Методические рекомендации по организационной защите физическим лицом своих персональных данных*

Данный документ разработан для снижения рисков безопасности в условиях "транзитного мира" и эффективного перехода к цифровой эпохе.

Документ предназначен для специалистов в области безопасности информационных технологий и персональных данных, а также для заинтересованных лиц. На основе документа предполагается разработка обучающих программ и документов для различных аудиторий.

1. Термины и определения

Аппаратно-программный комплекс – сочетание аппаратных и программных средств, а также внесенных изменений в конфигурации, способствующих достижению максимально возможного уровня защиты персональных данных от утечек

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

Большие данные (BigData) – обозначение подходов, инструментов и методов распределенной обработки полуструктурированных и неструктурированных данных самого разного типа и огромных объемов. В отличие от традиционных баз данных, большие данные не относятся к структурированным, хранятся децентрализовано и слабо связаны между собой

* Настоящие Методические рекомендации по организационной защите физическим лицом своих персональных данных разработаны Консультативным советом при уполномоченном органе по защите прав субъектов персональных данных

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных

Всемирная паутина – распределенная система доступа к связанным документам, расположенным на различных компьютерах, подключенных к Интернету

Доступ в операционную среду компьютера (информационной системы персональных данных) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ

Доступ к информации – возможность получения информации и ее использования

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации

Интернет – глобальная система, объединяющая компьютерные сети и используемая для передачи и хранения данных

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

Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации

Контролируемая зона – физическое пространство, в котором помимо субъекта персональных данных исключено пребывание посторонних лиц и посторонних транспортных, технических и иных материальных средств

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания

Метаданные – персональные данные, создаваемые электронными устройствами при их использовании человеком, с его ведома или без такового

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин

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

Обработка персональных данных – действия (автоматизированные и неавтоматизированные) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных

Онлайн-присутствие – персональные данные человека, доступные в цифровой среде

Онлайн-сервис – идентифицируемая веб-адресом программная система со стандартизированными интерфейсами и предоставляющая пользователю определенные услуги, например, доступ к базе данных

Офлайн-присутствие – персональные данные человека, доступные в реальном мире

Оператор (персональных данных) – государственный, региональный или муниципальный орган власти, юридическое или физическое лицо, организующее и/или осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация

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

Профиль – совокупность персональных данных пользователя, предоставляемых им в цифровой и реальной среде, при определенном типе взаимодействия

Разрешение на использование персональных данных – разрешение субъекта персональных данных, которое он дает заинтересованной стороне на получение, сбор, хранение и использование персональных данных о себе

Раскрытие персональных данных – умышленное или случайное нарушение конфиденциальности персональных данных

Распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том

числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы

Содержательные данные – персональные данные, создаваемые человеком, в том числе текстовые сообщения, фотографии, видео- и аудиозаписи, передаваемые через Интернет файлы

Социальная инженерия – совокупность приемов, методов и технологий создания пространства, условий и обстоятельств, которые максимально эффективно приводят к конкретному необходимому результату, с использованием социологии и психологии. В контексте данного документа – приводящие к результату утечки персональных данных и/или ущербу пользователя или третьей стороны – жертвы социальной инженерии

Социальная сеть – платформа или веб-сервис, направленный на выстраивание, отражение и организацию социальных взаимоотношений между пользователями (включая незарегистрированных в сети)

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и технических средств, которыми добывается защищаемая информация

Транзитный мир – промежуточное состояние экономики, сложившееся на сегодняшний день и характеризующееся процессами перехода от классических моделей и технологий организации жизнедеятельности к цифровым

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

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации

Целостность информации – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право

Цифровая тень – цифровое присутствие, осуществляющееся без участия самого субъекта за счет деятельности и устройств третьих лиц

Цифровая экономика – хозяйственная деятельность, ключевым фактором производства в которой являются данные в цифровой форме, и которая способствует формированию информационного пространства, а также формированию новой технологической основы для социальной и экономической сферы

Цифровое присутствие – постоянное участие в обмене информацией и взаимодействие вне зависимости от местоположения, необходимое для обеспечения производственной деятельности и эффективного общения

Цифровой след – результат цифрового присутствия, осуществленного самим субъектом за счет деятельности и с помощью своих устройств

Цифровой штамп – совокупность цифровых теней и цифровых следов пользователя, доступных в цифровой среде

2. Общие положения

2.1. Актуальность темы

В настоящее время цифровое присутствие, определяемое как постоянное участие в обмене информацией и взаимодействие вне зависимости от местоположения субъекта, получает все большее распространение, становится необходимым фактором обеспечения производственной деятельности и эффективного общения. Для его организации используются электронные приборы, а также значительное число объектов физического мира (лицо человека, номера автомобилей и т.д.). При этом цифровое присутствие может быть как контролируемым, так и вынужденным, то есть осуществляющимся без участия самого субъекта посредством деятельности и устройств третьих лиц.

