БАЖИН Константин Алексеевич

Гл. специалист лаборатории ЗИ НИИ КИТ
Офицер безопасности ТюмГУ

kabazhin@gmail.com
www.kbinform.ru

План доклада

- Систематический подход к защите персональных данных в организации
- Обработка ПДн с использованием средств автоматизации и без такового
- Пошаговая инструкция по защите ПДн

ПОЕХАЛИ ….

СТАДИИ СОЗДАНИЯ СЗПДН

ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНСТИТУТ МАТЕМАТИКИ И КОМПЬЮТЕРНЫХ НАУК

Стадии создания СЗПДн.

- ***предпроектная стадия,*** включающая предпроектное обследование ИСПДн, разработку технического (частного технического) задания на её создание;
- ***стадия проектирования и реализации ИСПДн,*** включающая разработку СЗПДн в составе ИСПДн;
- ***стадия ввода в действие СЗПДн,*** включающая опытную эксплуатацию и приёмо-сдаточные испытания, а также оценку соответствия ИСПДн требованиям безопасности информации.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПДН ПО ШАГАМ

ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНСТИТУТ МАТЕМАТИКИ И КОМПЬЮТЕРНЫХ НАУК

ШАГ 1. РАСПРЕДЕЛЕНИЕ ОТВЕТСТВЕННОСТИ

ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНСТИТУТ МАТЕМАТИКИ И КОМПЬЮТЕРНЫХ НАУК

Распределение ответственности.

- Должно быть определено структурное подразделение или должностное лицо, ответственное за обеспечение безопасности ПДн.

Распределение ответственности.

- обработка защищаемой информации регламентирована, проводится регулярный контроль соблюдения установленного порядка обработки;
- защита информации организована, проводится постоянный контроль и оценка эффективности данной защиты;
- физическая защита элементов инфраструктуры, участвующих в обработке защищаемой информации, организована, проводится регулярный контроль эффективности защиты.

Распределение ответственности.

РЕЗУЛЬТАТ

- для организации-оператора - Руководство по защите информации от технических разведок и от её утечки по техническим каналам, регламенты и процедуры;
- для подразделения - Положение о структурном (производственном) подразделении;
- для должностного лица - его должностная инструкция.

Распределение ответственности.

- документы должны быть утверждены (введены в действие) приказом Руководителя
- доведены до лиц, вовлеченных в деятельность, связанную с необходимостью выполнять требования к безопасности информации, под роспись
- обязанность выполнения указанных требований должна быть зафиксирована в трудовых договорах с сотрудниками организации-оператора.

ШАГ 2. ОПРЕДЕЛЕНИЕ ПРАВОВЫХ ОСНОВАНИЙ ОБРАБОТКИ ПДН

ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНСТИТУТ МАТЕМАТИКИ И КОМПЬЮТЕРНЫХ НАУК

Определение правовых оснований обработки ПДн

- Необходимо определить состав обрабатываемых ПДн, цели и условия обработки, сроки хранения ПДн различных категорий. Перечень обрабатываемых в ИСПДн персональных данных должен быть утверждён приказом руководителя.

Определение правовых оснований обработки ПДн

- Перечень персональных данных - подробный, четко структурированный документ, содержащий информацию обо всех категориях и видах персональных данных, обрабатываемых в организации с применением средств автоматизации или без такового

Определение правовых оснований обработки ПДн

- изучение внутренней и внешней организационно-распорядительной документации;
- интервьюирование должностных лиц и специалистов оператора;
- идентификация точек входа и выхода информации ограниченного распространения и пути её миграции в структуре оператора;
- изучение содержания входящих и исходящих информационных потоков всех типов и направлений;

Определение правовых оснований обработки ПДн

- выявление в информационных потоках, сопровождающих бизнес-процессы оператора, персональных данных и других видов информации ограниченного распространения, обрабатываемых как с использованием, так и без использования средств автоматизации;
- анализ оснований и установление категорий и степеней конфиденциальности выявленных персональных данных и других видов информации ограниченного распространения, циркулирующих в структуре оператора;

Определение правовых оснований обработки ПДн

- уточнение целей, выявление условий начала и прекращения и определение сроков обработки (хранения) для каждой установленной категории персональных данных и другой информации ограниченного распространения;
- определение структурных подразделений и должностных лиц оператора, использующих в своей деятельности персональные данные и другую информацию ограниченного распространения, их правомочности в принятии решений, касающихся определения целей, условий и сроков обработки указанной информации;

Определение правовых оснований обработки ПДн

- составление и представление на утверждение Перечня сведений конфиденциального характера (Перечня персональных данных), отвечающего
- требованиям руководящих документов и содержащего информацию, необходимую и достаточную для достижения целей работ.

