ФГБОУ ВПО «Воронежский государственный
технический университет»

Кафедра систем информационной безопасности

134-2015

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к практическим занятиям по дисциплине
«Основы информационной безопасности»
для студентов специальностей
090301 «Компьютерная безопасность»,
090302 «Информационная безопасность
телекоммуникационных систем»,
090303 «Информационная безопасность
автоматизированных систем»
очной формы обучения

Воронеж 2015

Составители: д-р техн. наук О. Н. Чопоров, Н. Н. Корнеева

УДК 004.056.5

Методические указания к практическим занятиям по дисциплине «Основы информационной безопасности» для студентов специальностей 090301 «Компьютерная безопасность», 090302 «Информационная безопасность телекоммуникационных систем», 090303 «Информационная безопасность автоматизированных систем» очной формы обучения / ФГБОУ ВПО «Воронежский государственный технический университет»; сост. О. Н. Чопоров, Н. Н. Корнеева. – Воронеж, 2014. 48 с.

В методических указаниях приведены основные понятия и краткие теоретические сведения для разработки студентами политик безопасности для однотипных объектов. В ходе выполнения приведенных заданий студенты получат практические навыки по составлению документов, регламентирующих порядок обеспечения информационной безопасности в различных организациях.

Методические указания подготовлены в электронном виде в текстовом редакторе MS Word 2013 и содержатся в файле Чопоров_ПЗ_Основы ИБ.pdf.

Библиогр.: 10 назв.

Рецензент д-р техн. наук, проф. А. Г. Остапенко

Ответственный за выпуск зав. кафедрой д-р техн. наук, проф. А. Г. Остапенко

Издается по решению редакционно-издательского совета Воронежского государственного технического университета

ВАРИАНТЫ ОБЪЕКТОВ ДЛЯ ВЫПОЛНЕНИЯ ПРАКТИЧЕСКИХ РАБОТ

Выполнение практических работ происходит индивидуально. Возможны обсуждения этапов выполнения по ходу проведения занятия, а также запланирована дискуссия по окончанию с обсуждением результатов и внесением корректировок.

Прежде чем приступить к выполнению серии практических работ, студенту необходимо выбрать интересный для себя объект из предложенного ниже списка, для которого он будет составлять политики безопасности, и внимательно ознакомиться с его описанием:

1. Детская поликлиника «Солнце». Оказывает услуги медицинского характера; должна иметь возможность записи пациентов через Интернет, в регистратуре и получение талона у лечащего врача; результаты обследования должны заноситься в базу поликлиники и дополнительно дублироваться в карту пациента (бумажный носитель); должна предусматриваться система хранения персональных медицинских карт в поликлинике; должна предусматриваться возможность получения удаленного доступа пациента к результатам обследований; необходимо учитывать возможность перевода пациента и его данных в другое лечащее учреждение, а также получение дополнительных данных из других учреждений.
2. Туристическое агентство «Чемодан». Оказывает услуги туристического характера; должно иметь возможность оформления паспортов, виз, разрешений на вывоз несовершеннолетних детей за границу; бронирование и оплату санаториев, баз отдыха, гостиниц, экскурсий, перелета, трансфера.
3. Автошкола «Пятое колесо». Оказывает образовательные услуги; должна иметь возможность дистанционной записи на практические и дополнительные занятия; учета промежуточных результатов обучения.

4. Агентство недвижимости «Новоселье». Оказывает услуги по покупке/продаже/обмену/съему жилья.

5. Реабилитационный центр «Силушка богатырская». Оказывает восстановительные медицинские услуги пациентам всех возрастов; должен иметь возможность доступа к данным обследований пациента в других клиниках за большой период времени; помимо всех требований, предъявляемым к детской поликлинике (см. пункт 1) необходимо предусмотреть запись пациента в другие медицинские учреждения.

6. Страховое агентство «Цунами». Оказывает услуги в сфере страхования; должна предусматриваться возможность страхования жизни, здоровья, жилья, автосредства, отпуска и т.д.

7. Негосударственный пенсионный фонд «Гарантия». Оказывает услуги по формированию пенсионных выплат; должна поддерживаться функция «горячей линии»;

8. Управляющая компания «Теремок». Оказывает услуги по восстановлению и поддержке состояния жилищного фонда клиентов; должна иметь возможность взаимодействия с коммунальными службами, поставщиками услуг.

9. Центр занятости «Статус». Оказывает услуги по трудоустройству населения; должен предусматривать возможность сотрудничества с другими компаниями; проведения статистических исследований.

10. Охранное предприятие «Спокойствие». Оказывает услуги по охране различных объектов; должна поддерживаться функция оперативного внесения в базу состояние объектов охраны.

При выполнении практических занятий студенту выпадает роль сотрудника отдела информационной безопасности и технической защиты выбранного объекта, который представляет собой корпоративную информационную систему (КИС), обрабатывающую и хранящую персональные данные клиентов.

КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Политика безопасности (информации в организации) – совокупность документированных правил, процедур, практических приёмов или руководящих принципов в области безопасности информации (БИ), которыми руководствуется организация в своей деятельности.

Основной целью политики ИБ является общее описание правил работы с информацией компании. Наличие сформулированных и закрепленных на бумаге правил обеспечения информационной безопасности позволит достичь:

1. Стабильность защиты.
2. Независимость защиты от личных и профессиональных качеств исполняющего персонала.
3. Возможность контроля как защиты, так и процедур обработки информации.

Перед разработкой политики информационной безопасности (ИБ) должен быть проведен анализ активов, включающий их учет и оценку. Готовая политика должна иметь в своем составе отдельный раздел для каждого обнаруженного актива, группы взаимосвязанных активов или обособленной части актива компании в зависимости от ранее проведенного анализа их структуры и взаимосвязи.

В дополнение и исходя из политики ИБ могут быть разработаны другие документы, такие как руководства или стандарты. В отличии от политик они более конкретны, что выражается в привязке к определенному оборудованию, версиям программ или в точном указании необходимой последовательности действий для достижения заданного результата.

Политика ИБ разрабатывается специалистами ИБ компании для использования остальными сотрудниками компании. Поэтому, она должна быть изложена максимально просто, на обычном языке с использованием минимума специальной лексики только там, где это необходимо.

Практическое занятие № 1
Политика «Требования по обеспечению информационной безопасности»

Цель занятия: рассмотрение основных и наиболее важных моментов при разработке политики «Требования по обеспечению информационной безопасности» для выбранной КИС.

Задачи: формализовать требования по обеспечению безопасности ресурсов КИС в соответствии с действующим законодательством [1, 9].

Ход работы

Преступим к разработке политики безопасности «Требования по обеспечению информационной безопасности (ИБ)» для выбранной КИС. Выделим следующие разделы для будущего документа:

1. Общие положения;
2. Рабочее место пользователя;
3. Парольная политика;
4. Работа с электронной почтой;
5. Работа в сети Интернет;
6. Действия в нестандартных ситуациях;
7. Ответственность.