Для организации эффективного цифрового присутствия человека необходимо определение требующегося ему уровня взаимодействия, каналов и средств его реализации, объема передаваемой информации, а также выбор и внедрение средств защиты. При этом персональные данные – это ключевой фактор цифрового присутствия, т.к. они необходимы как для его организации, так и составляют в значительном количестве случаев его содержание. Таким образом, эффективность и безопасность цифрового присутствия во многом зависят от культуры производства и распространения персональных данных.

В настоящее время подавляющее большинство граждан всех возрастов не имеют информации о том, какие персональные данные они производят, кому, с какой целью и в каком объеме их передают. Такое поведение не только неэффективно с точки зрения использования ресурсов цифровой экономики, но и опасно.

Бесконтрольное распространение персональных данных является существенной угрозой для частной жизни лица. Одновременно, активное обращение данных, подавляющее большинство из которых относимы к категории персональных, является базовым условием динамичного развития технологии больших данных. По сути, большие данные эксплуатируют беспечность людей по отношению к информации о себе, при этом находясь в сером правовом поле,

прежде всего, не соблюдая цели обработки, для которых персональные данные были получены. На лицо фундаментальное противоречие принципов больших данных с концепцией охраны частной жизни.

2.2. Концептуальные подходы

Законодательством о защите прав субъектов персональных данных предусмотрены три группы методов защиты, применяемых в информационных системах персональных данных: правовые, технические, организационные. Проанализировав по аналогии возможность использования тех же методов для защиты физическими лицами своих персональных данных, очевидно, что правовой и технический методы являются не столь применимыми в индивидуальных целях: первый по причине объективного отставания нормативно-правовых актов от реалий развития цифрового мира, второй вследствие, как правило, недостаточного уровня технической грамотности лица и недоступности достоверной информации о конкретных схемах функционирования используемых им оборудования и программ. При этом организационный метод защиты собственных персональных данных является реальным к применению физическим лицом в силу возможности осознания и контроля всех своих действий на любых этапах организации цифрового присутствия, а также по причине имеющейся возможности нивелирования значительного количества потенциальных информационных угроз со стороны оборудования и программ, а также третьих лиц.

Методические рекомендации по организационной защите физическим лицом своих персональных данных являются информационно-инструктивным документом базового уровня, предоставляющим любому совершеннолетнему лицу практическую информацию по организации своей деятельности в указанной сфере. Документ включает в себя базовые модели информационных угроз и нарушителя, описание путей противодействия актуальным информационным угрозам, принципов, методов и инструментов организации цифрового присутствия (контролируемые зоны, профили, настройка аппаратно-программного комплекса, правила онлайн и офлайн присутствия и т.п.). Использование Методических рекомендаций позволяет определить индивидуальные цели и задачи цифрового

присутствия субъекта, принять решение об объеме производства персональных данных и их распространении, выбрать способы оплаты потребляемых услуг, выработать меры защиты и правила построения информационного взаимодействия, а также сформировать необходимый аппаратно-программный комплекс, выработать и реализовать организационную стратегию в сфере персональных данных, внедрить меры и правила онлайн и офлайн присутствия.

В развитие Методических рекомендаций по организационной защите физическим лицом своих персональных данных планируется разработка учебных программ для студентов и преподавателей ВУЗов, школьников, дошкольников, учителей, родителей и широкого круга заинтересованных лиц. Методические рекомендации могут быть использованы как самостоятельный организационно-технический комплекс, а также лечь в основу создания аппаратно-программного продукта на базе принципов и механизмов регламента цифрового присутствия. Предложенные подходы могут быть использованы для совершенствования механизмов регулирования цифровой экономики, в первую очередь, сферы персональных данных.

