто взломы совершаются не ради выкупа, а чтобы нанести максимальный ущерб компаниям и их клиентам. По данным аналитической компании InfoWatch, ежегодно утекает больше 667 млн записей с информацией о пользователях российских сервисов.

Информационная безопасность защищает системы от проникновения и от атак. Сюда входит не только взлом, это и DDoS-атаки, в результате которых может «лечь» сервер сайта, и утечка данных. Злоумышленников с каждым годом становится все больше. И никто не хочет, чтобы их сервис потерял работоспособность, а данные оказались доступны всем вокруг. Для этого и нужна информационная безопасность.

У компаний есть еще одна причина задуматься о безопасности данных: за утечку конфиденциальных данных пользователей они несут ответственность по закону, поэтому меры по безопасности — это еще и способ избежать проблем с законодательством и потери доверия клиентов.

Без мер по информационной безопасности кто угодно мог бы получить доступ к конфиденциальным сведениям или взломать любой сайт или систему.

Компьютерным пространством стало бы фактически невозможно пользоваться.

Обучение
информационной
безопасности



Информационная безопасность организации



Это комплекс мероприятий, направленных на предотвращение несанкционированного доступа к внутренней IT-инфраструктуре, незаконного завладения конфиденциальной информацией и внесения изменений в базы данных, то есть в информационную безопасность входит защита от злоумышленников данных в электронной форме и на физических носителях

В большинстве случаев краже подлежат следующие данные:

- информация о реальном финансовом состоянии компании
- инновационные разработки научно-технических отделов
- регистрационные данные сотрудников и пользователей
- исходный код и документация на разрабатываемые системы и сервисы

Обучение
информационной
безопасности



Виды ответственности за нарушения ИБ



Уголовная ответственность

Преступления в сфере компьютерной информации (гл. 28): неправомерный доступ к компьютерной информации (ст. 272), создание, использование и распространение вредоносных программ для ЭВМ (ст. 273) и нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274)

Административная ответственность

За нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) (ст. 13.11) и правил защиты информации (ст. 13.12); незаконную деятельность в области защиты информации (ст. 13.13); разглашение информации с ограниченным доступом (ст. 13.14)

Обучение
информационной
безопасности



Виды ответственности за нарушения ИБ



Гражданско-правовая ответственность

В п. 2 ст. 139 ГК РФ закреплено, что информация, составляющая служебную или коммерческую тайну, защищается способами, предусмотренными настоящим Кодексом и другими законами

Лица, незаконными методами получившие информацию, которая составляет служебную или коммерческую тайну, обязаны возместить причиненные убытки.

Такая же обязанность возлагается на работников, разгласивших служебную или коммерческую тайну вопреки трудовому договору, в том числе контракту, и на контрагентов, сделавших это вопреки гражданско-правовому договору

Обучение
информационной
безопасности



Виды ответственности за нарушения ИБ



Дисциплинарная ответственность

За правонарушения в информационной сфере предусмотрена и материальная ответственность – это имущественная ответственность работников, по вине которых предприятие, учреждение, организация понесли расходы по возмещению вреда, причиненного информационным правонарушением

разд. XI Трудового кодекса РФ

Обучение
информационной
безопасности



Типы нарушителей безопасности информации



Физическое лицо (субъект), случайно или преднамеренно совершившее действия (бездействия), следствием которых является нарушение безопасности информации при ее обработке техническими средствами в информационных системах

- ❖ Бывшие/действующие сотрудники
- ❖
- ❖ Криминальные/преступные организации
- ❖
- ❖ Разработчики, производители ПО
- ❖
- ❖ Хакерские группировки
- ❖
- ❖ Конкуренты
- ❖
- ❖ Террористические организации

Обучение
информационной
безопасности



Виды аудита информационной безопасности



Виды аудита информационной безопасности

Внутренний аудит проводят на регулярной основе силами самой компании и в соответствии с согласованными внутри организации требованиями

Внешний аудит проводят независимые, привлеченные со стороны эксперты, выполняющие работу в соответствии с договором

Методы аудита

Инструментальный аудит (пентест) — поиск максимально возможного числа уязвимостей и векторов атак за ограниченный промежуток времени

Аудит на соответствие стандартам — сравнение характеристик информационной безопасности компании с требованиями конкретных стандартов

Комплексный аудит — сочетание методик, дающее всестороннюю оценку, но отнимающее больше времени и ресурсов

Обучение
информационной
безопасности



Типы контроля информационной безопасности



Выбор и внедрение подходящих видов контроля безопасности поможет организации снизить риск до приемлемых уровней

Виды контроля:

Административный. Состоит из утвержденных процедур, стандартов и принципов. Он формирует рамки для ведения бизнеса и управления людьми. Законы и нормативные акты, созданные государственными органами, также являются одним из видов административного контроля. Другие примеры административного контроля включают политику корпоративной безопасности, паролей, найма и дисциплинарные меры.

Логический. Логические средства управления, также называемые техническими средствами контроля, базируются на защите доступа к информационным системам, программном обеспечении, паролях, брандмауэрах, информации для мониторинга и контроле доступа к системам информации.

Физический. Это контроль среды рабочего места и вычислительных средств: отопление и кондиционирование воздуха, дымовые и пожарные сигнализации, противопожарные системы, камеры, баррикады, ограждения, замки, двери и др.

Обучение
информационной
безопасности



Внутренние документы для защиты ИБ



1. Положения:

- о защите персональных данных и конфиденциальных сведений;
- о правилах пользования внутренней информационной сетью, использования интернет-ресурсов.

2. Распоряжения:

- о назначении ответственных лиц по обеспечению безопасности обработки персональных данных;
- о правилах хранения электронных и бумажных носителей ценных сведений, определения порядка допуска к ним;
- о создании комиссии, которая занимается классификацией системы и присваивает ей соответствующий класс защиты.

3. Должностные инструкции специалистов, ответственных за программное обеспечение, работу технических средств, контролирующих доступность сведений.

4. Модель угроз безопасности информации, составленную на основе анализа.

5. Утвержденный список лиц с доступом к информации, имеющей критическое значение.

Обучение
информационной
безопасности



Внутренние документы для защиты ИБ



6. Правила:

- проведения процедуры идентификации пользователей;
- установки (инсталляции) программного обеспечения;
- резервирования баз данных, их восстановления при возникновении нештатных ситуаций.

7. Формы журналов учета:

- приема/выдачи съемных носителей данных;
- технических средств для обработки и передачи информации;
- проведения инструктажей по вопросам защиты данных, безопасного пользования персональными компьютерами;
- тестирования средств, обеспечивающих конфиденциальность, защиту информации;
- плановых мероприятий, проводимых с целью предотвращения хищений, несанкционированного доступа к секретной информации, выявления потенциальных угроз.

ЛНА по обработке, использованию и хранению персональных данных (на основе Федерального закона № 152-ФЗ) и по использованию криптографических средств защиты информации.

Обучение
информационной
безопасности



Практические задания



Кейс 1

Компании, которые занимаются предоставлением товаров и услуг, незаконным способом покупают персональные данные, чтобы расширить базу потенциальных клиентов. Это могут быть ФИО, номер телефона, адрес электронной почты. На такой спрос есть и предложение.

Так, сотрудник одной организации искал способы дополнительного заработка и продавал третьим лицам персональные данные.

Обучение
информационной
безопасности



Практические задания



Решение

Компании должны следить за своими информационными базами. Должен быть организован контроль за распространением персональных данных, контроль доступа к ним.

Служба информационной безопасности должна следить за действиями сотрудников с карточками клиентов, и, в случае если кто-то из сотрудников копирует всю базу, необходимо провести служебное расследование, потребовать у сотрудника докладную записку — для каких целей копировались данные.

Кроме того, должно быть организовано раздельное хранение информационных баз: ФИО отдельно, паспортные данные, ИНН, юридические адреса отдельно. И только у ограниченного круга сотрудников должен быть доступ к единой базе (разграничение доступа).

Обучение
информационной
безопасности



Практические задания



Кейс 2

В сетевой отель X пришли с проверкой прокуратура и ФСБ России по анонимной жалобе, в которой говорилось, что сотрудники отеля собирают персональные данные без согласия на обработку и неправильно их хранят: копии паспортов остаются на стойке регистрации, есть опасения утечки данных (такие жалобы могут поступать как посетителей отеля, так и от конкурентов).

При проверке были выявлены нарушения Федерального закона №152, а именно нарушения по требованиям к соблюдению мер безопасности персональных данных при их обработке с использованием средств криптографической защиты информации. Выписали предписание и штраф.

Обучение
информационной
безопасности



Практические задания



Решение

Провести обследование процессов обработки персональных данных, получить рекомендации по устранению всех нарушений Федерального закона №152-ФЗ и всех подзаконных актов.

Разработать организационно-распорядительные документы, которые также регламентируют работу и хранение средств криптографической защиты информации.

Обучение
информационной
безопасности



Практические задания



Кейс 3

Организация X не считает себя оператором персональных данных, т.к. обрабатывает персональные данные только своих сотрудников, а персональные данные клиентов обрабатывает «тайно». По этой же логике организация X не подавала уведомление об обработке персональных данных в Роскомнадзор и не была включена в Реестр операторов персональных данных.

Права ли Организация X? И нужно ли в таком случае подавать Уведомление об обработке персональных данных в Роскомнадзор?

Обучение
информационной
безопасности



Практические задания



Решение

Провести обследование процессов обработки персональных данных. Определить цели, субъекты, обработки, информационные системы и прочее. Выполнить базовый перечень мероприятий, подать уведомление в Роскомнадзор.

Обучение
информационной
безопасности



Порядок создания системы защиты данных



Система защиты информации – это совокупность органов и исполнителей, используемой ими техники защиты информации, а также объектов защиты, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации

В организационную структуру системы входят:

- руководитель, который несет персональную ответственность за обеспечение информационной безопасности (устав организации, положение об органе)
- заместитель руководителя, курирующий вопросы информационно-технической безопасности (должностной регламент)
- постоянно действующий коллегиальный орган, вырабатывающий предложения по решению проблемных вопросов в области защиты информации (положение о комиссии)

Обучение
информационной
безопасности



Порядок создания системы защиты данных



- подразделение или специалист, ответственные за реализацию мероприятий по технической защите информации (положение о подразделении, должностная инструкция или регламент специалиста)
- подразделение или специалист, ответственные за реализацию мероприятий по криптографической защите информации (положение о подразделении, должностная инструкция или регламент специалиста)

Обучение
информационной
безопасности



Этапы создания системы защиты данных



1. Формирование требований к системе защиты информации (предпроектный этап)
2. Разработка системы защиты информации (этап проектирования)
3. Внедрение системы защиты информации (этап установки, настройки, испытаний)
4. Подтверждение соответствия системы защиты информации (этап оценки)

Обучение
информационной
безопасности



Важные термины и определения



Обладатель информации – лицо, создавшее информацию и (или) имеющее право разрешать или ограничивать доступ к информации

Заказчик – лицо, заключившее контракт на создание объекта обработки информации

Оператор – лицо, эксплуатирующее объект, в том числе непосредственно осуществляющее обработку содержащейся в нем информации

Уполномоченное лицо – лицо, осуществляющее на договорной основе с заказчиком или оператором обработку информационного ресурса и (или) предоставляющее для этих целей вычислительные ресурсы.

