Введено в действие приказом
от 31.08.2022 № 212-осн
Директор МБОУ СОШ № 13
Н.Н.Васильченко

Утверждено решением
педагогического совета МБОУ С
Протокол от 29.08.22 № 1
Секретарь педагогического совета
О.В. Аринцева

Алгоритм
построения системы защиты персональных данных

Организационные меры защиты персональных данных включают в себя комплекс мероприятий по разработке организационно-распорядительных документов, регламентирующих весь процесс получения, обработки, хранения, передачи и защиты персональных данных.

Шаг 1. Создать специальную комиссию по защите персональных данных или назначить ответственного за обеспечение информационной безопасности.

В зависимости от величины организации целесообразно назначить либо одного человека, ответственного за обеспечение информационной безопасности, либо создать специальную комиссию по защите персональных данных. В качестве председателя комиссии целесообразно назначить кого – либо из первых заместителей руководителя организации, начальника службы безопасности организации или руководителя кадровой службы организации. В состав комиссии рекомендуется включить главного бухгалтера (при наличии), руководителей подразделений организации обрабатывающих персональные данные, так как они знают структуру обрабатываемых персональных данных, задачи проводимой обработки, а также сотрудников организации, ведущих обработку персональных данных. В качестве лиц, обладающих специальным образованием в области защиты информации и необходимыми познаниями, в состав комиссии следует включить сотрудников организации, имеющей лицензию на техническую защиту конфиденциальной информации, если таковые имеются в штате организации.

Шаг 2. Произвести инвентаризацию информационной системы, обрабатывающей персональные данные.

Часто проведение этого этапа предпроектного обследования считают неразумным или нерациональным, но для построения сбалансированной системы защиты информации он необходим. На этом этапе составляется перечень всех информационных и аппаратных ресурсов организации. Данный перечень будет использоваться в дальнейшем для проведения категорирования, переконфигурирования локальной сети, выработки рекомендаций по построению системы защиты.

Выявляется топология локальной сети, ее архитектура и технологические связи внутренней сети, а также основные информационные потоки.

Также на данном этапе осуществляется определение физической и логической структуры будущей системы защиты информационной системы персональных данных. Устанавливается наличие средств защиты и существующей системы разграничения доступа к информационным ресурсам. Также изучаются имеющиеся сертификаты на средства защиты информации и выясняется необходимость сертификации уже установленных программных и программно-аппаратных комплексов защиты информации.
По итогам данного этапа составляется акт инвентаризации информационных ресурсов.

Шаг 3. Пересмотреть договоры с субъектами и контрагентами

Пересмотреть договоры с работниками и клиентами. Необходимо выяснить, содержаться ли в них пункты, касающиеся обработки и защиты персональных данных. В случае отсутствия подготовить дополнительные соглашения, ознакомить сотрудников и контрагентов. Подписать их.

Шаг 4. Сформировать перечень персональных данных.

В первую очередь, необходимо установить перечень персональных данных (далее ПДн) физических лиц, которые обрабатываются в учреждении. Если кадровый учет и бухгалтерия есть в любом учреждении, то другие направления деятельности, где используются персональные данные, требуется установить: это могут быть данные посетителей, партнеров, контрагентов и т.п.

Также нужно определить цели обработки персональных данных: трудовые отношения с работниками; договор оказания услуг и т.п.

Сроки обработки и хранения. Хранение ПДн должно быть не дольше, чем этого требуют цели их обработки, по достижению которых ПДн подлежат уничтожению. Установить перечень ПДн, по которым цели обработки достигнуты.

Шаг 5. Составить "Уведомление об обработке персональных данных".

Начав деятельность, организация обязана подать уведомление о начале обработки персональных данных в Управление Роскомнадзора. На основании уведомления организация регистрируется в реестре операторов, осуществляющих обработку персональных данных.

Уведомление должно быть направлено в письменной форме и подписано руководителем или направлено в электронной форме и подписано электронной цифровой подписью.

Одной из самых распространенных ошибок операторов, не желающих выполнять требования Закона, является ссылка на начало п. 2 ст. 22 Закона: Операторы ссылаются на оформление договорных отношений с субъектами и размышляют так: «Уведомление подавать не обязательно, значит, работы по созданию системы защиты персональных данных проводить излишне».
«Оператор вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных…»

Ссылаясь на этот пункт статьи, забывают о том, что персональные данные сами отправляют в Управление Федеральной налоговой службы, Управление Пенсионного фонда России, в страховые компании, в аутсорсинговые компании и т.д., то есть третьим лицам.