Ниже подробно рассмотрим содержание перечисленных разделов с представленными в скобках примерами. Отметим сразу, что результаты по ходу работы будем заносить в форму 1 (прил. 1).

Рабочее место пользователя

Начнем разработку нашей политики с данного раздела, в котом отметим следующие моменты:

– Правила предоставления сотруднику рабочего места и ограничение прав на его эксплуатацию *(Для выполнения своих должностных обязанностей сотруднику компании*

выделяется персональный компьютер (ПК) с предустановленным программным обеспечением (ПО) и доступом к локально-вычислительной сети (ЛВС) компании. ПК предоставляется сотруднику во временное пользование на период работы в организации и должен использоваться им для служебных целей. Установку, настройку, а также подключение к ЛВС выполняют только сотрудники, уполномоченные на перечисленные операции);

– Исходя из важности обеспечения сохранности информации, введем правило создания резервной копии *(Сотрудник должен периодически* (как часто?) *создавать резервные копии, сохраняя важную информацию в выделенной папке файлового сервера компании; резервная копия информации создается автоматически* (как часто и какие действия необходимы со стороны сотрудника для исключения ошибок)*)*;

– Исключения доступа к рабочему месту сотрудника посторонних лиц *(Оставляя рабочее место, даже на короткое время, пользователь обязан заблокировать доступ к работающему ПК* (можно использовать средства операционной системы или, в случае наличия, средствами защиты информации, которыми оснащен ПК));

– Действия, которые запрещено производить сотрудникам *(Открывать корпус ПК и изменять его конфигурацию; Несанкционированно изменять настройки ПО, параметры доступа к ресурсам КИС; Отключать антивирусное ПО, а также предусмотренные средства защиты; Подключать к ЛВС несанкционированное оборудование* (Например, активное сетевое оборудование, незарегистрированные компьютеры и т.д.)*; умышленно использовать недокументированные свойства и ошибки в ПО или в настройках средств защиты; Осуществлять действия, направленные преодоление систем безопасности, получение несанкционированного доступа к ресурсам КИС, ухудшение рабочих характеристик КИС, перехват информации, циркулирующей в КИС; Оставлять переносные компьютеры*

и средства хранения информации без личного присмотра, в случаях, если это может привести к их краже (можно ввести правило использования замков для переносных компьютеров или требование по помещению их в закрывающийся на ключ шкаф на время обеденного перерыва и после окончания рабочего дня)*; Осуществлять обработку информации ограниченного доступа на ПК в присутствии лиц, не уполномоченных для доступа к данной информации, если при этом указанные лица смогут ознакомиться с обрабатываемой информацией; Несанкционированно записывать и хранить информацию на неучтенных носителях информации, а также оставлять без личного присмотра на рабочем месте носители информации и распечатки, содержащие информацию ограниченного доступа; Хранить и обрабатывать развлекательные мультимедийные файлы в КИС; Допускать к работе на ПК лиц, не имеющих прав доступа в КИС).*

Парольная политика

Для предотвращения несанкционированного доступа к ресурсам КИС используются пароли и/или аппаратные средства аутентификации.

Рассмотрим основные правила, которые должен выполнять сотрудник организации:

– Сотрудники обязаны обеспечить безопасное хранение *пароля и/или средства утентификации*, исключающие их утерю или разглашение;

– Рекомендуется изменять пароли с периодичностью *не более 90 дней*, при смене пароля новое значение должно отличаться от предыдущего не менее чем в *3-х* позициях;

– Запрещается сообщать кому-либо, даже администраторам сети, свой пароль для доступа к информационным ресурсам КИС;

– В случае подозрения на разглашение пароля необходимо немедленно изменить пароль и

проинформировать начальника *(своего отдела, отдела безопасности)*;

– Требования, в соответствии с которыми сотрудник обязан создавать пароль (пароль должен состоять не менее чем из *восьми* символов; пароль не должен быть легко угадываемым *(пароль не должен включать повторяющуюся, последовательность каких-либо символов (например, «111111», «аааааа», «12345», «qwerty», «йцукен» и т.п.), пароль не должен включать в себя легко подбираемые сочетания символов (имена, фамилии, наименования, клички домашних животных, даты рождения и т.д.) и общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.)*);

Работа с электронной почтой

При эксплуатации электронной почты, сотрудники обязаны выполнять следующие требования:

– Допускается использовать корпоративную электронную почту только для выполнения своих служебных обязанностей;

– Запрещается самовольно менять настройки почтовой системы;

– Запрещается отправлять сообщения противозаконного, враждебного или неэтического содержания;

– Запрещается использовать публичные сервисы электронной почты *(например, Yahoo, Mail, Yandex и др.)* для осуществления корпоративной деятельности;

– Для защиты сообщений от подмены, модификации и прочтения третьими лицами следует использовать *средства шифрования электронной почты* и *электронной подписи*;

– При получении электронных содержаний сомнительного содержания и/или из незнакомого источника не следует открывать файлы, вложенные в сообщение, так как они с большой вероятностью могут содержать вирусы. *Такие сообщения необходимо удалять*;

– Не следует отвечать на подозрительные письма, а также сообщать любые данные о себе, если сотрудник не доверяет отправителю письма;

– Запрещается в личных целях публиковать личный корпоративный адрес сотрудника при заполнении анкет, так как эти данные могут быть использованы для рекламных рассылок;

– Запрещается самостоятельно настраивать и включать автоматическую пересылку сообщений корпоративной электронной почты на внешние адреса электронной почты.

Работа в сети Интернет

При использовании Интернет, пользователи обязаны выполнять следующие требования:

– допускается использовать ресурсы Интернет только для выполнения своих служебных обязанностей;

– запрещается посещать ресурсы Интернет, содержащие материалы противозаконного, экстремистского или неэтического характера, использовать доступ в Интернет в развлекательных целях;

– запрещается несанкционированно размещать какую-либо информацию в Интернет;

– запрещается использовать Интернет для несанкционированной передачи (выгрузки) или получения (загрузки) материалов, защищенных авторским правом;

– запрещается несанкционированно загружать программы из сети Интернет и запускать их;

– запрещается осуществлять попытки несанкционированного доступа к защищенным ресурсам Интернет *(перебор паролей, использование уязвимостей и неправильных настроек информационных систем)*;

– запрещается осуществлять туннелирование сетевого трафика при обращении к ресурсам сети Интернет через корпоративные прокси сервера;

– запрещается несанкционированное использование систем мгновенного обмена сообщениями *(Instant Messaging),*

систем передачи голоса по IP-протоколу *(VOIP),* систем видеосвязи по IP-протоколу *(Skype),* систем для удалённого доступа и общего доступа к рабочему столу.