Поставщик информации – лицо, наделенное полномочиями по предоставлению сведений для их внесения в базу данных объекта

Обучение
информационной
безопасности



Методики управления рисками



Комплексный подход к оценке рисков (CCTA Risk Analysis and Management Method) – в основе метода лежит комплексный подход к оценке рисков, сочетающий количественные и качественные методы анализа

Исследование информационной безопасности системы с помощью метода CRAMM проводится в несколько этапов:

Инициирование (Initiation)

Идентификация и оценка IT-активов (Identification and Valuation of Assets).

Оценка производится по десятибалльной шкале, причем критериев оценки может быть несколько: финансовые потери, потери репутации и т.д. В описаниях CRAMM в качестве примера приводится шкала оценки по критерию «Финансовые потери, связанные с восстановлением ресурсов»

Обучение
информационной
безопасности



Методики управления рисками



Оценка угроз и уязвимостей (Threat and Vulnerability Assessment)

В дополнение к оценке критичности IT-активов важной частью методологии CRAMM является оценка вероятности угроз и уязвимостей IT-активов

Вычисление риска (Risk Calculation)

Вычисление риска производится по формуле: $\text{Риск} = P(\text{реализации}) \times \text{Ущерб}$

При этом вероятность реализации риска вычисляется по формуле:

$P(\text{реализации}) = P(\text{угрозы}) * P(\text{уязвимости})$

На этапе вычисления рисков для каждого IT-актива определяются требования к набору мер по обеспечению его информационной безопасности по шкале от 1 до 7, где значению 1 соответствует минимальный необходимый набор мер по обеспечению информационной безопасности, а значению 7 – максимальный

Управление риском (Risk Management)

На основе результатов вычисления риска методология CRAMM определяет необходимый набор мер по обеспечению информационной безопасности

Обучение
информационной
безопасности



Методология COBIT of Risk



Каждый рисковый сценарий содержит следующую информацию:

- тип источника угрозы – внутренний/внешний
- тип угрозы – злонамеренное действие, природное явление, ошибка и др.
- описание события – доступ к информации, уничтожение, внесение изменений, раскрытие информации, кража и др.
- типы активов (компонентов) организации, на которые влияет событие, – люди, процессы, IT-инфраструктура и др.
- время события

Обучение
информационной
безопасности



Методология COBIT of Risk



Каждый рисковый сценарий содержит следующую информацию:

- тип источника угрозы – внутренний/внешний
- тип угрозы – злонамеренное действие, природное явление, ошибка и др.
- описание события – доступ к информации, уничтожение, внесение изменений, раскрытие информации, кража и др.
- типы активов (компонентов) организации, на которые влияет событие, – люди, процессы, IT-инфраструктура и др.
- время события

Обучение
информационной
безопасности



Виды тайн и их особенности



Законодательство также регулирует защиту различных видов тайн, каждая из которых требует специальных мер по защите данных. Основные виды тайн:

- **Государственная тайна.** Этот вид тайны включает информацию, связанную с национальной безопасностью и государственными секретами. Примером может служить информация о военных операциях, оборонных системах, стратегических объектах или внешнеполитических планах. Защита государственной тайны предполагает высокие стандарты безопасности и строгое соблюдение правил обращения с такими данными. Например, для передачи секретных данных могут использоваться системы с повышенным уровнем шифрования и контроля доступа.
- **Коммерческая тайна.** Коммерческая тайна касается информации, имеющей высокую ценность для бизнеса, таких как производственные секреты, данные о клиентах, партнерах и стратегии компании. Защита коммерческой тайны важна для сохранения конкурентных преимуществ компании на рынке. Законодательство обязывает компании обеспечивать защиту этой информации, внедряя специальные меры, такие как шифрование, контроль доступа и обучение сотрудников правилам работы с конфиденциальной информацией.

Обучение
информационной
безопасности



Виды тайн и их особенности



- **Профессиональная тайна.** Этот вид тайны включает информацию, которую обязаны защищать представители определенных профессий. Например, врачебная тайна обязует медицинские учреждения защищать данные пациентов, юридическая тайна защищает данные клиентов адвокатов, а банковская тайна касается информации о банковских счетах клиентов. Нарушение профессиональной тайны может привести к серьезным юридическим последствиям, включая потерю доверия клиентов и судебные иски.

- **Служебная тайна.** Этот вид тайны касается сведений, не составляющих государственную тайну, но распространение которых запрещено или ограничено в соответствии с законодательством и внутренними документами организации. Нарушение служебной тайны может привести к утечке конфиденциальной информации и нанести ущерб компании, включая потерю конкурентных преимуществ.

Обучение
информационной
безопасности



Ограничительные пометки и грифы секретности



Для обозначения уровня секретности и регулирования доступа к информации используются специальные ограничительные пометки и грифы секретности. Они помогают классифицировать информацию по уровню ее важности и степени необходимости защиты

- **Ограничительные пометки**, такие как «Для служебного пользования» (ДСП). Эта пометка обозначает, что информация предназначена только для внутреннего использования в компании или системе и не может быть передана сторонним лицам без соответствующего разрешения
- **Гриффы секретности**, такие как «Секретно» и «Совершенно секретно». Эти гриффы используются для обозначения уровня секретности информации и устанавливают специальные правила обращения с такими данными. Например, документы с грифом «Совершенно секретно» требуют особого контроля доступа, их передача осуществляется через защищенные каналы связи, а физический доступ к ним ограничен только определенными лицами

Эти пометки и гриффы играют важную роль в системе защиты информации, так как они помогают регулировать доступ к данным и предотвращать их утечку или неправомерное использование

Обучение
информационной
безопасности



Практические задания



Задание 1. Анализ последствий утечки данных

Описание задания

Представьте, что крупная компания столкнулась с утечкой персональных данных о клиентах и партнерах. На основе информации из конспекта, опишите три основные категории последствий (финансовые потери, утрата репутации и юридические последствия), которые могут возникнуть в результате утечки

Приведите примеры конкретных ситуаций для каждой категории

Ожидаемый результат

1. Описание финансовых потерь, включая убытки от компенсаций или штрафов.
2. Анализ последствий для репутации, включая снижение доверия клиентов.
3. Указание юридических последствий, таких как штрафы и уголовная ответственность.

Обучение
информационной
безопасности



Практические задания



Задание 2. Разработка политики информационной безопасности

Описание задания

Вам поручено разработать краткий план создания информационной безопасности для небольшой компании. Используя информацию из конспекта, опишите основные технические, организационные и правовые меры, которые вы бы внедрили для защиты данных.

Включите примеры конкретных решений, таких как шифрование, обучение сотрудников и соблюдение законодательства.

Ожидаемый результат

1. Перечисление технических мер (например, антивирусы, межсетевые экраны).
2. Описание организационных мер (например, контроль доступа, обучение персонала).
3. Указание правовых мер (соблюдение ФЗ № 152-ФЗ, GDPR, внутренние политики).

Обучение
информационной
безопасности



Практические задания



Задание 3. Влияние информационного общества на бизнес

Описание задания

Опишите, как переход к информационному обществу влияет на ведение бизнеса в условиях цифровизации и глобализации. Обратите внимание на важность управления данными и их защиты.

Как компаниям удаётся получать конкурентные преимущества за счет внедрения систем управления информацией? Приведите примеры из конспекта или из реальных ситуаций. Приведите пример компании, которая можно обходиться без информационных технологий в электронном виде для своей деятельности.

Ожидаемый результат

1. Описание ключевой роли информации в современном бизнесе.
2. Примеры внедрения систем управления информацией и их влияние на конкурентоспособность.
3. Выводы о значении защиты данных для успешной работы компании.

Обучение
информационной
безопасности



Защита персональных данных



Обучение
информационной
безопасности



Защита персональных данных



Федеральный закон № 152-ФЗ "О персональных данных"

Основные положения закона включают:

- **Принципы обработки персональных данных.** Обработка должна осуществляться на законной и справедливой основе, с соблюдением принципов прозрачности, ограничения цели, минимизации данных, точности, ограничения срока хранения, целостности и конфиденциальности.
- **Правовые основания обработки.** Обработка персональных данных допускается только при наличии законных оснований, таких как согласие субъекта, исполнение договора, выполнение обязательств оператора, предусмотренных законодательством.
- **Права субъектов персональных данных.** Закон предоставляет гражданам право на получение информации об обработке их персональных данных, право требовать уточнения, блокирования или уничтожения данных, а также право на судебную защиту своих прав.
- **Обязанности операторов.** Операторы обязаны обеспечивать безопасность персональных данных, принимать необходимые организационные и технические меры для предотвращения несанкционированного доступа, а также соблюдать требования законодательства при передаче данных третьим лицам.
- **Трансграничная передача данных.** Устанавливаются условия для передачи персональных данных за пределы Российской Федерации, в том числе требования к обеспечению надлежащего уровня защиты данных в принимающей стране.

Обучение
информационной
безопасности



Требования к обработке и хранению персональных данных



- 1. Законность и справедливость обработки.** Обработка должна осуществляться на законных основаниях и не нарушать права и свободы субъектов персональных данных.
- 2. Определение конкретных целей обработки.** Персональные данные должны собираться для конкретных, заранее определённых и законных целей. Их дальнейшая обработка должна соответствовать этим целям и не выходить за их рамки.
- 3. Минимизация данных.** Обрабатываемые персональные данные должны быть ограничены необходимым минимумом, достаточным для достижения целей обработки.
- 4. Точность данных.** Операторы обязаны обеспечивать точность, полноту и актуальность персональных данных. При выявлении неточных или неполных данных они должны быть исправлены или дополнены.
- 5. Ограничение срока хранения.** Персональные данные должны храниться не дольше, чем этого требуют цели их обработки. По достижении целей данные должны быть уничтожены или обезличены.
- 6. Обеспечение безопасности данных.** Операторы обязаны принимать необходимые организационные и технические меры для защиты персональных данных.
- 7. Прозрачность обработки.** Субъекты персональных данных должны быть информированы об обработке их данных, включая информацию о целях, способах, правах и обязанностях операторов.