Завершается п. 2 ст. 22 Закона словами: «… если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных»

Таким образом, все юридические лица обязаны подавать уведомление и создавать систему защиты персональных данных.

Шаг 6. Получить согласие субъектов на обработку их персональных данных.

Необходимо разработать "Согласие субъекта на обработку персональных данных", в котором обязательными полями будут перечень персональных данных, цель их обработки, а также методы и способы обработки персональных данных и получить подписи каждого субъекта, персональные данные которого обрабатывает Ваша организация.

Шаг 7. Документально регламентировать работу с персональными данными.

Разработать документы, регламентирующие работу с персональными данными.

Шаг 8. Ограничить доступ своих сотрудников и пользователей информационных систем к персональным данным.

Лица, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании «Перечня лиц, допущенных персональным данным».

Шаг 9. Сформировать модель угроз персональным данным.

Частная модель угроз организации – оператора составляется в соответствии с руководящим документом ФСТЭК России от 14.02.2008 «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных». Поскольку данный документ имеет гриф «для служебного пользования», то получить его можно, отправив запрос в территориальное Управление ФСТЭК с просьбой о предоставлении комплекта документов по защите персональных данных.

Квалифицированное составление частной модели угроз имеет важное значение для организации - оператора. Именно от этого зависит выбор необходимых и достаточных способов защиты информационной системы, подбор оборудования, а, следовательно, конечная стоимость всех работ по обеспечению безопасности персональных данных.

Шаг 10. Классифицировать ИСПДн согласно приказа ФСТЭК/ФСБ/Мининформсвязи от 13.02.2008 №55/86/20 «Об утверждении порядка проведения классификации ИСПДн».

На основании закона «О персональных данных» любая информационная система персональных данных должна быть классифицирована. Процесс классификации - это процесс отнесения информационной системы персональных данных к одному из четырех классов, определенных Приказом Мининформсвязи/ФСТЭК/ФСБ от 13.02.2008 № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных».

Класс присваивается в зависимости от количества субъектов, персональные данные которых обрабатываются в ИСПДн, а также с учетом категории обрабатываемых данных. Категории персональных данных установлены приказом Федеральной службы по техническому и экспортному

контролю (ФСТЭК России) Федеральной службы безопасности Российской Федерации (ФСБ России) Министерства информационных технологий и связи Российской Федерации (Мининформсвязи России) от 13 февраля 2008 г. N 55/86/20 г. Москва "Об утверждении Порядка проведения классификации информационных систем персональных данных".

Шаг 11. Получить лицензию ФСТЭК на техническую защиту конфиденциальной информации (в случае самостоятельной установки программно-аппаратных средств защиты информации) или воспользоваться услугами сторонней организации, имеющей данную лицензию.

После изучения вопроса и понимания того, что выполнять работы необходимо, каждый руководитель задает себе следующий вопрос: можно ли самостоятельно выполнить требования законодательства или лучше воспользоваться услугами специализированной организации?

С учетом временных ограничений (срок завершения работ – 01.01.2011 года) проведение работ собственными силами может растянуться на длительный период, превышающий установленные законом сроки. Соответственно, возникают риски предъявления претензий со стороны регуляторов за неисполнение требований законодательства.

Шаг 12. Организовать эксплуатацию ИСПДн и контролировать безопасность обработки персональных данных путем проведения ежегодного аудита информационной безопасности.

Необходимо контролировать соблюдение условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией. Проводить разбирательство и составлять заключения по фактам несоблюдения условий хранения носителей ПДн, использования средств защиты информации, которые могут привести к нарушению конфиденциальности ПДн.

Шаг 13. Обучить лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними.

Для того, чтобы организация могла выполнять требования законодательства по защите персональных данных, мало разработать организационно-распорядительные и эксплуатационные документы и купить технические средства защиты информации. Очень важно на постоянной основе проводить обучение сотрудников новым средствам защиты информации, которые они используют в силу выполнения своих должностных обязанностей, а также правилам работы с этими средствами.