Действия в нестандартных ситуациях

Сотрудники, пользующиеся ресурсами КИС обязаны немедленно ставить в известность своего непосредственного руководителя и/или начальника отдела информационной безопасности и технической защиты, в случае возникновения или возможного возникновения следующих событий:

– разглашения учетных данных; потери, кражи средств аутентификации;

– несанкционированных *(произведенных с нарушением установленного порядка)* изменений в конфигурации программных или аппаратных средств рабочей станции;

– фактов совершения попыток несанкционированного доступа к ресурсам КИС;

– фактов потери, кражи компьютеров или носителей информации, особенно если они содержали информация ограниченного доступа;

– заражение ПК пользователя вирусами;

– сбоев в работе средств защиты информации;

– в любых других случаях, если, по мнению пользователя, возникают риски нарушения безопасности информации.

Ответственность

Ответственность за выполнение требований Политики возлагается на всех работников, являющихся пользователями КИС.

Любой работник компании, нарушивший требования данного политики, может быть, подвергнут дисциплинарному наказанию, в соответствии с законодательством РФ и трудовым договором.

Общие положения

Итак, разработав основные разделы политики, вернемся к общим положениям. В данном разделе должны быть отражены следующие моменты:

– На кого будет распространяться данный документ *(все пользователи КИС; персонал, непосредственно работающий с клиентами)* и в какой момент они должны с ним ознакомиться *(только при получении первичного доступа к КИС, при получении первичного доступа к КИС, а также ежегодно в рамках проведения внутренних профилактических работ по обеспечению ИБ);*

– Необходимо предупредить работников организации об ответственности и обязанности соблюдения установленных документом правил *(каждый пользователь несет персональную ответственность за свои действия и обязан строго соблюдать установленные правила по работе с программными и техническими средствами)*;

– Обоснование уникальных учетных записей *(С целью соблюдения принципа персональной ответственности за свои действия каждому пользователю назначается персональное уникальное имя. Запрещается использовать чужую учетную запись, а также передавать кому-либо свои учетные данные);*

– Ресурсы КИС предоставляются пользователям для осуществления ими своих обязанностей, связанных с деятельностью компании. При этом соблюдают принципы разумной достаточности и минимальной необходимости. *(Сотруднику компании разрешается пользоваться только той информацией и в том объеме, которые ему необходимы для выполнения своих должностных обязанностей. Сотрудник не имеет права предпринимать попыток получить доступ к ресурсам КИС, не пройдя процедуру официального получения разрешения на доступ к ресурсам.)*;

– Осуществление контроля за правильностью обработки информации, ввиду принадлежности информационных ресурсов организации *(Информация,*

циркулирующая в КИС, является собственностью компании. Компания оставляет за собой право протоколировать и контролировать действия работников при обработке информации в КИС);

– Необходимо минимизировать возможность внешнего проникновения в КИС *(Пользователи не должны разглашать информацию о процедурах и технической реализации защиты информации в КИС)*;

– Обязанность работников сообщать о фактах нарушения установленных в документе правил *(Пользователи должны информировать своего непосредственного руководителя и/или уполномоченного сотрудника отдела информационной безопасности и технической защиты обо всех фактах нарушения данной политики)*.

Контрольные вопросы

1. Дайте определение и опишите основные характеристики политики безопасности.
2. Обоснуйте важность основных положений раздела «Рабочее место». Какие дополнительные требования необходимо ввести для Вашей организации?
3. Опишите как бы Вы ввели процедуру официального получения разрешения на доступ к ресурсам?
4. Составьте список возможностей Вашей организации, реализуемых с помощью сети Интернет. Каких доработок в связи с особенностями работы компании требует раздел «Работа в сети Интернет»?
5. Необходима ли разработка и внедрение политики безопасности в рассматриваемые на практических занятиях организации? Обоснуйте свой ответ.

Практическое занятие № 2
Политика «Обработка персональных данных в организации»

Цель занятия: рассмотрение основных и наиболее важных моментов при разработке политики «Обработка персональных данных в организации» для выбранной организации в соответствии с требованиями законодательства о ПДн [1, 5, 6, 7, 10].

Задачи: определить принципы, порядок и условия обработки персональных данных (ПДн) абонентов, работников организации и иных лиц, чьи ПДн обрабатываются организацией, а также третьими лицами по поручению организации.

Ход работы

Преступим к разработке политики безопасности «Обработка персональных данных (ПДн) в организации» для выбранной организации. Раскроем необходимые в работе определения терминов и сокращений [2].

Термины и сокращения

Абонент – физическое или юридическое лицо, с которым заключен Договор о предоставлении услуг связи;

Персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

Биометрические персональные данные – сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных;

Оператор персональных данных – государственный орган, муниципальный орган, юридическое или физическое

лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;

Локальный нормативный акт (ЛНА) – локальный нормативный акт.

Ниже подробно изчим содержание рассматриваемой Политики. По окончанию студентам предлагается ответить на контрольные вопросы, выполнить задания, результаты занести в форму ответов. (прил. 2).

Конфиденциальность персональных данных

Главным условием при обработке персональных данных является конфиденциальность. Организация и иные лица, получившие доступ к ПДн, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта ПДн, если иное не предусмотрено федеральным законом *(например в рамках оперативно-розыскной деятельности. Обеспечение безопасности ПДн, обрабатываемых в информационных системах при обеспечении оперативно-розыскных мероприятий, осуществляется в соответствии с законодательством РФ об оперативно-розыскной деятельности).*

Права субъекта персональных данных

Субъект ПДн принимает решение о предоставлении его ПДн и даёт согласие на их обработку свободно, своей волей и в своём интересе. Согласие на обработку ПДн может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным

законом;

Обязанность предоставить доказательство получения согласия субъекта ПДн на обработку его персональных данных или доказательство наличия оснований возлагается на организацию;

Субъект ПДн имеет право на получение информации, касающейся обработки его персональных данных *(подтверждение факта обработки ПДн оператором; правовые основания и цели обработки ПДн; цели и способы обработки ПДн; сроки обработки ПДн, в том числе сроки их хранения; наименование и адрес лица, осуществляющего обработку ПДн по поручению оператора, если обработка поручена или будет поручена такому лицу)*, если такое право не ограничено в соответствии с федеральными законами. Субъект ПДн вправе требовать от организации уточнения его персональных данных, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав. Сведения предоставляются субъекту ПДн в доступной форме, и в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн;

Обработка ПДн в целях продвижения товаров, работ, услуг на рынке путём осуществления прямых контактов с потенциальным потребителем с помощью средств связи, допускается только при условии предварительного согласия субъекта ПДн. Организация обязана немедленно прекратить по требованию субъекта персональных данных обработку его ПДн в вышеуказанных целях.

Получение персональных данных

Получение персональных данных в организации организуется таким способом, чтобы не нарушить конфиденциальность собираемых ПДн.