Определение правовых оснований обработки ПДн

Появление ПДн вероятнее всего:

- оформления трудовых договоров с работниками;
- ведения учёта труда работников и их оплаты;
- осуществления обязательного государственного пенсионного страхования работников;
- осуществления обязательного пенсионного страхования в негосударственном пенсионном фонде;
- продажи товаров дистанционным способом;
- оказания услуг связи;
- оказания услуг по обязательному (добровольному) медицинскому страхованию граждан;
- оказания банковских услуг;

ШАГ 3. ПОЛУЧЕНИЕ СОГЛАСИЙ НА ОБРАБОТКУ ПДН

ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНСТИТУТ МАТЕМАТИКИ И КОМПЬЮТЕРНЫХ НАУК

Установление необходимого уровня правоотношений между оператором и субъектом персональных данных.

- Согласие субъекта на обработку его ПДн должно быть при необходимости получено, в том числе и в письменной форме.
- Порядок реагирования на запросы со стороны субъектов персональных данных, внесения изменений в ПДн, а также условия прекращения обработки ПДн должны быть также определены документально в соответствующих приказах, инструкциях и процедурах, определяющих в том числе степень участия должностных лиц в обработке ПДн и характер их взаимодействия между собой.

Согласие не требуется

- обработка персональных данных осуществляется на основании федерального закона, устанавливающего её цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора;
- обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных;
- обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

Согласие не требуется

- обработка персональных данных необходима для доставки почтовых отправлений организациями почтовой связи, для осуществления операторами электросвязи расчетов с пользователями услуг связи за оказанные услуги связи, а также для рассмотрения претензий пользователей услугами связи;
- обработка персональных данных осуществляется в целях профессиональной деятельности журналиста либо в целях научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и свободы субъекта персональных данных;
- обработка персональных данных необходима в связи с реализацией международных договоров Российской Федерации о реадмиссии;
- осуществляется обработка персональных данных, подлежащих опубликованию в соответствии с федеральными законами, в том числе персональных данных лиц, замещающих государственные должности, должности государственной гражданской службы, персональных данных кандидатов на выборные государственные или муниципальные должности.

Работы включают в себя:

- анализ состава и содержания документов, подтверждающих легитимность обработки оператором персональных данных, в отдельности для каждого из субъектов, чьи ПДн обрабатываются оператором;
- идентификацию субъектов персональных данных, чьё разрешение на обработку их ПДн отсутствует, и принятие решения о необходимости или об отсутствии необходимости получения такого разрешения;
- разработку (корректировку) договоров с сотрудниками и клиентами организации- оператора в части внесения в них положений об условиях и формах обработки ПДн оператором и о согласии на такую обработку;
- разработку типовых форм согласия и направление запросов субъектам для получения их согласия на обработку их ПДн оператором;

Работы включают в себя:

- организацию юридически значимого получения согласия через web-формы;
- формирование юридически значимой базы согласий субъектов на обработку их ПДн;
- разработку процедур и порядка реагирования на отсутствие ответа от субъекта, подтверждающего его согласие на обработку его ПДн;
- разработку процедур и порядка реагирования на отзыв субъектом своего согласия на обработку его ПДн;
- идентификацию ПДн, подлежащих опубликованию в соответствии с федеральными законами, в инфраструктуре оператора;

Работы включают в себя:

- установление наличия или отсутствия целей обработки персональных данных, подлежащих опубликованию в соответствии с федеральными законами, в инфраструктуре оператора, направление субъектам при необходимости запросов о предоставлении таких ПДн для обработки оператором;
- идентификацию прочих ПДн, согласия субъектов на обработку которых не требуется в соответствии с частью 2 статьи б федерального закона № 152-ФЗ «О персональных данных»;
- формирование документированной, юридически значимой доказательной базы правомерности обработки ПДн, осуществляемой без согласия субъекта персональных данных.

ШАГ 4. ОПРЕДЕЛЕНИЕ ПОРЯДКА РЕАГИРОВАНИЯ

ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНСТИТУТ МАТЕМАТИКИ И КОМПЬЮТЕРНЫХ НАУК

Определение порядка реагирования

- оператор должен предоставлять субъекту персональных данных сведения о его персональных данных в установленном формате;
- оператор должен блокировать ПДн в ряде случаев, предусмотренных законом;
- оператор должен уничтожать ПДн в ряде случаев, предусмотренных законом.