Обучение
информационной
безопасности



Требования к обработке и хранению персональных данных



Права субъектов персональных данных:

- **Право на информацию.** Граждане имеют право получать от операторов информацию об обработке своих персональных данных.
- **Право на доступ к данным.** Субъекты могут требовать предоставления копий своих персональных данных в доступной форме.
- **Право на уточнение, блокирование или уничтожение данных.** При выявлении неточных или незаконно обрабатываемых данных граждане имеют право требовать их исправления, блокирования или уничтожения.
- **Право на отзыв согласия.** Если обработка данных осуществляется на основании согласия, субъект может в любой момент отозвать его.
- **Право на судебную защиту и обращение в надзорные органы.** В случае нарушения своих прав граждане могут обратиться в Роскомнадзор или в суд.

Обучение
информационной
безопасности



Требования к обработке и хранению персональных данных



Обязанности операторов:

- **Соблюдение принципов обработки.** Операторы обязаны действовать в соответствии с принципами законности, справедливости и прозрачности.
- **Получение согласия.** При необходимости операторы должны получать информированное и добровольное согласие субъектов на обработку их персональных данных.
- **Информирование субъектов.** Операторы должны предоставлять субъектам информацию об обработке их данных, правах и способах защиты этих прав.
- **Обеспечение безопасности данных.** Принятие необходимых мер по защите данных от угроз безопасности.
- **Уведомление надзорного органа.** В определённых случаях операторы обязаны уведомлять Роскомнадзор о своём намерении обрабатывать персональные данные.
- **Назначение ответственного лица.** Операторы должны назначить ответственного за организацию обработки персональных данных и обеспечение их безопасности.
- **Соблюдение требований при передаче данных третьим лицам.** Операторы обязаны обеспечивать, чтобы третьи лица, получающие персональные данные, соблюдали требования законодательства.

Обучение
информационной
безопасности



Административная ответственность



КоАП РФ, статья 13.11 — нарушение законодательства в области персональных данных

Наиболее важные для организации случаи:

- **Обработка ПД без законного основания или с нарушением целей обработки**
ч. 1 ст. 13.11:
должностные лица — 50 000–100 000 руб.;
юридические лица — 150 000–300 000 руб.
- **Обработка ПД без письменного согласия**, когда оно обязательно, либо с нарушением требований к содержанию согласия
ч. 2 ст. 13.11:
должностные лица — 100 000–300 000 руб.;
юридические лица — 300 000–700 000 руб.
- **Неуведомление или несвоевременное уведомление Роскомнадзора о намерении осуществлять обработку ПД**
ч. 10 ст. 13.11:
должностные лица — 30 000–50 000 руб.;
юридические лица — 100 000–300 000 руб.

Обучение
информационной
безопасности



Административная ответственность



КоАП РФ, статья 13.11 — нарушение законодательства в области персональных данных

- **Неуведомление Роскомнадзора об инциденте с ПД**, повлекшем нарушение прав субъектов
ч. 11 ст. 13.11:
должностные лица — **400 000–800 000 руб.**;
юридические лица — **1–3 млн руб.**
- За неправомерную передачу или доступ к ПД также предусмотрены **существенно более высокие штрафы**, размер которых зависит, в частности, от количества субъектов, вида данных и характера нарушения (**ч. 12–18 ст. 13.11**).

Статья 13.12 КоАП РФ — нарушение правил защиты информации

Применяется при нарушении установленных требований к защите информации. Например, **ч. 6 ст. 13.12** предусматривает штраф для должностных лиц **10 000–50 000 руб.**, для юридических лиц — **50 000–100 000 руб.**

Обучение
информационной
безопасности



Уголовная ответственность



Статья 137 УК РФ — нарушение неприкосновенности частной жизни

Ответственность наступает, в частности, за незаконное собирание или распространение сведений о частной жизни, составляющих личную или семейную тайну.

- **ч. 1:** штраф — до **200 000 руб.**, а также возможны другие виды наказания, вплоть до лишения свободы на срок до **2 лет**.
- **ч. 2:** если деяние совершено, например, **с использованием служебного положения**, — штраф **100 000–300 000 руб.** либо иные виды наказания, вплоть до лишения свободы на срок до **4 лет**.

Статья 272 УК РФ — неправомерный доступ к компьютерной информации

Предусматривает ответственность за неправомерный доступ к охраняемой законом компьютерной информации, если он повлек её уничтожение, блокирование, модификацию или копирование.

Важно: для незаконных действий именно с компьютерной информацией, содержащей персональные данные, в УК РФ также предусмотрена **статья 272.1**.

Обучение
информационной
безопасности



Примеры нарушений требований к персональным данным



1. Крупная IT-компания — нарушение требований локализации

В 2020 году Роскомнадзор привлёк к ответственности крупную международную IT-компанию за отказ локализовать персональные данные граждан РФ на серверах, расположенных на территории России.

Штраф — 4 млн рублей.

2. Банковский сектор — недостаточная защита данных

Российский банк был привлечён к ответственности за ненадлежащие меры защиты персональных данных клиентов, что сопровождалось **утечкой информации**.

3. Образовательная организация — незаконное распространение данных учащихся

Школа получила штраф за распространение персональных данных учащихся **без надлежащего согласия родителей (законных представителей)**.

Обучение
информационной
безопасности



Примеры нарушений требований к персональным данным



1. Крупная IT-компания — нарушение требований локализации

В 2020 году Роскомнадзор привлёк к ответственности крупную международную IT-компанию за отказ локализовать персональные данные граждан РФ на серверах, расположенных на территории России.

Штраф — 4 млн рублей.

2. Банковский сектор — недостаточная защита данных

Российский банк был привлечён к ответственности за ненадлежащие меры защиты персональных данных клиентов, что сопровождалось **утечкой информации**.

3. Образовательная организация — незаконное распространение данных учащихся

Школа получила штраф за распространение персональных данных учащихся **без надлежащего согласия родителей (законных представителей)**.

Обучение
информационной
безопасности



Определение персональных данных



Персональные данные (ПД) — любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу — субъекту персональных данных (*ст. 3 Федерального закона № 152-ФЗ*)

К персональным данным могут относиться, например:

- **Идентификационные данные:** ФИО, дата и место рождения, паспортные данные, ИНН, СНИЛС.
- **Контактные данные:** адрес, номер телефона, адрес электронной почты.
- **Сведения об образовании и трудовой деятельности:** образование, профессия, должность, место работы.
- **Семейные и социальные сведения:** семейное положение, сведения о составе семьи и другие данные, позволяющие идентифицировать человека.
- **Финансовые сведения:** данные о банковских счетах, доходах, кредитной истории и др.
- **Сведения о здоровье:** диагнозы, состояние здоровья, медицинские процедуры и иная информация о состоянии здоровья. *Для таких данных действуют специальные правила обработки.*
- **Биометрические персональные данные:** сведения о физиологических и биологических особенностях человека, например изображение лица или голос в соответствующем контексте.

Обучение
информационной
безопасности



Определение персональных данных



Важно

152-ФЗ не устанавливает закрытый перечень персональных данных.

Информация является персональными данными, если она позволяет прямо или косвенно определить конкретного человека.

Обучение
информационной
безопасности



Организация работы по защите персональных данных



Проведение аудита текущих процессов

Первым шагом в организации работы по защите персональных данных является проведение комплексного аудита текущих процессов обработки и защиты данных. Цель аудита — выявление:

- **Перечня персональных данных, обрабатываемых в организации.**
- **Текущих методов и средств обработки данных, включая используемые информационные системы и базы данных.**
- **Уровня соответствия действующему законодательству и внутренним нормативным документам.**
- **Уязвимостей и рисков, связанных с возможными нарушениями в сфере защиты данных.**

Аудит позволяет получить полное представление о состоянии дел в организации, определить слабые места и разработать план действий по их устранению.

Обучение
информационной
безопасности



Организация работы по защите персональных данных



При проведении аудита рекомендуется:

- **Составить опросные листы для различных подразделений**, чтобы собрать информацию о том, какие данные обрабатываются, как они хранятся и передаются.
- **Провести интервью с ключевыми сотрудниками**, ответственными за обработку и защиту данных.
- **Оценить техническую инфраструктуру**, включая программное обеспечение, сетевое оборудование и системы безопасности.
- **Проанализировать существующие документы и процедуры**, регулирующие обработку персональных данных.

Обучение
информационной
безопасности



Организация работы по защите персональных данных



Определение перечня обрабатываемых персональных данных

После проведения аудита необходимо составить подробный перечень всех персональных данных, обрабатываемых в организации. Это включает:

- **Категории персональных данных:** общие данные (ФИО, контактная информация), специальные категории (медицинские данные, биометрические данные), данные о судимости и т.д.
- **Источники данных:** от кого и каким образом данные поступают в организацию (от клиентов, сотрудников, партнеров и т.д.).
- **Цели обработки данных:** для каких целей данные собираются и используются (исполнение договоров, маркетинговые акции, кадровый учет и т.д.).
- **Методы обработки:** как данные собираются, хранятся, используются, передаются и уничтожаются.
- **Сроки хранения данных:** как долго данные сохраняются в организации и что происходит после истечения этого срока.

Обучение
информационной
безопасности



Организация работы по защите персональных данных



На основе результатов аудита необходимо разработать ЛНА. К таким документам относятся:

Политика обработки персональных данных. Основной документ, определяющий цели, принципы и общие положения обработки данных в организации. Политика должна быть доступна для всех сотрудников и, при необходимости, для субъектов данных (например, размещена на сайте компании).

Регламенты и процедуры. Подробные инструкции по обработке данных в различных подразделениях. Они должны описывать:

Порядок сбора данных: получение согласия субъектов, использование форм и опросников.

Хранение данных: использование информационных систем, правила доступа, резервное копирование.

Передача данных: внутри организации и третьим лицам, требования к работе с контрагентами.

Уничтожение данных: процедуры удаления или обезличивания данных после достижения целей обработки или по требованию субъекта.

Положение о защите персональных данных. Документ, устанавливающий меры по обеспечению безопасности данных, включая технические и организационные меры, порядок реагирования на инциденты.