Обработка персональных данных

Обработка ПДн в организации допускается в следующих случаях:

- *обработка ПДн необходима для предоставления государственной или муниципальной услуги;*
- *обработка ПДн необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн, а также для заключения договора по инициативе субъекта ПДн или договора, по которому субъект ПДн будет являться выгодоприобретателем или поручителем;*
- *обработка ПДн осуществляется с согласия субъекта ПДн на обработку его ПДн;*
- *обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн, если получение согласия субъекта ПДн невозможно;*
- *обработка ПДн необходима для осуществления прав и законных интересов организации или третьих лиц, либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта ПДн;*
- *обработка ПДн необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта ПДн;*
- *обработка ПДн осуществляется в статистических или иных исследовательских целях, за исключением целей продвижения товаров, работ, услуг на рынке, политической*

агитации, при условии обязательного обезличивания ПДн;

- *осуществляется обработка ПДн, доступ неограниченного круга лиц к которым предоставлен субъектом ПДн, либо по его просьбе (общедоступные ПДн);*
- *осуществляется обработка ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.*

Обработка персональных данных субъектов ПДн в организации осуществляется в целях:

- Предоставление услуг связи *(Обеспечение безопасности тайны связи и сведений об абонентах при обработке информации в системах и сетях связи осуществляется в соответствии с требованиями законодательства РФ о связи);*
- *Обеспечение трудовых и производственных процессов и выполнения законодательства РФ связанного с трудовыми отношениями;*
- *Учет и регистрация посетителей офисов организации;*
- *Предоставление услуг, неразрывно связанных с услугами связи;*
- *Выполнение иных требований законодательства РФ.*

Организация является оператором ПДн, самостоятельно или совместно с другими лицами организует и (или) осуществляет обработку ПДн, а также определяет цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн;

Обработка ПДн в организации может осуществляться:

– работниками организации;

*– другими лицами, осуществляющими обработку ПДн по поручению организации (*Обработка ПДн

другими лицами может осуществляться только на основании договора, в котором содержится поручение на обработку ПДн. В поручении должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку ПДн, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность ПДн и обеспечивать безопасность ПДн при их обработке, а также должны быть указаны требования к защите обрабатываемых ПДн).

Рассмотри основные принципы работы с ПДн:

- *Обработка ПДн должна осуществляться на законной и справедливой основе;*
- *Обработке подлежат только ПДн, которые отвечают целям их обработки;*
- *Обработка ПДн должна ограничиваться достижением конкретных, заранее определенных и законных целей;*
- *Не допускается обработка ПДн, несовместимая с целями сбора ПДн;*
- *Содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки;*
- *Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки;*
- *Не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой.*

При обработке ПДн должны быть обеспечены точность ПДн, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн. В

организации должны приниматься необходимые меры по удалению или уточнению неполных или неточных данных. Ответственность за своевременное предоставление в организацию сведений об изменении ПДн, обрабатываемых в организацию, возлагается на субъектов ПДн, которым они принадлежат.

Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если иной срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн. Обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом *(Сроки обработки (хранения) ПДн определяются в соответствии со сроком действия договора с субъектом ПДн, приказом [3], сроками исковой давности, а также иными сроками, установленными законодательством. Хранение ПДн после истечения срока хранения допускается только после их обезличивания)*;

Обработка в организации специальных категорий ПДн, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, допускается только в случаях, предусмотренных федеральным законодательством. Обработка указанных специальных категорий ПДн должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась их обработка;

Биометрические ПДн, которые используются организацией для установления личности субъекта ПДн, могут обрабатываться в организации только при наличии согласия в письменной форме субъекта ПДн *(В случае недееспособности субъекта ПДн письменное согласие на обработку его ПДн получается от его законного*

представителя), за исключением случаев, предусмотренных ч. 2 ст. 11 ФЗ «О персональных данных» [2];

Обработка ПДн в организации может осуществляться как с использованием, так и без использования средств автоматизации;

– Автоматизированная обработка ПДн должна осуществляться в ИСПДн в строгом соответствии с настоящей политикой.

– Неавтоматизированная обработка ПДн должна осуществляться таким образом, чтобы ПДн обособлялись от иной информации (*путем фиксации их на отдельных материальных носителях ПДн, в специальных разделах или на полях форм (бланков) и иным способом*).

Лица, осуществляющие обработку ПДн без использования средств автоматизации, должны быть проинформированы о факте обработки ими ПДн, категориях обрабатываемых ПДн, а также об особенностях и правилах осуществления такой обработки.

При неавтоматизированной обработке ПДн, предполагающей использование типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн *(далее - типовая форма)*, необходимо выполнять следующие условия:

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать:

– *сведения о цели обработки ПДн, осуществляемой без использования средств автоматизации;*

– *фамилию, имя, отчество и адрес субъекта ПДн;*

– *источник получения ПДн, сроки обработки ПДн;*

– *перечень действий с ПДн, которые будут совершаться в процессе их обработки;*

– *общее описание используемых оператором способов обработки ПДн;*

b) *типовая форма должна предусматривать поле, в котором субъект ПДн может поставить отметку о своем согласии на обработку ПДн, осуществляемую без использования средств автоматизации;*

c) *типовая форма должна быть составлена таким образом, чтобы каждый из субъектов ПДн, содержащихся в документе, имел возможность ознакомиться со своими ПДн, содержащимися в документе, не нарушая прав и законных интересов иных субъектов ПДн;*

d) *типовая форма должна исключать объединение полей, предназначенных для внесения ПДн, цели обработки которых заведомо не совместимы.*

При сохранении ПДн на материальных носителях не допускается сохранение на одном материальном носителе ПДн, цели обработки которых заведомо не совместимы. Для обработки различных категорий ПДн, осуществляемой без использования средств автоматизации, для каждой категории ПДн следует использоваться отдельный материальный носитель.

При несовместимости целей обработки ПДн, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку ПДн отдельно от других зафиксированных на том же носителе ПДн и при необходимости уничтожения или блокирования части ПДн уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование ПДн, подлежащих уничтожению или блокированию;

Уточнение персональных данных

Уточнение ПДн, обрабатываемых в организации, осуществляется по запросам субъектов ПДн, их законных представителей или в случае обращения уполномоченного органа по защите прав субъектов ПДн.

Предоставление и передача персональных данных

При предоставлении ПДн третьей стороне должны выполняться следующие условия:

- передача (предоставление доступа) ПДн третьей стороне осуществляется на основании договора, существенным условием которого является обеспечение третьей стороной конфиденциальности ПДн и безопасности персональных данных при их обработке;
- наличие письменного согласия субъекта ПДн на передачу его ПДн третьей стороне, за исключением случаев, предусмотренных законодательством.

В целях информационного обеспечения в организации могут создаваться специализированные справочники (телефонные, адресные книги и др.), содержащие персональные данные, к которым с письменного согласия субъекта ПДн может предоставляться доступ неограниченному кругу лиц;

Сведения о субъекте ПДн должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

Блокирование персональных данных

Основанием блокирования организацией персональных данных, относящихся к соответствующему субъекту ПДн, является обращение или запрос субъекта ПДн (законного представителя или уполномоченного органа) при

условии подтверждения факта недостоверности, устаревания, неполноты персональных данных, отсутствия необходимости в них для заявленной цели обработки, неправомерных действий с ними, незаконного их получения.