Определение порядка реагирования

Необходимо провести следующие работы:

- определить лиц, ответственных за соблюдение требований № 152-ФЗ «О персональных данных» в части реагирования на запросы субъектов персональных данных;
- разработать механизмы реагирования на запросы субъектов персональных данных (например, документальные регламенты или процедуры);
- ввести в действие в рамках организации-оператора разработанные регламенты реагирования на запросы субъектов персональных данных;
- разработать типизированные шаблоны ответов на запросы субъектов персональных данных;
- провести мероприятия по проверке выполнения разработанных механизмов реагирования на запросы субъектов персональных данных.

Определение порядка реагирования

Регламенты реагирования должны содержать следующие сведения:

- лицо (список лиц), ответственных за получение запросов субъектов персональных данных;
- порядок проверки корректности сведений указанных в форме запроса субъекта персональных данных;
- порядок формирования ответа на запрос субъекта персональных данных;
- порядок внесения в ПДн уточняющих и/или корректирующих сведений, полученных от субъекта персональных данных;
- лицо (список лиц), ответственных за определение фактов достижения целей обработки ПДн;
- порядок блокирования и/или уничтожения ПДн при наступлении факта достижения цели обработки ПДн;
- лицо (список лиц), ответственных за контроль наличия согласий субъектов персональных данных, а также за получение отзыва согласия субъектов персональных данных;
- порядок блокирования и/или уничтожения ПДн при отзыве согласия субъекта персональных данных.

Определение порядка реагирования

Ответ на запрос:

- подтверждение факта обработки персональных данных оператором, а также цель такой обработки;
- способы обработки персональных данных, применяемые оператором;
- сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
- перечень обрабатываемых персональных данных и источник их получения;
- сроки обработки персональных данных, в том числе сроки их хранения;
- сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

ШАГ 5. УВЕДОМЛЕНИЕ (В СЛУЧАЕ НЕОБХОДИМОСТИ) УПОЛНОМОЧЕННОГО ОРГАНА ПО ЗАЩИТЕ ПДН

ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНСТИТУТ МАТЕМАТИКИ И КОМПЬЮТЕРНЫХ НАУК

Уведомление (в случае необходимости) уполномоченного органа по защите ПДн

- определить необходимость подачи уведомления об обработке персональных данных в уполномоченный орган по защите прав субъектов персональных данных;
- подготовить правовое обоснование отсутствия необходимости подачи уведомления об обработке ПДн, если все обрабатываемые ПДн подпадают под исключения, предусмотренные частью 2 статьи 22 Федерального закона № 152-ФЗ;
- в случае необходимости, подготовить уведомление об обработке ПДн в соответствии с требованиями регулятора и отправить в уполномоченный орган.

Уведомлять не требуется

- относящихся к субъектам персональных данных, которых связывают с оператором трудовые отношения;
- полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных, если его ПДн 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;
- относящихся к членам (участникам) общественного объединения или религиозной организации и обрабатываемых соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что ПДн не будут распространяться без согласия субъектов персональных данных, данного в письменной форме;

Уведомлять не требуется

- являющихся общедоступными персональными данными;
- включающих в себя только фамилии, имена и отчества субъектов персональных данных;
- необходимых в целях однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях;
- включенных в ИСПДн, имеющие в соответствии с федеральными законами статус федеральных автоматизированных информационных систем, а также в государственные ИСПДн, созданные в целях защиты безопасности государства и общественного порядка;
- обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности ПДн при их обработке и к соблюдению прав субъектов персональных данных.

ШАГ 6. ИДЕНТИФИКАЦИЯ ИСПДН И ИХ КЛАССИФИКАЦИЯ

ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНСТИТУТ МАТЕМАТИКИ И КОМПЬЮТЕРНЫХ НАУК

Идентификация и классификация

- выделение (идентификация) и определение состава ИСПДн, имеющихся в ИТ- инфраструктуре предприятия;
- классификация ИСПДн в соответствии с нормативно-правовым и актами Минкомсвязи, ФСТЭК России и ФСБ России;
- разработка первого комплекта обязательных документов для каждой идентифицированной ИСПДн.