Обучение
информационной
безопасности



Организация работы по защите персональных данных



Назначение ответственных лиц за защиту данных

- **Ответственный за организацию обработки персональных данных.**
Должностное лицо, в обязанности которого входит:
- **Контроль за соблюдением законодательства и внутренних документов.**
- **Обучение и консультирование сотрудников по вопросам защиты данных.**
- **Взаимодействие с надзорными органами, в частности с Роскомнадзором.**
- **Рассмотрение обращений субъектов персональных данных и урегулирование инцидентов.**

Команда по безопасности информации. Группа специалистов, отвечающих за технические аспекты защиты данных, включая:

Разработку и внедрение технических средств защиты

Мониторинг и анализ событий безопасности

Проведение аудитов безопасности и тестирование систем на уязвимости

Обучение
информационной
безопасности



Организация работы по защите персональных данных



Обучение и информирование персонала

Программы обучения сотрудников

Человеческий фактор является одной из основных причин инцидентов в сфере информационной безопасности. Обучение играет ключевую роль в организации защиты персональных данных.

Программы обучения должны включать:

- **Общие сведения о законодательстве:** основные положения закона "О персональных данных", права субъектов данных, обязанности операторов.
- **Внутренние политики и процедуры:** ознакомление с политикой обработки данных, регламентами и инструкциями.
- **Практические навыки:** правильное использование информационных систем, безопасная работа с документами, реагирование на инциденты.
- **Специальные темы:** для сотрудников, работающих с особыми категориями данных или в высокорисковых областях, необходимо углубленное обучение.

Обучение
информационной
безопасности



Практические задания



Задание 1. Анализ правовой ситуации в сфере защиты персональных данных

Вы работаете в компании, которая занимается онлайн-продажами и собирает персональные данные клиентов для обработки заказов и маркетинговых рассылок. Один из клиентов обнаружил, что без его согласия компания передала его персональные данные третьим лицам, и подал жалобу в Роскомнадзор.

Задание

- Проанализируйте, какие нарушения законодательства о персональных данных были допущены.
- Определите, какие права субъекта персональных данных были нарушены.
- Какие административные или уголовные санкции могут быть применены к компании и ответственным лицам?
- Разработайте план действий для компании по урегулированию ситуации и предотвращению подобных нарушений в будущем.

Обучение
информационной
безопасности



Практические задания



Задание 2. Разработка политики обработки персональных данных

Вы — ответственный за организацию обработки персональных данных в новой технологической компании, которая собирается запустить мобильное приложение для отслеживания фитнес-активности пользователей. Вам необходимо разработать внутреннюю политику обработки персональных данных, соответствующую законодательству РФ.

Вопросы

- Определите перечень персональных данных, которые будут обрабатываться приложением (включая специальные категории, если есть).
- Укажите цели и правовые основания обработки этих данных.
- Опишите меры, которые компания примет для обеспечения безопасности персональных данных пользователей.
- Разработайте процедуру получения согласия пользователей на обработку их персональных данных.
- Определите порядок предоставления пользователям информации об их правах и способах их реализации.

Обучение
информационной
безопасности



Практические задания



Задание 3. Краткий анализ ситуации с нарушением законодательства о персональных данных

Представьте, что вы работаете юрисконсультom в компании, которая собирается запустить новую маркетинговую акцию. Менеджер по маркетингу предлагает использовать существующую базу персональных данных клиентов для рассылки рекламных материалов, не получая от них дополнительного согласия.

Вопросы

- Определите, какие принципы и положения законодательства о персональных данных будут нарушены, если компания реализует эту идею без получения согласия клиентов.
- Кратко опишите риски и возможные юридические последствия для компании.
- Сформулируйте рекомендации менеджеру по маркетингу, как действовать в соответствии с законодательством и избежать нарушений.

Обучение
информационной
безопасности



Коммерческая тайна



Обучение
информационной
безопасности



Коммерческая тайна



Критерии отнесения информации к коммерческой тайне

Для того чтобы информация была признана коммерческой тайной, она должна соответствовать ряду критериев:

1. Незнестность третьим лицам:

Информация не должна быть общедоступной или широко известной в соответствующих кругах.

Данные не должны быть опубликованы в открытых источниках или стать достоянием общестственности без согласия обладателя.

2. Коммерческая ценность информации:

Сведения должны иметь экономическую ценность для организации благодаря их неизвестности конкурентам.

Утечка информации может привести к финансовым потерям или упущенной выгоде.

Обучение
информационной
безопасности



Коммерческая тайна



Критерии отнесения информации к коммерческой тайне

3. Принятие мер по охране конфиденциальности:

Организация должна предпринимать разумные действия для защиты информации (введение режима коммерческой тайны, ограничение доступа, использование технических средств защиты).

Наличие документально оформленных процедур и инструкций по защите информации.

4. Отсутствие законных оснований для раскрытия информации:

Информация не может быть отнесена к коммерческой тайне, если законодательство требует ее раскрытия (например, данные об экологических нарушениях, здоровье населения).

Обучение
информационной
безопасности



Коммерческая тайна



Практические примеры информации, составляющей коммерческую тайну

Технологические процессы и рецептуры: Уникальные методы производства, формулы продуктов.

Финансовые показатели и бюджеты: Детальные отчеты о прибыли, убытках, инвестиционных планах.

Маркетинговые стратегии: Планы по продвижению на новые рынки, рекламные кампании, анализ конкурентной среды.

Клиентские базы данных: Контактная информация, предпочтения клиентов, история покупок.

Договорные условия с партнерами: Цены, скидки, условия поставок, эксклюзивные соглашения.

Обучение
информационной
безопасности



Коммерческая тайна



Коммерческая тайна — режим конфиденциальности информации, который позволяет её обладателю увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке или получить иную коммерческую выгоду.

(ст. 3 Федерального закона № 98-ФЗ)

Права и обязанности обладателя информации

- **Право** — определить перечень сведений, составляющих коммерческую тайну.
- **Обязанность** — ограничить доступ к информации и установить правила её использования.
- **Обязанность** — вести учёт лиц, получивших доступ к информации.
- **Обязанность** — урегулировать использование информации работниками и контрагентами.
- **Обязанность** — обеспечить защиту информации и маркировать её носители грифом «**Коммерческая тайна**» с указанием обладателя.

Обучение
информационной
безопасности



Коммерческая тайна



Как вводится режим коммерческой тайны

1. Определяется **перечень сведений**, составляющих коммерческую тайну.
2. Ограничивается **доступ** к информации и устанавливается порядок работы с ней.
3. Ведётся **учёт лиц**, получивших доступ.
4. В трудовых и гражданско-правовых отношениях закрепляются правила использования и защиты информации.
5. На документы и иные материальные носители наносится гриф **«Коммерческая тайна»** с указанием обладателя.

Важно: режим коммерческой тайны считается установленным после принятия предусмотренных законом мер по охране конфиденциальности информации.

Обучение
информационной
безопасности



Коммерческая тайна



Что нельзя отнести к коммерческой тайне?

В соответствии со **ст. 5 Федерального закона № 98-ФЗ** режим коммерческой тайны не может быть установлен, в частности, в отношении сведений:

- о **нарушениях законодательства РФ** и фактах привлечения к ответственности;
- о **состоянии окружающей среды**;
- о **противопожарной безопасности**, санитарно-эпидемиологической и радиационной обстановке;
- о **безопасности пищевых продуктов** и других факторах, влияющих на безопасность граждан и населения;
- о **численности и составе работников**, системе оплаты труда и условиях труда, в том числе об охране труда;

Обучение
информационной
безопасности



Коммерческая тайна



- о производственном травматизме и профессиональной заболеваемости;
- о задолженности по заработной плате и социальным выплатам;
- о сведениях, **обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена федеральным законом.**

Главный принцип: нельзя объявить коммерческой тайной информацию, которую закон прямо запрещает закрывать от доступа.

Обучение
информационной
безопасности



Аспекты защиты коммерческой тайны



Технические меры защиты

Шифрование данных:

Использование современных криптографических методов для защиты информации при хранении и передаче.

Системы предотвращения утечек (DLP):

Программные решения, контролирующие потоки информации и предотвращающие несанкционированный вывод данных.

Антивирусные и антиспам-программы:

Защита от вредоносного ПО и фишинговых атак, которые могут привести к утечке информации.

Обучение
информационной
безопасности



Аспекты защиты коммерческой тайны



Организационные меры защиты

Разработка политики информационной безопасности:

Определение стратегических направлений и принципов защиты информации в организации.

Назначение ответственных лиц:

Создание отдела или назначение ответственного за информационную безопасность.

Проведение аудитов и оценок рисков:

Регулярный анализ уязвимостей и потенциальных угроз.

Обучение
информационной
безопасности



Порядок создания режима защиты коммерческой тайны



Критерии отбора информации для перечня

Первым шагом в создании режима коммерческой тайны является составление перечня сведений, которые будут считаться коммерческой тайной организации. Отбор информации для этого перечня должен осуществляться на основе четких критериев:

- 1. Коммерческая ценность информации.** Сведения должны иметь реальную или потенциальную ценность для организации, обеспечивая ей конкурентное преимущество или финансовую выгоду.
- 2. Незнание третьими лицами.** Информация не должна быть общедоступной или широко известной в соответствующих кругах.
- 3. Принятие мер по охране конфиденциальности.** Организация должна предпринимать разумные меры для защиты информации от несанкционированного доступа и распространения.
- 4. Законность отнесения информации к коммерческой тайне.** Информация не должна входить в перечень сведений, которые не могут составлять коммерческую тайну согласно законодательству (например, сведения об экологических нарушениях, задолженностях по зарплате и т.д.).

Обучение
информационной
безопасности



Порядок создания режима защиты коммерческой тайны



Рекомендуемые категории сведений

В перечень сведений, составляющих коммерческую тайну, **могут включаться**, в частности:

- **Финансово-экономическая информация.** Бюджеты, финансовые планы и прогнозы, данные о себестоимости, рентабельности, инвестиционных проектах — **если сведения не подлежат обязательному раскрытию по закону.**
- **Технологические сведения и ноу-хау.** Технологические процессы, технические решения, рецептуры, формулы, методики, результаты разработок и иные сведения, имеющие коммерческую ценность.
- **Маркетинговая и стратегическая информация.** Планы развития бизнеса, стратегии выхода на новые рынки, результаты исследований, планы рекламных кампаний, коммерческие стратегии.
- **Информация о клиентах, поставщиках и контрагентах.** Сведения о деловых связях, условиях сотрудничества, индивидуальных ценах и скидках, коммерческих предложениях, условиях договоров — **при наличии оснований для отнесения их к коммерческой тайне.**
- **Кадровая и организационная информация**

Внутренние планы развития персонала, кадровые планы, сведения о предполагаемых организационных изменениях и иная информация, имеющая коммерческую ценность.

⚠ Важно: сведения об условиях труда, охране труда, производственном травматизме, профессиональной заболеваемости, численности и составе работников, системе оплаты труда и другие сведения, прямо указанные в **ст. 5 Федерального закона № 98-ФЗ**, не могут составлять коммерческую тайну.