Уничтожение персональных данных

Основанием для уничтожения ПДн, обрабатываемых в организации является:

- достижение цели обработки ПДн;
- утрата необходимости в достижении цели обработки ПДн;
- отзыв субъектом ПДн согласия на обработку своих ПДн, за исключением случаев, когда обработка указанных ПДн является обязательной в соответствии с законом РФ или договором;
- выявление неправомерных действий с ПДн и невозможности устранения допущенных нарушений в срок, не превышающий трех рабочих дней с даты такого выявления;
- истечение срока хранения ПДн, установленного законодательством РФ;
- предписание уполномоченного органа по защите прав субъектов ПДн, Прокуратуры России или решение суда.

Уничтожение части ПДн, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих ПДн с сохранением возможности обработки иных данных, зафиксированных на материальном носителе.

Обеспечение безопасности персональных данных при их обработке

При обработке ПДн организация принимает правовые, организационные и технические меры для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения,

изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

Обеспечение безопасности ПДн осуществляется в рамках установления в организации режима безопасности информации конфиденциального характера.

Обеспечение безопасности ПДн, в частности, достигается:

- определением угроз безопасности ПДн при их обработке в ИСПДн;
- применением организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн, необходимых для выполнения требований к защите ПДн, исполнение которых обеспечивает установленные Правительством РФ уровни защищенности ПДн;
- применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- оценкой эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн;
- учетом машинных носителей ПДн;
- обнаружением фактов несанкционированного доступа к ПДн и принятием мер к блокированию каналов несанкционированного доступа;
- восстановлением ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установлением правил доступа к ПДн, обрабатываемым в ИСПДн, а также обеспечением регистрации и учета всех действий, совершаемых с ПДн в ИСПДн;

– контролем за принимаемыми мерами по обеспечению безопасности ПДн и уровнем защищенности ПДн в ИСПДн.

В соответствии с требованиями федерального закона «О лицензировании отдельных видов деятельности» при обеспечении безопасности ПДн в ИСПДн с использованием средств технической и/или криптографической защиты информации организация получает соответствующие лицензии ФСТЭК и/или ФСБ России;

Уровни защищенности ПДн при их обработке в ИСПДн, требования к защите ПДн, требования к материальным носителям биометрических ПДн и технологиям их хранения вне ИСПДн определяются в зависимости от угроз безопасности персональным данным с учетом возможного вреда субъекту ПДн, объема и содержания обрабатываемых ПДн, вида деятельности, при осуществлении которого обрабатываются ПДн, актуальности (уровня) угроз безопасности ПДн;

Использование и хранение биометрических ПДн вне ИСПДн осуществляется только с применением материальных носителей информации и технологии хранения, которые обеспечивают защиту биометрических ПДн от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления и распространения;

Защита ПДн при неавтоматизированной обработке осуществляется в соответствии с требованиями подзаконных нормативно-правовых актов РФ по работе с материальными носителями информации.

Ответственность за нарушение норм, регулирующих обработку персональных данных

Организация и/или работники организации, виновные в нарушении требований законодательства РФ о персональных данных, а также положений настоящей Политики, несут предусмотренную законодательством Российской Федерации ответственность.

Моральный вред, причиненный субъекту ПДн вследствие нарушения его прав, нарушения правил обработки ПДн, а также требований к защите ПДн подлежит возмещению в соответствии с законодательством Российской Федерации.

Контрольные вопросы

1. Дайте определение понятию «Биометрические ПДн», опишите особенности этой категории ПДн.
2. Укажите законные основания, на основе которых Ваша организация обязана обрабатывать персональные данные.
3. Составьте список угроз безопасности ПДн при их обработке в Вашей компании.
4. Продумайте и составьте правила учета машинных носителей ПДн в Вашей организации.
5. Продумайте и составьте правила обеспечения безопасности обработки ПДн сотрудников организации.

Практическое занятие № 3
Политика «Обеспечение безопасности персональных данных в организации»

Цель занятия: рассмотрение основных и наиболее важных моментов при разработке политики «Обеспечение безопасности персональных данных в организации» для выбранной КИС.

Задачи: определить порядок организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (ИСПДн), а также установить требования по защите персональных данных в ИСПДн компании.

Ход работы

Преступим к разработке политики безопасности «Обеспечение безопасности персональных данных (ПДн) в организации» для выбранной КИС. Раскроем необходимые в работе определения терминов и сокращений [2].

Термины и сокращения

Актуальная угроза – угроза, которая может быть реализована в ИСПДн и представляет опасность для ПДн.

Безопасность персональных данных – состояние защищенности ПДн, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность ПДн при их обработке в ИСПДн.

Инцидент информационной безопасности ПДн – имевшее место, предпринимаемое или вероятное нарушение требований обеспечения информационной безопасности ПДн.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к ПДн лицом требование не допускать их

распространения без согласия субъекта ПДн или наличия иного законного основания.

Модель нарушителя – предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности.

Модель угроз безопасности ПДн – систематизированный перечень угроз безопасности ПДн при их обработке в ИСПДн.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности ПДн при их обработке техническими средствами в ИСПДн.

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность ПДн конкретному субъекту ПДн.

Обеспечение безопасности ПДн – исключение несанкционированного, в том числе случайного, доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иные несанкционированные действия.

Обработка персональных данных, осуществляемая без использования средств автоматизации – обработка ПДн (а именно – использование, уточнение, распространение и уничтожение) содержащихся в ИСПДн либо извлеченных из такой системы, осуществляемая при непосредственном участии человека.

Общедоступные персональные данные – ПДн, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта ПДн или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Организация обеспечения безопасности ПДн при их обработке в ИСПДн – формирование и реализация совокупности согласованных по цели, задачам, месту и

времени организационных и технических мероприятий, направленных на минимизацию ущерба от возможной реализации угроз безопасности ПДн.

Распространение персональных данных – действия, направленные на передачу ПДн определенному кругу лиц (передача ПДн) или на ознакомление с ПДн неограниченного круга лиц, в том числе обнародование ПДн в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к ПДн каким-либо иным способом.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иных несанкционированных действий при их обработке в ИСПДн.

Также введем и опишем роли сотрудников организации (ролевая модель).

Для создания ролевой модели проводится комплексное обследование бизнес-процессов компании и задействованных в них ИТ-ресурсов, формируется структура прав доступа пользователей к информационным ресурсам (структура ролей пользователей), выявляются требования к условиям назначения ролей, закладываются механизмы развития ролевой модели при изменении бизнес-требований.

Назначение пользователю той или иной роли, как правило, зависит от его должности и места работы в компании. Поскольку данные параметры сотрудника являются обязательными и регистрируются в системе учета кадров, всегда может быть определен минимальный набор прав доступа сотрудника к информационным системам, что согласно ролевой модели определяется как ролевой профиль пользователя.