Идентификация и классификация

Идентификация ИСПДн

- Изучение бизнес-процессов
- Составление схемы сети
- Составление карты сети
- Сегментация сети
- Принятие решения (экранирование)

Классификация ИСПДн

- Назначение комиссии
- Изучение классификационных признаков
- Разработка и утверждение Акта классификации

ШАГ 7. РАЗРАБОТКА МОДЕЛЕЙ УГРОЗ

ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНСТИТУТ МАТЕМАТИКИ И КОМПЬЮТЕРНЫХ НАУК

Разработка моделей угроз

- адекватно оценить необходимость реализации тех или иных мероприятий по обеспечению безопасности ПДн исходя из состояния защищённости ИСПДн на текущий момент;
- спрогнозировать развитие СЗПДн на краткосрочную и среднесрочную перспективу, провести оптимизацию бюджетов соответствующих подразделений, выставить приоритеты принимаемым мерам по обеспечению безопасности ПДн.

Разработка моделей угроз

Определение общего перечня угроз безопасности ПДн

- Угрозы безопасности ПДн при их обработке в ИСПДн представляются в виде совокупности возможных источников угроз НСД, уязвимостей программного и аппаратного обеспечения ИСПДн, способов реализации угроз, объектов воздействия (носителей защищаемой информации, директориев, каталогов, файлов с ПДн или самих ПДн) и возможных деструктивных воздействий.

Разработка моделей угроз

Определение уровня исходной защищённости ИСПДн

- По результатам анализа предоставленных исходных данных и результатов обследования состояния защищённости ИСПДн определяется уровень её исходной защищённости, характеризуемый числовым коэффициентом.

Разработка моделей угроз

Расчёт актуальности полученных угроз безопасности ПДн для анализируемой ИСПДн

- На данном этапе проводится экспертная оценка сформированных наборов угроз безопасности ПДн с точки зрения частоты (вероятности) их реализации с определением для каждой угрозы соответствующего числового коэффициента с последующей вербальной интерпретацией полученных коэффициентов для всех выявленных угроз в диапазоне «низкая - средняя - высокая - очень высокая».

Разработка моделей угроз

Создание документа «Модель угроз безопасности персональных данных при их обработке в ИСПДн»

- описание объекта моделирования (анализируемой ИСПДн) и его характеристик;
- перечни характерных для данной ИСПДн источников угроз безопасности персональных данных, уязвимостей компонентов ИСПДн, способов реализации данных уязвимостей в рамках анализируемой ИСПДн, объектов воздействия и последствий реализации вышеуказанных способов;
- перечни характерных для данной ИСПДн угроз безопасности ПДн;
- оценку ущерба (опасности) для субъектов персональных данных от реализации тех или иных угроз безопасности ПДн;
- анализ рисков реализации вышеуказанных угроз;
- выводы относительно класса криптосредств, обязательных к использованию в анализируемой ИСПДн.

ШАГ 8. ПРОЕКТИРОВАНИЕ И РЕАЛИЗАЦИЯ СЗПДН

ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНСТИТУТ МАТЕМАТИКИ И КОМПЬЮТЕРНЫХ НАУК

Проектирование и реализация СЗПДн

- *«Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии».*

Проектирование и реализация СЗПДн

Организация проведения работ по защите ПДн

- Основой для организации работ по построению СЗПДн в организации- операторе служит **концепция информационной безопасности.**
- Данный документ определяет нормативно-правовое обеспечение, цели, задачи и основные принципы создания системы обеспечения безопасности ПДн, содержание базовых компонентов СЗПДн и основные направления их формирования и развития.

Проектирование и реализация СЗПДн

Разработка требований по обеспечению безопасности ПДн при обработке в ИСПДн

- Для каждой из ИСПДн, используемых в организации, с учётом их класса, обрабатываемых персональных данных, особенностей и условий функционирования выполняется разработка требований по обеспечению безопасности ПДн при обработке в ИСПДн, определяющих необходимые для реализации меры обеспечения безопасности. Данные требования являются основой для разработки технического задания, выбора средств защиты и технического проектирования.

Проектирование и реализация СЗПДн

Разработка технического задания

- обоснование разработки СЗПДн;
- исходные данные создаваемой (модернизируемой) ИСПДн в техническом, программном, информационном и организационном аспектах;
- класс ИСПДн;
- ссылку на нормативные документы, с учётом которых будет разрабатываться СЗПДн и приниматься в эксплуатацию ИСПДн;
- конкретизацию мероприятий и требований к СЗПДн;
- перечень предполагаемых к использованию сертифицированных средств защиты информации;
- обоснование проведения разработок собственных средств защиты информации при невозможности или нецелесообразности использования имеющихся на рынке сертифицированных средств защиты информации;
- состав, содержание и сроки проведения работ по этапам разработки и внедрения СЗПДн.

Проектирование и реализация СЗПДн

Проектирование СЗПДн

Система защиты в типовом варианте представляет собой совокупность следующих подсистем:

- управления доступом;
- регистрации и учёта;
- обеспечения целостности;
- криптографической защиты;
- антивирусной защиты;
- обнаружения вторжений.