- **Информация об информационных системах и технологиях**

Архитектура IT-инфраструктуры, внутренние технические решения, сведения о системах защиты информации, конфигурации и иные технические сведения, раскрытие которых может причинить ущерб организации.

Обучение
информационной
безопасности



Процедуры ограничения доступа к информации, составляющей коммерческую тайну



Технические и организационные меры защиты

1. Технические меры:

Контроль доступа: Использование систем идентификации и аутентификации пользователей (пароли, биометрия, смарт-карты).

Шифрование данных: Применение криптографических средств для защиты информации при хранении и передаче.

Системы обнаружения вторжений (IDS/IPS): Мониторинг сети на предмет подозрительной активности и предотвращение несанкционированного доступа.

Резервное копирование и восстановление данных: Регулярное создание резервных копий для предотвращения потери информации.

Защита физических носителей: Использование сейфов, замков, контроль доступа в помещения с конфиденциальной информацией.

Обучение
информационной
безопасности



Процедуры ограничения доступа к информации, составляющей коммерческую тайну



Технические и организационные меры защиты

⚠ Важно: сведения об условиях труда, охране труда, производственном травматизме, профессиональной заболеваемости, численности и составе работников, системе оплаты труда и другие сведения, прямо указанные в **ст. 5 Федерального закона № 98-ФЗ**, не могут составлять коммерческую тайну.

• Информация об информационных системах и технологиях

Архитектура IT-инфраструктуры, внутренние технические решения, сведения о системах защиты информации, конфигурации и иные технические сведения, раскрытие которых может причинить ущерб организации.

Обучение
информационной
безопасности



Процедуры ограничения доступа к информации, составляющей коммерческую тайну



1. Организационные меры:

Разработка политики информационной безопасности: Определение правил и процедур обращения с конфиденциальной информацией.

Обучение персонала: Проведение регулярных тренингов и инструктажей по вопросам безопасности и сохранения коммерческой тайны.

Классификация информации: Присвоение уровня конфиденциальности различным видам информации.

Мониторинг и аудит: Регулярная проверка соблюдения установленных правил и процедур, проведение внутренних аудитов безопасности.

Обучение
информационной
безопасности



Процедуры ограничения доступа к информации, составляющей коммерческую тайну



Установление уровней доступа для сотрудников

Разграничение доступа к коммерческой тайне является одной из ключевых мер по ее защите. Для этого необходимо:

Определить категории сотрудников: Разделить персонал на группы в зависимости от их должностных обязанностей и необходимости доступа к определенной информации.

Назначить уровни доступа:

Общий доступ: Информация, доступная всем сотрудникам организации.

Ограниченный доступ: Информация, доступная определенным отделам или группам.

Конфиденциальный доступ: Информация, доступная только узкому кругу лиц (руководство, ключевые специалисты).

Установить процедуры выдачи и отзыва прав доступа: Определить порядок предоставления доступа новым сотрудникам и отзыва прав у уволенных или переведенных сотрудников.

Обучение
информационной
безопасности



ЛНА информации, составляющей коммерческую тайну



Положение о коммерческой тайне

Положение о коммерческой тайне является основным внутренним документом, регламентирующим порядок обращения с конфиденциальной информацией в организации. В него должны быть включены:

- **Цели и задачи защиты коммерческой тайны.**
- **Перечень сведений, составляющих коммерческую тайну.**
- **Права и обязанности сотрудников по сохранению конфиденциальности.**
- **Порядок доступа к коммерческой тайне.**
- **Меры ответственности за нарушение режима коммерческой тайны.**
- **Порядок взаимодействия с контрагентами и государственными органами.**

Обучение
информационной
безопасности



ЛНА информации, составляющей коммерческую тайну



Должностные инструкции и обязанности работников

В должностные инструкции сотрудников, имеющих доступ к коммерческой тайне, необходимо включить следующие положения:

Обязанность по сохранению конфиденциальности: Четкое указание на необходимость неразглашения коммерческой тайны как в период работы, так и после увольнения.

Правила обращения с конфиденциальной информацией: Порядок получения, использования и передачи информации внутри организации.

Ответственность за нарушение: Указание на возможные дисциплинарные меры в случае нарушения обязательств по сохранению коммерческой тайны.

Обучение
информационной
безопасности



ЛНА информации, составляющей коммерческую тайну



Порядок внесения изменений и дополнений при введении режима коммерческой тайны

При необходимости обновления или корректировки положений о коммерческой тайне следует:

Провести анализ актуальности информации: Проверить соответствие перечня сведений текущей деятельности организации.

Разработать изменения: Подготовить проекты поправок или дополнений.

Согласовать изменения: Обсудить предложения с руководством и юридическим отделом.

Утвердить обновленные документы: Подписать изменения и довести их до сведения всех заинтересованных лиц.

Обучить персонал: Провести инструктажи или тренинги по новым правилам.

Обучение
информационной
безопасности



Обязательства работников по сохранению тайны



Порядок заключения соглашений о неразглашении

Сотрудники, имеющие доступ к коммерческой тайне, должны официально подтвердить свое обязательство по ее сохранению. Для этого необходимо:

Подготовить соглашение о неразглашении (NDA): Документ должен содержать:

Определение конфиденциальной информации.

Обязанности работника по ее сохранению.

Срок действия обязательств (в том числе после увольнения).

Ответственность за нарушение соглашения.

Обучение
информационной
безопасности



Обязательства работников по сохранению тайны



Заключить соглашение:

При приеме на работу: Включить положение о неразглашении в трудовой договор или заключить отдельное соглашение.

При изменении условий: Заключить дополнительное соглашение в случае изменения должностных обязанностей или расширения доступа к информации.

Хранить оригиналы соглашений: Обеспечить сохранность документов в личных делах сотрудников.

В случае нарушения обязательств по сохранению коммерческой тайны работник может быть привлечен к:

Дисциплинарной ответственности: Замечание или выговор\Увольнение по соответствующим основаниям.

Материальной ответственности: Возмещение причиненного ущерба в полном объеме.

Гражданско-правовой ответственности: Иск о возмещении убытков или упущенной выгоды.

Уголовной ответственности: Уголовный кодекс РФ (например, статья 183 УК РФ).

Обучение
информационной
безопасности



Контроль информации и работы сотрудников



Обучение
информационной
безопасности



Для чего и как вводить контроль сотрудников



80% инцидентов безопасности приходится на внутренних нарушителей

Контроль вводится для обеспечения защиты конфиденциальной информации, обрабатываемой в организации. Для этого требуется в **письменном виде** собрать с сотрудников согласия на обработку и использование данных, содержащие **перечень собираемых данных**, а также **цели и способы их обработки**.

"Что не запрещено — разрешено"

Этот подход предполагает, что сотрудники могут выполнять любые действия, если они прямо не запрещены политиками компании. Он характерен для компаний с гибким подходом к контролю и повышенным доверием к сотрудникам. Подходит для менее критичных данных, где инциденты не приведут к серьёзным последствиям.

Плюсы: увеличивает свободу действий, позволяет сотрудникам быстрее выполнять задачи, находить решения и адаптироваться к изменениям, также повышает лояльность к компании и снижает уровень бюрократии.

Минусы: Требуется более детальной начальной проработки политик безопасности, повышает риск утечек и ошибок, если не предусмотрены все возможные угрозы.

Обучение
информационной
безопасности



Для чего и как вводить контроль сотрудников



"Что не разрешено — запрещено"

Этот подход означает, что любые действия, прямо не разрешённые политиками безопасности, считаются запрещёнными. Применяется в финансовых и государственных организациях, где требуется высокий уровень защиты данных. Подходит для защиты критичных данных, где последствия инцидента могут быть серьёзными.

Плюсы: обеспечивает изначально более высокий уровень безопасности, снижает вероятность инцидентов, связанных с неправильным использованием системы.

Минусы: может ограничивать гибкость и производительность сотрудников, особенно в быстро меняющихся условиях за счет усложнения процессов для получения дополнительных доступов. повышает уровень бюрократии, недовольство сотрудников.

Обучение
информационной
безопасности



Для чего и как вводить контроль сотрудников



При выявлении инцидентов информационной безопасности важно следовать установленной процедуре, чтобы минимизировать возможные последствия, обычно она выглядит следующим образом и в таком виде автоматизируется программными средствами:

Фиксация инцидента: Документирование обстоятельств инцидента, регистрация события в системе учёта, что позволяет отследить все действия сотрудников.

Уведомление руководства и службы безопасности: Сообщение должно содержать описание инцидента, его последствия и возможные меры по устранению.

Анализ инцидента и его причины: Проведение расследования, чтобы выяснить, как произошёл инцидент, кто был его инициатором и оценка последствий.

Взаимодействие с государственными регуляторами: Роскомнадзор и другие органы, если инцидент выходит за рамки персональных данных и затрагивает сферы отдельных ведомств (таких как ФСБ, Центробанк и другие).

Устранение последствий и обновление политики безопасности: После разбора и устранения последствий инцидента необходимо также устранить слабые места, ставшие причиной его возникновения, внося корректировки в текущие политики безопасности.

Обучение
информационной
безопасности



Защита информации, персональные данные и работа с ними для ОО



Обучение
информационной
безопасности



Какие персональные данные обрабатывает школа и сад



Школы и детские сады обрабатывают персональные данные учащихся и воспитанников, родителей, работников и физических лиц, которые выполняют работы по договорам подряда, оказывают услуги.

К персональным данным можно отнести любую совокупность информации о конкретном человеке (п. 1 ст. 3 Закона № 152-ФЗ). По режиму обработки их делят на общие и специальные. Специальные – информация о расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни (ч. 1 ст. 10 Закона № 152-ФЗ). Школа и детский сад вправе обрабатывать ее только с согласия субъекта. Общие персональные данные – все остальные. Обрабатывать их можно и без согласия, но только в границах, установленных законодательством (п. 2–11 ч. 1 ст. 6 Закона № 152-ФЗ).

Отдельно выделяют категорию биометрических персональных данных. Они характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором только с этой целью (ч. 1 ст. 11 Закона № 152-ФЗ).