Профили пользователей могут иметь различную степень детализации, при этом ролевая модель может распространяться на все информационные ресурсы или только на базовые сервисы (почта, доступ к файловым каталогам, доступ в интернет, основные бизнес-приложения и.т.д.). При этом пользователи или их руководители получают возможность запроса доступа к информационным ресурсам, не входящим в типовой профиль, что позволяет начать внедрение системы до завершения работ по созданию всеобъемлющей ролевой модели в компании.

Определения ролей

Администратор ресурса – работник блока информационных технологий осуществляющий конфигурацию, настройку и управление программными, техническими, программно-аппаратными средствами ИСПДн, в том числе средствами защиты ПДн;

Владелец ИСПДн – должностное лицо, которое устанавливает цель обработки определенной Группы ПДн, ее состав, объем и порядок обработки в подконтрольной ИСПДн с учетом законодательных и корпоративных требований, а также управляет рисками, связанными с обработкой данной Группы ПДн;

Владелец процесса обработки ПДн – должностное лицо, управляющее процессом и несущее ответственность за внедрение, регулярный контроль и анализ хода процесса, реализацию мероприятий по улучшению процесса, соблюдение требований по обработке и защите ПДн, а также результаты реализации процесса в подконтрольном процессе обработки ПДн;

Владелец ресурса обработки персональных данных – работник или подразделение, распоряжающийся информационным ресурсом, в том числе определяющий порядок доступа и его использования;

Распорядитель ИСПДн – должностное лицо, назначаемое владельцем ИСПДн, координирующее

взаимодействия между всеми участниками процесса обработки ПДн в подконтрольной ИСПДн.

Выделим следующие разделы для будущего документа:

1. Общие положения;
2. Организационная структура обеспечения безопасности ПДн;
3. Требования по обеспечению безопасности ПДн;
4. Организация обеспечения безопасности ПДн;
5. Ответственность за нарушение норм, регулирующих обработку персональных данных.

Ниже подробно рассмотрим содержание перечисленных разделов с представленными в примерами.

Общие положения

В соответствии с законодательными и нормативно-правовыми актами Российской Федерации оператор ПДн обязан обеспечить конфиденциальность персональных данных и безопасность персональных данных при их обработке в информационных системах.

Конфиденциальность персональных данных достигается организацией обработки ПДн в соответствии с Политикой «Обработка персональных данных в организации», рассмотренной в практическом занятии № 2.

Безопасность ПДн достигается реализацией организационных и технических мер защиты ПДн в бумажном документообороте и в информационных системах персональных данных (ИСПДн) от несанкционированного, в том числе случайного, доступа к ПДн, результатом которого может стать несанкционированное уничтожение, изменение, блокирование, копирование, распространение ПДн:

- обеспечение безопасности ПДн в бумажном документообороте достигается установлением режима безопасности информации для процессов

обработки ПДн и организацией документооборота в подразделениях организации;

– обеспечение безопасности ПДн при их обработке в ИСПДн достигается установлением режима безопасности информации для процессов обработки ПДн, созданием системы защиты персональных данных (СЗПДн) в ИСПДн и выполнением комплекса сопутствующих организационно-технических мероприятий, с учетом особенностей защиты ПДн установленных требованиями подзаконных нормативно-правовых актов ФСТЭК и ФСБ России по технической и криптографической защите ПДн.

Работы по обеспечению безопасности ПДн в организации реализуются на всех этапах жизненного цикла ИСПДн и делопроизводства с материальными носителями информации.

Политика направлена на решение следующих задач:

– формирование и проведение единой политики в области обеспечения безопасности ПДн;
– координация деятельности структурных подразделений организации при проведении работ по созданию, развитию и эксплуатации ИСПДн с соблюдением требований по обеспечению безопасности ПДн;
– принятие управленческих решений и разработка практических мер по реализации согласованных мер организационно-технического характера, направленных на выявление, отражение и уменьшение вероятности реализации угроз безопасности ПДн.

Организационная структура обеспечения безопасности ПДн

В мероприятиях по защите ПДн участвуют следующие структурные подразделения и категории сотрудников:

– Комитет по информационной безопасности (ИБ);

– Владельцы ИСПДн;

– Распорядители ИСПДн;

– Владельцы процессов обработки ПДн;

– Владельцы ресурсов обработки ПДн;

– Пользователи ИСПДн;

– Администраторы автоматизированных ресурсов обработки ПДн;

– Отдел по работе с персоналом;

– Отдел информационной безопасности и технической защиты информации.

Комитет по ИБ выполняет функции утверждения перечней объектов защиты ПДн *(«Перечня ПДн, обрабатываемых в ОАО», «Перечня процессов обработки ПДн», «Перечня ресурсов автоматизированной обработки ПДн» и т.п.)*, владельцев ИСПДн, процессов и ресурсов обработки ПДн.

Владельцы ИСПДн утверждают требования к уровню защиты ПДн, а также согласуют решения по созданию или модернизации подсистемы защиты ПДн.

Распорядители ИСПДн готовят проекты решений для владельцев ИСПДн по защите ПДн.

Владельцы процессов обработки ПДн согласуют с владельцами ресурсов обработки ПДн и владельцами ИСПДн создание или изменение процессов обработки ПДн в части соблюдения требований по защите ПДн при их обработке в ИСПДн.

Владельцы ресурсов обработки ПДн обеспечивают эксплуатацию подсистем защиты ПДн в подконтрольных ресурсах обработки ПДн.

Пользователи ИСПДн выполняют требования по использованию средств защиты ПДн при обработке ПДн, которые предусмотрены для использования на автоматизированных рабочих местах пользователей.

Администраторы автоматизированных ресурсов обработки ПДн обеспечивают правильное использование средств и подсистем защиты ПДн для защиты ПДн в подконтрольных ИСПДн по указанию владельцев ресурсов обработки ПДн.

Отдел по работе с персоналом отвечает за: организацию обучения работников по вопросам обеспечения безопасности ПДн; организацию переподготовки работников подразделений безопасности и администраторов ресурсов обработки ПДн по вопросам защиты ПДн.

Отдел информационной безопасности и технической защиты информации отвечает за:

– организацию режима безопасности информации, в том числе ПДн, в процессах обработки ПДн;

– актуализацию лицензий ФСТЭК и ФСБ России по технической и криптографической защите информации;

– развертывание и эксплуатацию подсистем и средств защиты ПДн;

– контроль выполнения требований по защите ПДн и мониторинг безопасности;

– аудит безопасности и оценку защищенности ПДн, подготовку заключений о состоянии защиты ПДн.

Требования по обеспечению безопасности ПДн

Методы и способы защиты информации в ИСПДн устанавливаются Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

Мероприятия по защите ПДн при их обработке в ИСПДн от несанкционированного доступа и неправомерных действий определяются в соответствующих технических

проектах, внутренней технической документации на ИСПДн и должны включать в себя:

– управление доступом;

– регистрацию и учет;

– обеспечение целостности;

– антивирусную защиту;

– криптографическую защиту;

– анализ защищенности;

– обнаружение вторжений;

– контроль межсетевого взаимодействия;

– управление безопасностью процессов обработки информации.