Проектирование и реализация СЗПДн

Внедрение и контроль

- Внедрение разработанных при проектировании ИСПДн технических решений осуществляется в соответствии с технической документацией на внедряемые средства и системы.
- По окончании внедрения средств защиты проводится итоговый контроль защищённости.

Проектирование и реализация СЗПДн

Разработка документации

- Ввод СЗПДн в эксплуатацию предполагает собой не только внедрение технических средств, но и разработку пакета организационной и методической документации, позволяющей эффективно оценивать и контролировать состояние защищённости ИСПДн.
- **Инструкции**
- **Регламенты**
- **Журналы**

ШАГ 9. ОПИСАНИЕ СЗПДН. ОЦЕНКА СООТВЕТСТВИЯ (АТТЕСТАЦИЯ)

ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНСТИТУТ МАТЕМАТИКИ И КОМПЬЮТЕРНЫХ НАУК

Описание СЗПДн. Оценка соответствия (аттестация)

- Подтверждение работоспособности информационной системы организации с внедрёнными в её инфраструктуру средствами и системами защиты ПДн и подтверждение соответствия каждой идентифицированной ИСПДн требованиям к безопасности информации, предъявляемым согласно присвоенному ей классу и принятой модели угроз, с получением документа, удостоверяющего соответствие.

ШАГ 10. ОБРАБОТКА ПДН БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНСТИТУТ МАТЕМАТИКИ И КОМПЬЮТЕРНЫХ НАУК

Обработка ПДн без использования средств автоматизации

Провести инвентаризацию и определить места хранения носителей ПДн

Необходимо определить перечни ПДн (материальных носителей ПДн), обработка которых осуществляется без использования средств автоматизации, и для каждой категории таких ПДн определить места их хранения и установить перечень лиц, осуществляющих обработку ПДн либо имеющих к ним доступ.

Должно быть обеспечено размещение ПДн на материальных носителях таким образом, чтобы ПДн были обособлены от другой информации и имели идентичные цели их обработки, т.е. на одном материальном носителе не должно быть ПДн, обрабатываемых для различных целей.

Хранение материальных носителей ПДн должно быть организовано таким образом, чтобы:

- обеспечивалось раздельное хранение материальных носителей ПДн, обработка которых осуществляется в различных целях;
- обеспечивалась сохранность ПДн и исключался несанкционированный доступ к ним (перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц ответственных за реализацию указанных мер, устанавливаются организацией-оператором).

Обработка ПДн без использования средств автоматизации

Уведомить персонал

Все работники организации-оператора, допущенные к неавтоматизированной обработке ПДн, должны быть уведомлены под роспись:

- о факте обработки ими ПДн;
- о категориях обрабатываемых ПДн;
- об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами организации-оператора.

Обработка ПДн без использования средств автоматизации

Разработать внутренние нормативные документы

Формы документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны быть приведены в соответствие следующим требованиям:

- типовая форма или связанные с ней документы (инструкция по её заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;
- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных (при необходимости наличия такого согласия);
- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;
- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

Обработка ПДн без использования средств автоматизации

Принять меры по обеспечению безопасности ПДн

Несмотря на то, что меры по обеспечению безопасности материальных носителей ПДн для каждой организации-оператора индивидуальны и выбираются ею самостоятельно, следующие меры и средства рекомендуются как базовые:

- меры, обеспечивающие безопасное хранение материальных носителей ПДн. К таким мерам относятся закупка и установка сейфов, металлических шкафов, создание специально оборудованных помещений и т.п.;
- меры защиты от НСД к ПДн (материальным носителям ПДн). К таким мерам относятся установка замков, систем сигнализации и видео наблюдения и т.п.;
- средства гарантированного уничтожения ПДн (материальных носителей ПДн). К таким относятся средства измельчения, сжигания, размагничивания и другие им подобные, гарантирующие невозможность последующего восстановления данных.

ШАГ 11. ПОСТОЯННЫЙ КОНТРОЛЬ

ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНСТИТУТ МАТЕМАТИКИ И КОМПЬЮТЕРНЫХ НАУК

Постоянный контроль

Не стоит останавливаться…

Планирование, реализация, проверка, модернизация

- Аудит
- Инструктаж
- Обучение
- Ведение журналов
- Отчеты о проверках
- Планы по модернизации

Спасибо. Вопросы?

kabazhin@gmail.com
www.kbinform.ru
(3452) 768-800