Обучение
информационной
безопасности



Какие персданные обрабатывает школа и сад



Биометрические персданные обрабатывают только с личного письменного согласия субъекта. В связи с этим Роскомнадзор и Минцифры решили, что в образовательных организациях такие данные обрабатывать нельзя, потому что несовершеннолетние не вправе давать на это письменное согласие (письма Роскомнадзора от 10.02.2020 № 08АП-6782, Минцифры от 17.07.2020 № ОП-П24-070-19433, Минкомсвязи от 28.08.2020 № ЛБ-С-074-24059). Без него обрабатывать биометрию можно только, чтобы осуществить правосудие и исполнить судебные акты, провести обязательную государственную дактилоскопическую регистрацию, а также в случаях, предусмотренных уголовно-исполнительным законодательством, законодательством об обороне, оперативно-розыскной деятельности, о безопасности, противодействии терроризму и коррупции, транспортной безопасности, нотариате, порядке выезда из России и въезда в Россию, гражданстве РФ (ч. 2 ст. 11 Закона № 152-ФЗ).

Обучение
информационной
безопасности



Какие персональные данные обрабатывает школа и сад



К персональным данным не относят обезличенную информацию. Она не дает возможности точно определить человека, хоть и содержит некоторые сведения о нем – например, возраст или район проживания. Однако совокупности формально обезличенной информации бывает достаточно, чтобы понять, о ком идет речь.

Например, если написать о «директоре школы» либо «жителе города Воронеж», то сведений недостаточно. А если о «директоре школы – жителе города Воронеж», которое находится вне пределов транспортной доступности от иных населенных пунктов и имеет только одну школу, то человека определить легко. В таком случае суды и проверяющие не признают информацию обезличенной и отнесут к персональным данным.

Обучение
информационной
безопасности



Какие персданные обрабатывает школа и сад



Перечень документов, в которых есть персональные данные

Субъект данных	Документ	Персональные данные
Учащийся Воспитанник	Заявление о приеме. Копия свидетельства о рождении ребенка. Копия свидетельства о регистрации ребенка по месту жительства или месту пребывания. Медицинская карта ребенка. Рекомендация психолого-медико-педагогической комиссии. Заключение и протоколы психолого-педагогического консилиума. Справка-допуск после перенесенного заболевания. Документы, которые образуются во время учебы, например, характеристики по результатам психолого-педагогической помощи, справки по результатам учебно-методической деятельности. Распорядительные акты школы и детского сада	Фамилия, имя, отчество. Дата и место рождения. Адрес места жительства. Особенности ребенка, определяющие необходимость создания специальных условий. Сведения о здоровье, диагноз. Сведения о личных качествах, успеваемости. СНИЛС

Обучение
информационной
безопасности



Какие персданные обрабатывает школа и сад



Перечень документов, в которых есть персональные данные

Родитель	Заявление о приеме. Заявление на право забирать ребенка. Заявление о переводе. Договоры	Фамилия, имя, отчество. Дата и место рождения. Адрес места жительства. Паспортные данные. Контакты – телефон, электронная почта. Номер банковского счета и наименование банка
----------	---	---

Обучение
информационной
безопасности



Какие персданные обрабатывает школа и сад



Перечень документов, в которых есть персональные данные

Работник	Заявление о приеме на работу. Резюме соискателя. Документы об образовании и квалификации. Трудовая книжка. Трудовой договор. Личная карточка. Документы из личного дела. Медицинское заключение, медкнижка и заключительный акт по итогам медосмотра. Листок нетрудоспособности. Справка 2-НДФЛ. Распорядительные акты школы	Фамилия, имя, отчество. Пол, возраст. Изображение. Паспортные данные. Дата и место рождения. Адрес места жительства. Образование, квалификация, профессиональная подготовка и сведения о повышении квалификации. Семейное положение, наличие детей, родственные связи. Факты биографии и предыдущей трудовой деятельности. Сведения о деловых и личных качествах. Сведения о здоровье. Сведения о заработной плате. Номер банковского счета и наименование банка. СНИЛС
----------	---	---

Обучение
информационной
безопасности



Какие персданные обрабатывает школа и сад



Перечень документов, в которых есть персональные данные

Физическое лицо, выполняющее работы по договорам подряда, оказывающее услуги	Гражданско-правовой договор	Фамилия, имя, отчество. Паспортные данные. Адрес места жительства. Номер банковского счета и наименование банка
Физическое лицо, сотрудничающее с организацией в рамках некоммерческой совместной деятельности –просветительских мероприятий и т.п.	Договор, соглашение. Согласие на обработку персональных данных. Документы для допуска на территорию	Фамилия, имя, отчество. Паспортные данные. Биографические данные – о трудовом стаже, научной и образовательной деятельности, достижениях и т. п.

Обучение
информационной
безопасности



В каких целях можно обрабатывать персданные



Обрабатывать персональные данные можно только в целях, которые установлены в законодательстве или локальных актах (ч. 2, 4–6 ст. 5 Закона № 152-ФЗ). Закрепите цели обработки в политике, так как с этим документом должны быть знакомы все, кто взаимодействует с вашей организацией.

Если цель не закрепили, то собирать персональные данные для нее нельзя. Например, обрабатывать личную информацию о кандидатах, если в политике указали, что собираете данные, чтобы регулировать трудовые отношения с работниками. Кандидат – еще не работник школы.

Обучение
информационной
безопасности



В каких целях можно обрабатывать персданные



Чтобы определить цели обработки персданных, проанализируйте деятельность образовательной организации в целом и направления деятельности структурных подразделений, отдельных должностных лиц – в частности. Например, школы и детские сады обрабатывают персданные в целях:

- организации образовательной деятельности по основным образовательным программам общего образования, дополнительным общеобразовательным программам;
- ведения иных видов деятельности в соответствии с уставом;
- приема на работу и оформления трудовых отношений с работниками;
- реализации гражданско-правовых договоров, стороной, выгодоприобретателем или получателем которых является субъект персональных данных;
- обеспечения безопасности.

Обучение
информационной
безопасности



В каких целях можно обрабатывать персданные



Не собирайте избыточные персональные данные

При приёме на работу собирайте только те персональные данные, которые необходимы для конкретной цели обработки.

 Проверьте необходимость копирования документов:

- паспорта;
- документов об образовании;
- иных документов, содержащих персональные данные.

Само наличие документа у работодателя не означает, что его копию необходимо хранить. Если для выполнения требований закона достаточно предъявления документа и фиксации необходимых сведений, избыточное копирование может стать нарушением принципа минимизации персональных данных.

Обучение
информационной
безопасности



В каких целях можно обрабатывать персданные



⚠ Для образовательных организаций особенно важно: не формировать кадровые дела по принципу «копируем всё подряд». Для каждого вида персональных данных должна быть **конкретная законная цель и правовое основание обработки**.

Ответственность

За нарушение требований законодательства о персональных данных предусмотрена административная ответственность по **ст. 13.11 КоАП РФ**.

С 30 мая 2025 года размеры ряда штрафов существенно увеличены.

Практический принцип:

Нужны данные — обоснуйте цель и правовое основание.

Не нужны — не собирайте и не храните.

Обучение
информационной
безопасности



Как организовать обработку персональных данных в школе и саду



- 1. Определить, какие данные обрабатываются.** Учащиеся и воспитанники • родители • работники • контрагенты • иные физические лица.
- 2. Определить цели обработки.** Для каждой категории данных должна быть конкретная, заранее определённая и законная цель.
- 3. Определить правовое основание.** Обработка осуществляется на основании закона, договора, иных предусмотренных законом оснований или согласия — когда оно необходимо.
- 4. Не собирать лишние данные.** Объём и содержание персональных данных должны соответствовать заявленным целям обработки.
- 5. Ограничить доступ.** Доступ получают только работники, которым данные необходимы для выполнения должностных обязанностей.
- 6. Обеспечить защиту данных.** Организационные и технические меры должны предотвращать неправомерный или случайный доступ, изменение, распространение и уничтожение данных.
- 7. Установить порядок хранения и уничтожения.** Определить сроки хранения и порядок уничтожения либо обезличивания данных.
- 8. Назначить ответственного за организацию обработки ПД**
Полномочия и обязанности закрепляются приказом руководителя.

Обучение
информационной
безопасности



Как организовать обработку персональных данных в школе и саду



Какие персональные данные обрабатывают школа и детский сад?



Обучающиеся и воспитанники

- ФИО, дата и место рождения;
- адрес, СНИЛС и другие идентификаторы;
- сведения об обучении и успеваемости;
- сведения о состоянии здоровья — в предусмотренных законом случаях;
- сведения о специальных образовательных потребностях.



Родители и законные представители

- ФИО и контактные данные;
- паспортные данные — когда необходимы;
- сведения, необходимые для оформления образовательных и иных отношений.

Обучение
информационной
безопасности



Как организовать обработку персональных данных в школе и саду



Работники

- сведения, необходимые для оформления трудовых отношений;
- образование и квалификация;
- сведения о трудовой деятельности;
- сведения о заработной плате;
- медицинские сведения — когда их обработка предусмотрена законом.



Контрагенты и исполнители

- данные, необходимые для заключения и исполнения гражданско-правовых договоров;
- контактные и платёжные реквизиты.

Важно: перечень персональных данных не является закрытым.

К ПД относится информация, которая прямо или косвенно относится к определённому или определяемому физическому лицу.

Обучение
информационной
безопасности



Как организовать обработку персональных данных в школе и саду



Специальные и биометрические персональные данные

Специальные категории ПД — сведения:

- о расовой и национальной принадлежности;
- политических взглядах;
- религиозных или философских убеждениях;
- состоянии здоровья;
- интимной жизни.

Для их обработки действуют **специальные требования ст. 10 152-ФЗ**.

Обучение
информационной
безопасности



Как организовать обработку персональных данных в школе и саду



Биометрические ПД

Биометрическими являются сведения о физиологических и биологических особенностях человека, которые используются оператором **для установления личности**.

Примеры: данные, используемые для идентификации по лицу, голосу, отпечаткам пальцев.

Общее правило: обработка биометрических ПД допускается при наличии письменного согласия субъекта, кроме прямо предусмотренных законом случаев.

Практический вывод для школы и ДОУ:

Перед использованием систем распознавания лица, голоса, отпечатков и других технологий идентификации необходимо отдельно проверить правовое основание обработки и требования законодательства.

Обучение
информационной
безопасности



Уведомление Роскомнадзора об обработке персональных данных



До начала обработки персональных данных оператор должен уведомить Роскомнадзор о намерении осуществлять обработку ПД.

Основание: ч. 1 ст. 22 Закона № 152-ФЗ.

Для школы и детского сада уведомление, как правило, **обязательно**, поскольку организация обрабатывает ПД работников, детей, родителей и других лиц с использованием информационных систем.

Важно: уведомление подается **однократно**, но сведения в нем необходимо актуализировать при изменениях.

Для каждой цели обработки указываются:

- категории персональных данных;
- категории субъектов ПД;
- правовое основание обработки;
- действия с персональными данными;
- способы обработки.