Организация обеспечения безопасности ПДн

Работы по обеспечению безопасности ПДн при их обработке в ИСПДн реализуются в рамках единой политики обеспечения информационной безопасности на основе процессного подхода. В интересах данного подхода в организации реализуются следующие процессы по обеспечению безопасности ПДн:

– инвентаризация ресурсов автоматизированной обработки ПДн, используемых в ИСПДн;

– документирование сведений об ИСПДн;

– классификация ИСПДн;

– анализ рисков безопасности ПДн в ИСПДн (разработка модели угроз и модели нарушителя безопасности ПДн);

– оценка возможности оптимизации ИСПДн;

– реализация мероприятий по обеспечению безопасности ПДн:

– допуск персонала к обработке ПДн;

– обучение персонала, участвующего в обеспечении безопасности ПДн;

– обоснование выбора требований по безопасности ПДн в ИСПДн;

– реализация механизмов обеспечения безопасности ПДн в ИСПДн;

– реагирование на инциденты безопасности ПДн;

– оценка (аудит) соответствия процесса обеспечения безопасности ПДн требованиям нормативных документиов (НД);

– совершенствование процесса обеспечения безопасности ПДн.

Инвентаризация и классификация ИСПДн

Классификация ИСПДн проводятся в соответствии с «Порядком проведения классификации информационных систем персональных данных» (утвержденным приказом ФСТЭК России от 13 февраля 2008 года №55, ФСБ России №86 и Министерства информационных технологий и связи №20 и моделью угроз безопасности ПДн в ИСПДн ОАО «»).

Результатом классификации ИСПДн является акт классификации.

Оценка необходимости пересмотра класса ИСПДн должна осуществляться каждый раз, когда изменились характеристики, учитываемые при классификации ИСПДн.

Анализ рисков безопасности ПДн в ИСПДн

Методической базой для разработки Модели угроз и нарушителя безопасности ПДн является [4, 5, 6].

Результатом разработки Модели угроз и нарушителя безопасности ПДн должно являться:

– перечень актуальных угроз;

– вывод о классе специальной ИСПДн;

– вывод о типе нарушителя безопасности ПДн, существующем в ИСПДн и требуемом классе средств криптографической защиты информации.

Модель угроз и нарушителя безопасности ПДн должна содержать:

– описание структуры и состава ИСПДн (состав обрабатываемых ПДн, состав технических средств и

программного обеспечения, существующие процессы обработки ПДн, схему организации связи и т.п.);
- обоснование характеристик безопасности ПДн (конфиденциальность, целостность, доступность и т.п.), нарушение которых ведет к ущербу для субъектов ПДн;
- модель угроз (перечень угроз, оценку вероятностей угроз, показатели опасности угроз для ИСПДн, оценки возможностей реализации угроз, выводы об актуальности угроз);
- модель нарушителя (объекты атак, возможные типы нарушителей, предположения о возможностях нарушителей, предположения об ограничениях на эти возможности, предположения о каналах атак и средствах атак, выводы о типе нарушителя).

Модель угроз и нарушителя безопасности ПДн должна пересматриваться каждый раз, когда изменяются характеристики, влияющие на актуальность угроз, класс ИСПДн, тип нарушителя.

Оценка возможности оптимизации ресурсов и ИСПДн

Данный процесс организуется в целях снижения правоприменительных рисков вероятности реализации инцидентов безопасности с ПДн за счет снижения числа и типов обрабатываемых ПДн, процессов и ресурсов обработки ПДн, внешних и внутренних лиц, допущенных к обработке ПДн. Критериями оптимизации являются снижение рисков предъявления претензий регуляторами, повышение безопасности ПДн и снижение затрат на обеспечение безопасности ПДн.

При проведении оптимизации должна оцениваться возможность:
- исключения обработки ПДн, не имеющих законодательных целей обработки;
- снижения количества и категорий пользователей ИСПДн;

– снижения числа потоков ПДн передаваемых внешним физическим и юридическим лицам;
– снижения категории, объемов и сроков хранения обрабатываемых ПДн;
– обезличивания ПДн;
– придания ПДн статуса общедоступных;
– изменения процесса обработки ПДн в целях повышения безопасности ПДн;
– оптимизации структуры и состава технических и программных средств ИСПДн, технологических процессов обработки ПДн по критерию безопасности ПДн.

Оптимизация в общем случае позволяет снизить класс защиты ИСПДн и уровень требований по безопасности ПДн, а также вероятность нарушения безопасности ПДн.

Результаты оценки оформляются в виде соответствующего отчета, включающего, как минимум:
– варианты оптимизации;
– технический анализ вариантов оптимизации;
– стоимостной анализ вариантов оптимизации;
– выводы об оптимальном варианте оптимизации.

Доступ персонала к обработке ПДн

Доступ к ПДн предоставляется только лицам, указанным в «Перечнях лиц, допущенных к обработке персональных данных» (далее Перечень лиц).

Перечни лиц составляются и ведутся руководителями структурных подразделений, на основании данных о лицах, допущенных к обработке ПДн.

Доступ лиц к конкретным ПДн осуществляется на основании соответствующих заявок.

В организации должен проводиться комплекс мероприятий, направленных на исключение присутствия злоумышленников среди Администраторов ресурсов, а также возможность сговора двух и более злоумышленников.

Комплекс мероприятий может включать, в том числе:

– проверки пользователей ИСПДн при приеме на работу и первоначальном допуске к ПДн, в том числе:

- изучение личного дела сотрудника;
- проверка правильности данных указанных в документах, предоставляемых работником при приеме на работу;

– проверки администраторов ресурсов при назначении на соответствующую должность, в том числе:

- изучение личного дела сотрудника;
- проверка правильности данных указанных в документах, предоставляемых работником при приеме на работу;
- получение (проверка) отзывов о работе данного сотрудника на предыдущих местах работы;
- проверка личных и профессиональных характеристик посредством общения с руководителями с прошлых мест работы (по возможности);
- тестирование квалификации работника, с использованием тестов;
- периодический мониторинг действий пользователей и администраторов ресурсов (для администраторов ресурсов не реже 1 раза в год).

Факт и результаты проведения проверки администраторов ресурса должны документироваться. Наличие отрицательных результатов по каким-либо проведенным проверкам должны являться основанием для отстранения от выполнения функций администратора ресурса.

Обучение персонала, участвующего в обработке ПДн

Должно проводиться обучение всех сотрудников организации, участвующих в процессе обработки ПДн, требованиям обеспечения безопасности ПДн персонала.

Контроль прохождения обучения, отправка работников на обучение осуществляется руководителями структурных подразделений участвующих в процессах обработки и защиты ПДн.

Обоснование выбора требований по безопасности ИСПДн

Выбор и реализация методов и способов защиты информации в ИСПДн осуществляются на основе определяемых угроз безопасности ПДн (модели угроз) и в зависимости от класса ИСПДн.