Также указываются дата начала обработки; срок или условие прекращения обработки; наличие/отсутствие трансграничной передачи; место нахождения базы данных ПД граждан РФ; сведения об ответственном за организацию обработки ПД; сведения о лицах, имеющих доступ к ПД в государственных и муниципальных информационных системах.

Обучение
информационной
безопасности



Уведомление Роскомнадзора об обработке персданных



КАК ПОДАТЬ УВЕДОМЛЕНИЕ

Удобнее всего — в электронной форме через портал Роскомнадзора.

Алгоритм:

Заполнить → подписать → направить → проверить сведения в реестре операторов

Уведомление можно направить в электронной форме либо на бумаге за подписью уполномоченного лица.

При изменении сведений

→ направить уведомление об изменениях

→ **не позднее 15-го числа месяца, следующего за месяцем изменений.**

Обучение
информационной
безопасности



Уведомление Роскомнадзора об обработке персональных данных



ПРОВЕРЬТЕ СЕБЯ В РЕЕСТРЕ

Если школа или детский сад уже подавали уведомление:

1. Найдите организацию в Реестре операторов ПД



2. Проверьте внесенные сведения



3. Сверьте их с фактической обработкой ПД



4. При необходимости подайте изменения

Проверить сведения можно по **наименованию организации или ИНН**.

Практический вывод:

Подали уведомление один раз — дальше главное **своевременно поддерживать сведения в актуальном состоянии**.

Обучение
информационной
безопасности



Ответственность за уведомление Роскомнадзора об обработке персональных данных



Обучение
информационной
безопасности



НЕ УВЕДОМИЛИ РОСКОМНАДЗОР — ШТРАФ

1. Не подали уведомление об обработке ПД

С 30 мая 2025 года действует специальная ответственность — **ч. 10 ст. 13.11 КоАП РФ**:

- **Должностное лицо — 30 000–50 000 ₽**
- **Организация — 100 000–300 000 ₽**

2. Не сообщили или несвоевременно сообщили иные сведения

Если обязанность представить сведения предусмотрена законом, применяется **ст. 19.7 КоАП РФ**:

- **Должностное лицо — 300–500 ₽**
- **Организация — 3 000–5 000 ₽**

Подали уведомление → следите за актуальностью сведений → своевременно сообщайте об изменениях.

Ответственность за уведомление Роскомнадзора об обработке персональных данных



Собираете персональные данные через сайт?

→ **Опубликуйте Политику обработки ПД.**

Например:

- форма обратной связи;
- запись на консультацию;
- электронное обращение;
- анкета или регистрационная форма.

Что должно быть доступно на сайте?

 **Политика в отношении обработки ПД**

 **Сведения о реализуемых требованиях к защите ПД**

Доступ к политике должен быть обеспечен **непосредственно на страницах сайта, где осуществляется сбор персональных данных.**

Основание: ч. 2 ст. 18.1 Закона № 152-ФЗ.

Обучение
информационной
безопасности



Ответственность за уведомление Роскомнадзора об обработке персональных данных



Политики недостаточно.

Организации нужны **политика + внутренние положения**, которые конкретизируют порядок обработки и меры защиты ПД.

Рекомендуется разработать отдельные положения:

-  о ПД работников;
-  о ПД обучающихся и воспитанников;
-  о ПД родителей (законных представителей).

Важно: положения дополняют Политику, но **не заменяют её**.

Для ПД работников: меры защиты разрабатываются с учетом требований ст. 86 ТК РФ и с участием работников.

Обучение
информационной
безопасности



Ответственность за уведомление Роскомнадзора об обработке персданных



Политики недостаточно.

Организации нужны **политика + внутренние положения**, которые конкретизируют порядок обработки и меры защиты ПД.

Рекомендуется разработать отдельные положения:

-  о ПД работников;
-  о ПД обучающихся и воспитанников;
-  о ПД родителей (законных представителей).

Важно: положения дополняют Политику, но **не заменяют её**.

Для ПД работников: меры защиты разрабатываются с учетом требований ст. 86 ТК РФ и с участием работников.

Обучение
информационной
безопасности



Ответственность за уведомление Роскомнадзора об обработке персональных данных



Обучение
информационной
безопасности



Подготовьте положения об обработке персональных данных. Они понадобятся, чтобы определить детали обработки и меры защиты, дополнить политику обработки персональных данных (п. 2 ч. 1 ст. 18.1 Закона № 152-ФЗ, п. 10 ст. 86 ТК). Документы не могут заменить друг друга, поэтому надо принять и политику, и положения.

Универсальной формы положения нет, как и рекомендаций по его подготовке. Определите самостоятельно, что включить в документ. Не забудьте выполнить требования пункта 2 части 1 статьи 18.1 Закона № 152-ФЗ.

Лучше составить отдельные положения по обработке данных работников, детей и их родителей. Это объясняется тем, что отношения между ними и образовательной организацией регулируют разные законы.

Ответственность за уведомление Роскомнадзора об обработке персданных



Обучение
информационной
безопасности



Положение об обработке персональных данных учащихся, воспитанников и их родителей поручите подготовить ответственному. Вопрос с положением для работников можно решить иначе. Трудовой кодекс требует, чтобы образовательная организация разрабатывала меры по защите их персональных данных совместно с ними (п. 10 ст. 86 ТК). Есть два варианта, чтобы соблюсти требование:

- 1) создать комиссию по разработке положения и включить в нее представителей общего собрания работников или профкома;
- 2) согласовать проект положения на заседании общего собрания работников.

Если решили создать комиссию, попросите общее собрание работников выбрать одного или нескольких представителей для подготовки положения. Включите их в комиссию вместе с ответственным за обработку персональных данных и специалистом по кадрам. При наличии профкома попросите его также выделить представителя.

Как взять согласие на обработку персданных



С работника берите согласие на обработку персданных, которых нет в документах по трудовому законодательству

Например, для приема работник должен предоставить паспорт, трудовую книжку или сведения по форме СТД-Р, документы воинского учета, диплом и т. д.

Согласие брать не нужно, если персданные будете использовать только для того, чтобы обеспечить трудовой процесс. Это же правило действует, если персданные надо переслать третьему лицу или опубликовать на сайте по требованию законодательства (п. 2 ч. 1 ст. 6 Закона № 152-ФЗ, методические рекомендации, направленные письмом Минкомсвязи от 28.08.2020 № ЛБ-С-074-24059).

Согласие понадобится, чтобы обработать другие данные – фотографию для сайта или сведения о семье для личной карточки.

Получайте отдельное согласие по каждой цели.

Работник вправе предоставить согласие как на бумаге с собственноручной подписью, так и в электронном виде с электронной подписью (ч. 1, 4 ст. 9 Закона № 152-ФЗ).

Обучение
информационной
безопасности



Что о педагогах можно размещать без разрешения



Образовательная организация обязана разместить на сайте:

- Ф. И. О.;
- должность;
- преподаваемые предметы, курсы, дисциплины;
- образование, направление подготовки, специальность и квалификацию;
- ученую степень и звание — при наличии;
- повышение квалификации за последние 3 года;
- профессиональную переподготовку — при наличии;
- опыт работы в соответствующей профессиональной сфере;
- образовательные программы, в реализации которых участвует педагог.

Почему без согласия?

Эти сведения подлежат обязательному раскрытию по законодательству об образовании.

Обучение
информационной
безопасности



Что о педагогах можно размещать без разрешения



ОТДЕЛЬНОЕ СОГЛАСИЕ НУЖНО



Фото педагога



Подробная биография



Дополнительные сведения о достижениях, конкурсах и профессиональном пути, если они не относятся к обязательным сведениям.

Правило: публикуем только тот объем ПД, который предусмотрен законом или на который получено соответствующее согласие.

Обучение
информационной
безопасности



Когда нужно согласие родителей



Согласие необходимо, когда школа или детский сад обрабатывает дополнительные персональные данные, для которых нет другого законного основания.

Например:

- оформление льгот;
- сведения об участии ребенка в конкурсах и олимпиадах, проведенных сторонними организациями;
- публикация фотографии ребенка на сайте;
- иные действия, не необходимые для реализации образовательной программы.



ВАЖНО

Согласие ≠ универсальное основание.

Сначала определите, предусмотрена ли обработка законом или необходима для выполнения обязанностей организации.

Согласие за ребенка дает его законный представитель.

Если родители расходятся во мнении относительно дополнительной обработки, до разрешения ситуации **не выполняйте спорное действие** — например, не размещайте фотографию ребенка на сайте.

Обучение
информационной
безопасности



Согласие родителей: важное правило



ОДНО СОГЛАСИЕ — ЕСЛИ ОБРАБОТКА ОХВАТЫВАЕТ УКАЗАННЫЕ В НЕМ ЦЕЛИ

Согласие должно быть **конкретным, предметным и информированным**. В нем указываются цели, данные и действия с ними.

Другие лица, забирающие ребенка

Получите только необходимые данные для идентификации и связи:

Ф. И. О. + телефон.

ОТЗЫВ СОГЛАСИЯ

Родитель может отозвать согласие. Но обработку не всегда нужно прекращать: если есть **другое законное основание**, она может продолжаться.

Например, при отзыве согласия на публикацию фото ребенка → **удалите фото**, если для дальнейшего размещения нет другого законного основания.

Обучение
информационной
безопасности



Согласие родителей: важное правило



БЕЗ СОГЛАСИЯ — КОГДА ЕСТЬ ИНОЕ ОСНОВАНИЕ

Обработка возможна, если она необходима:

- для исполнения обязанностей, установленных законом;
- для предоставления государственной или муниципальной услуги;
- для исполнения договора;
- для исполнения судебного акта;
- для защиты жизни и здоровья, когда согласие получить невозможно;
- для статистических или исследовательских целей — **при обязательном обезличивании.**

Главный принцип:

СНАЧАЛА ОПРЕДЕЛЯЕМ ЦЕЛЬ И ПРАВОВОЕ ОСНОВАНИЕ → ЗАТЕМ РЕШАЕМ, НУЖНО ЛИ СОГЛАСИЕ.

Обучение
информационной
безопасности



Как хранить персональные данные



Главный принцип — ограничить доступ и обеспечить сохранность ПД.



Бумажные документы

- храните в **запираемых шкафах или сейфах**;
- доступ — только у работников, которым он необходим;
- документы, с которыми работа не ведется, передавайте в архив;
- для отдельных документов действуют специальные требования к хранению.



Электронные данные

- ограничьте доступ к информационным системам;
- используйте индивидуальные учетные записи и права доступа;
- обеспечьте защиту от несанкционированного доступа.



Установите сроки хранения и не храните ПД дольше, чем это необходимо для целей обработки.