Реализация механизмов обеспечения безопасности ПДн в ИСПДн

Основным механизмом обеспечения безопасности ПДн в ИСПДн является защита ПДн от несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных.

Мероприятия по защите от несанкционированного физического доступа к компонентам ИСПДн включают:

– мероприятия по защите от несанкционированного физического доступа на территорию, на которой находятся компоненты ИСПДн;

– мероприятия по защите от несанкционированного физического доступа в помещения с компонентами ИСПДн;

– мероприятия по защите от несанкционированного физического доступа в спецпомещения;

– мероприятия по защите от несанкционированного физического доступа к кабельным коммуникациям, участвующим в процессах обработки ПДн;

– мероприятия по защите от несанкционированного физического доступа к компонентам ИСПДн;

– мероприятия по защите от несанкционированного физического доступа к носителям ПДн;

– мероприятия по контролю перемещений физических компонентов ИСПДн.

Реагирование на инциденты информационной безопасности ПДн

Для эффективного реагирования на инциденты, возникающие при обработке ПДн в организации, должны быть регламентированы следующие вопросы:

– порядок определения нештатной ситуации;
– порядок оповещения работников при возникновении различных нештатных ситуаций;
– порядок действий по нейтрализации нештатных ситуаций, сведения их негативных последствий к минимуму.

В организации должны проводиться расследования инцидентов связанных с несанкционированным доступом и другими несанкционированными действиями.

В рамках данного процесса должны решаться следующие задачи:

– расследование инцидентов, связанных с безопасностью ПДн;
– ликвидация последствий инцидентов, связанных с безопасностью ПДн;
– принятие мер по недопущению возникновения подобных инцидентов в дальнейшем.

Оценка (аудит) соответствия процесса обеспечения безопасности ПДн требованиям нормативных документов

Для обеспечения эффективности процесса защиты ПДн проводится:

– контроль за соблюдением требований по обработке и обеспечению безопасности персональных данных;
– контроль за соблюдением условий использования средств защиты ПДн, предусмотренных эксплуатационной и технической документацией;
– контроль эффективности средств защиты ПДн.

Для контроля эффективности СЗПДн должны использоваться средства анализа защищенности.

При проведении контроля эффективности в общем случае должно проверяться:

– наличие установленных средств защиты информации;
– корректность настроек средств защиты информации;
– выполнение пользователями ИСПДн и администраторами ресурсов требований корпоративных нормативных документов по защите ПДн;
– соответствие системы защиты ПДн требованиям, предъявляемым к ней.

Выявленные несоответствия процессов защиты ПДн обязательны к устранению.

Совершенствование процесса обеспечения безопасности ПДн

Исходными данными указанного процесса является следующая информация:

– об изменениях ИСПДн;
– об изменениях процессов обработки ПДн;
–об инцидентах ИБ, связанных с обработкой ПДн;
– результаты проведения аудитов информационной безопасности;
– изменения законодательных и нормативно-правовых актов РФ.

Каждое определенное выше изменение должно анализироваться на предмет их влияния на процесс обеспечения безопасности ПДн. При необходимости должна производиться модернизация СЗПДн и предприниматься другие необходимые организационно-технические меры.

Контрольные вопросы

1. Опишите особенности следующих структурных подразделений и категорий сотрудников: Комитет по ИБ; Владельцы ИСПДн; Распорядители ИСПДн; Владельцы процессов обработки ПДн; Владельцы ресурсов обработки ПДн; Пользователи ИСПДн; Администраторы автоматизированных ресурсов обработки ПДн.
2. Продумайте и опишите правила расследования инцидентов, связанных с несанкционированным доступом и другими несанкционированными действиями, возникшими в ходе процесса обеспечения безопасности ПДн.
3. Как Вы понимаете понятие «аудит информационной безопасности»? В чем заключается его необходимость?
4. Как Вы считаете, на сколько значимые результаты несет периодический мониторинг действий пользователей и администраторов ресурсов? Как организовать подобную проверку, чтобы она носила результативный, а не формальный характер?

ПРИЛОЖЕНИЕ 1

Форма для заполнения к практическому занятию № 1

ФИО студента, группа_____

Политика «Требования по обеспечению информационной безопасности» в _____

_____

1. Общие положения
   - 1.1._____
   - 1.2._____
   - 1... _____
2. Рабочее место пользователя
   - 2.1._____
   - 2.2._____
   - 2…_____
3. Парольная политика
   - 3.1._____
   - 3.2._____
   - 3... _____
4. Работа с электронной почтой
   - 4.1._____
   - 4.2._____
   - 4... _____
5. Работа в сети Интернет
   - 5.1._____
   - 5.2._____
   - 5... _____
6. Действия в нестандартных ситуациях
   - 6.1._____
   - 6.2._____
   - 6... _____
7. Ответственность
   - 7.1._____
   - 7.2._____
   - 7... _____

ПРИЛОЖЕНИЕ 2

Форма для заполнения к практическому занятию № 2

ФИО студента, группа_____

Рассматриваемая организация_____

_____

Укажите законные основания, на основе которых Ваша организация обязана обрабатывать персональные данные

_____

_____

_____

_____

_____

_____

Составьте список угроз безопасности ПДн при их обработке в Вашей компании

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

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

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

3. Приказ Минкультуры РФ от 25.08.2010 № 558 «Об утверждении «Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения»

4. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена заместителем директора ФСТЭК России 15 февраля 2008 года. [Электронный ресурс]. – Режим доступа: http://fstec.ru/component/attachments /download/289.

5. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена заместителем директора ФСТЭК России 14 февраля 2008 года.

6. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации, утвержденные руководством 8 Центра ФСБ России 21 февраля 2008 г., № 149/54-144.

7. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21. [Электронный ресурс]. – Режим доступа: http://fstec.ru/component/attachments/download/561

8. ГОСТ ИСО/МЭК 27004: 2009 – Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения. – М.: Стандартинформ, 2011. – 90 с.

9. Федеральный закон «О коммерческой тайне» от 29.07.2004 г. № 98-ФЗ

10. Требования к защите персональных данных при их обработке в информационных системах персональных данных. Постановление Правительства Россий Федерации от 1 ноября 2012 г. № 1119. [Электронный ресурс]. – Режим доступа: http://www.rg.ru/ 2012/11/07/pers-dannye-dok.html

СОДЕРЖАНИЕ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к практическим занятиям по дисциплине
«Основы информационной безопасности»
для студентов специальностей
090303 «Компьютерная безопасность»,
090303 «Информационная безопасность
телекоммуникационных систем»,
090303 «Информационная безопасность
автоматизированных систем»
очной формы обучения

Составители:
Чопоров Олег Николаевич
Корнеева Наталья Николаевна

В авторской редакции

Подписано к изданию 06.04.2015.
Уч.-изд. л. 3,0.

ФГБОУ ВПО «Воронежский государственный
технический университет»
394026 Воронеж, Московский просп., 14