Обучение
информационной
безопасности



Как хранить персональные данные



Разные цели обработки → раздельное хранение. Важно: место хранения должно быть защищено от доступа посторонних лиц.

Кадровые документы



отдельные дела и места хранения

Документы обучающихся и воспитанников



отдельные дела и места хранения

Иные документы с ПД



отдельные места хранения по назначению

Что закрепить локально?

- ✓ условия хранения ПД;
- ✓ перечень мест хранения;
- ✓ работников, имеющих доступ;
- ✓ порядок передачи в архив;
- ✓ сроки хранения и уничтожения.

Обучение
информационной
безопасности



Электронная защита персданных



Ограничьте доступ к электронным ПД

 Разделите данные по категориям:

- прием на обучение;
- кадровые документы;
- медицинские данные;
- иные категории ПД.

 Для каждой папки и системы:

- доступ — только уполномоченным работникам;
- используйте индивидуальные учетные записи;
- права доступа определяйте по должностным обязанностям;
- регулярно проверяйте и актуализируйте доступ.

Важно: электронные ПД должны быть защищены от несанкционированного доступа, изменения, копирования и уничтожения.

Обучение
информационной
безопасности



Электронная защита персданных



ЕСЛИ ИСПОЛЬЗУЕТЕ ИСПДн

ИСПДн — совокупность баз данных ПД и информационных технологий и технических средств, обеспечивающих их обработку.

Если школа или детский сад использует собственную **ИСПДн**, необходимо:

1. Определить угрозы безопасности



2. Обследовать информационную систему



3. Определить необходимые меры защиты



4. Установить правила доступа



5. Применить необходимые технические средства защиты



6. Контролировать соблюдение требований

 **Главный принцип:** доступ к ПД в ИСПДн получают только те работники, которым он необходим для выполнения должностных обязанностей

Обучение
информационной
безопасности



Сроки хранения персданных



ЦЕЛЬ ОБРАБОТКИ



СРОК ХРАНЕНИЯ

-  **Установлен законом** → храним по закону
-  **Установлен договором** → храним по договору
-  **Не установлен** → закрепляем локальным актом



Срок истек

→ архив / уничтожение / обезличивание

 **Сроки хранения закрепите в номенклатуре дел.**

Обучение
информационной
безопасности



Утечка персональных данных - куда сообщать



Обнаружили неправомерный доступ / передачу / распространение ПД?



ШКОЛА ИЛИ ДЕТСКИЙ САД



Роскомнадзор — в течение 24 часов



Роскомнадзор обеспечивает дальнейшее взаимодействие с **ГосСОПКА / НКЦКИ**.

Важно: не нужно самостоятельно направлять такое уведомление одновременно и в Роскомнадзор, и в ФСБ, если организация не относится к операторам, для которых установлен иной порядок взаимодействия с НКЦКИ.

Обучение
информационной
безопасности



Два уведомления - два срока



24 ЧАСА — ПЕРВИЧНОЕ УВЕДОМЛЕНИЕ

Сообщите:

- что произошло;
- когда обнаружили инцидент;
- предполагаемые причины и возможный вред;
- принятые меры;
- контактное лицо для взаимодействия с Роскомнадзором.



72 ЧАСА — РЕЗУЛЬТАТЫ РАССЛЕДОВАНИЯ

Сообщите:

- результаты внутреннего расследования;
- причины инцидента;
- принятые дополнительные меры;
- виновных лиц — если установлены.

Если расследование завершено в первые 24 часа — его результаты можно включить в первичное уведомление.

Обучение
информационной
безопасности



Когда уничтожить персданные



Ситуация	Срок
 Цель обработки достигнута	30 дней
 Обработка признана неправомерной	10 рабочих дней
 Гражданин требует уничтожить незаконно полученные или ненужные ПД	7 рабочих дней
 Отозвано согласие	30 дней
 Гражданин требует уничтожить ПД без указания причины	10 рабочих дней (+ 5 при необходимости)

Обучение
информационной
безопасности



Когда уничтожить персданные



Важно: сроки могут отличаться, если **закон или договор устанавливает иной срок хранения.**

АЛГОРИТМ

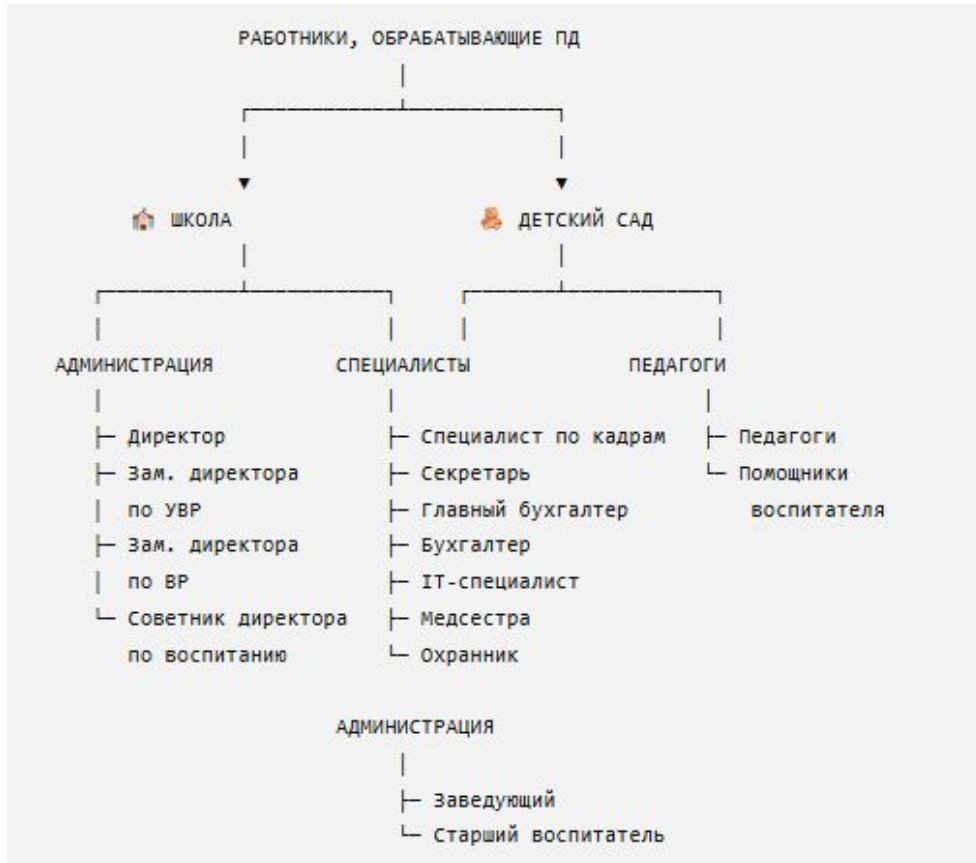
**Основание для уничтожения → проверяем срок хранения
→ уничтожаем → оформляем подтверждающий документ**

Основание: ст. 20–21 Закона № 152-ФЗ.

Обучение
информационной
безопасности



Кто может обрабатывать персданные



Обучение
информационной
безопасности



ЛНА для образовательных организаций



Документ	Зачем нужен	На каком основании
Политика обработки персональных данных в школе	Чтобы проинформировать всех заинтересованных, как школа обрабатывает персональные данные	Пункт 2 части 1 статьи 18.1 Федерального закона от 27.07.2006 № 152-ФЗ
Положение об обработке персданных работников	Чтобы зафиксировать порядок обработки и защиты персональных данных	Пункт 10 статьи 86 <u>ТК</u>
Положение об обработке персданных учащихся и третьих лиц		
Порядок уничтожения и обезличивания персональных данных	Чтобы урегулировать уничтожение и обезличивание данных	Пункт 2 части 1 статьи 18.1 Федерального закона от 27.07.2006 № 152-ФЗ
Приказ о создании комиссии по уничтожению персональных данных в школе		

Обучение
информационной
безопасности



ЛНА для образовательных организаций



Приказ о назначении ответственного в школе	Чтобы назначить работника, ответственного за организацию обработки персональных данных	Часть 1 статьи 22.1 Федерального закона от 27.07.2006 № 152-ФЗ
Приказ об утверждении списка работников школы	Чтобы определить круг работников, которые обрабатывают персональные данные	Часть 1 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ
Обязательство работника о неразглашении персданных	Чтобы уведомить работников, что они обязаны не разглашать персональные данные	Статья 88 <u>ТК</u>
Согласие на обработку персданных учащегося	Чтобы получить согласие на обработку персональных данных гражданина	Пункт 1 части 1 статьи 6 Федерального закона от 27.07.2006 № 152-ФЗ
Заявление на право забирать ученика с отметкой о согласии на обработку персданных		

Обучение
информационной
безопасности



ЛНА для образовательных организаций



Запрос информации об обработке переданных учащегося	Родитель вправе обратиться с запросом, чтобы узнать, какие данные <u>ребенка</u> и как обрабатывает школа	Статья 14 Федерального закона от 27.07.2006 № 152-ФЗ
Согласие работника на обработку переданных	Чтобы получить согласие на обработку персональных данных гражданина	Пункт 3 статьи 3, пункт 1 части 1 статьи 6 Федерального закона от 27.07.2006 № 152-ФЗ
Отзыв согласия работника на обработку переданных	Работник вправе в любое время отозвать согласие на обработку персональных данных	Часть 2 статьи 9 Федерального закона от 27.07.2006 № 152-ФЗ
Уведомление работника о получении переданных у третьих лиц	Чтобы уведомить работника, когда получаете его персональные данные от других лиц	Пункт 3 статьи 86 <u>ТК</u>
Согласие работника на получение переданных у третьих лиц	Чтобы получить согласие на обработку персональных данных гражданина	Пункт 3 статьи 3, пункт 1 части 1 статьи 6 Федерального закона от 27.07.2006 № 152-ФЗ
Согласие на передачу персональных данных работника третьей стороне		Пункт 3 статьи 3, пункт 1 части 1 статьи 6 Федерального закона от 27.07.2006 № 152-ФЗ Абзац 2 части 1 статьи 88 <u>ТК</u>

Обучение
информационной
безопасности



ЛНА для образовательных организаций



Ответ на запрос о предоставлении персональных данных	Чтобы ответить, можете ли вы предоставить персональные данные третьему лицу или нет	Часть 1 статьи 12 Федерального закона от 02.05.2006 № 59-ФЗ
Журнал учета персданных	Чтобы учитывать передачу персональных данных сторонним лицам. Журнал понадобится при проверках Роскомнадзора и в случае спора с работником	Часть 1 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ

Обучение
информационной
безопасности





едурегионлаб