3. Базовая модель угроз безопасности персональных данных физического лица

Приведенная ниже Модель угроз содержит краткий перечень угроз безопасности персональных данных физического лица. Эти угрозы обусловлены преднамеренными или непреднамеренными действиями физических лиц, зарубежных спецслужб или организаций (в том числе террористических), а также криминальных группировок, создающих условия (предпосылки) для нарушения безопасности персональных данных, которое ведет к ущербу жизненно важных интересов личности, общества и государства.

3.1. Актуальные информационные угрозы физического лица

В отношении физических лиц наиболее вероятна угроза неправомерного доступа к их персональным данным для завладения личной информацией и дальнейшего использования в корыстных и прочих противоправных целях. При возникновении угрозы со стороны постороннего физического лица или группы лиц целью, как правило, ставится нанесение финансового ущерба субъекту персональных данных. Заинтересованные лица могут манипулировать персональными данными с целью оказания давления на субъекта и принятие им выгодного нарушителю решения. Иностранные спецслужбы и организации могут ставить целью дестабилизацию экономической, социальной и политической жизни региона или целого государства.

Угрозы данным, обрабатываемым в информационных системах, связаны:

- с перехватом персональных данных по техническим каналам (с целью их копирования и/или неправомерного распространения и использования;
- с несанкционированным, в том числе случайным, доступом в информационную систему (с целью изменения, копирования, неправомерного распространения или уничтожения данных).

Стоит отметить, что перехват данных по техническим каналам менее актуален для деятельности конкретного пользователя, поэтому в принятии личных мер безопасности стоит акцентироваться на преодолении угроз несанкционированного доступа.

3.2. Целевая информация и среда ее сбора

Цифровое присутствие неизбежно сосуществует с такими явлениями, как «цифровой след» и «цифровая тень». Цифровая тень – это информация, создаваемая о людях автоматически посредством деятельности и устройств третьих лиц, а цифровой след – данные, самостоятельно передаваемые субъектом в цифровую среду, такие, как электронные письма, регистрационные данные на сайтах социальных сетей, фотографии, геопозиции и т.п.

В отношении информации, размещаемой и размещенной в виртуальном пространстве, можно выделить два критерия классификации. Первый – по

характеристике персональных данных: цифровой след или тень, то есть своими активными действиями размещаемой информации, либо действиями третьих лиц и устройств. Второй – по признаку среды: распространяемой по физическим каналам, по каналам телефонной связи или через Интернет.

Кроме того, персональные данные разделяются на содержательные данные и метаданные – «данные о данных». К содержательным данным, создаваемым человеком или устройствами, относятся текстовые, видео- и фото- сообщения, разговоры, передаваемые через Интернет файлы. Метаданные создаются только электронными приборами: cookie-файлы в браузере, журналы входящих/исходящих звонков, геопозиционные метки в фотографиях при съемке, видео-, аудио- мониторинг и т.п.

Интернет заполнен множеством цифровых следов и теней, все из которых могут использоваться для анализа поведения пользователя и с помощью которых это поведение может корректироваться и направляться в нужное русло.

3.3. Определение актуальных угроз безопасности персональных данных

Угрозы с применением программных и программно-аппаратных средств реализуются при осуществлении несанкционированного, в том числе случайного, доступа, в результате которого осуществляется нарушение конфиденциальности (копирование, несанкционированное распространение), целостности (уничтожение, изменение) и доступности (блокирование) персональных данных, и включают в себя:

- угрозы утечки персональных данных с сервера оператора персональных данных. Один из самых актуальных типов угроз в цифровой среде обусловлен недостаточными законодательными мерами в отношении операторов персональных данных, способствующими не соблюдением необходимых мер по защите персональных данных. Угроза возникает при передаче персональных данных оператору, не заинтересованному в тщательной проработке мер защиты доступа к хранимым на его серверах персональным

данным и допускающему (непреднамеренно или преднамеренно) утечки персональных данных;

- угрозы доступа (проникновения) в операционную среду устройства с использованием штатного программного обеспечения (средств операционной системы или прикладных программ общего применения) подразделяются на:
    1. Угрозы непосредственного доступа. Злоумышленник может получить доступ к устройству или ресурсу, содержащему персональные данные, оставленному без присмотра с недостаточной степенью защиты доступа;
    2. Угрозы удаленного доступа. Злоумышленник может получить доступ к устройству или ресурсу с используемыми дефолтными (по умолчанию) данными для авторизации; либо осуществить то же самое посредством взлома нестойких систем защиты;
- угрозы создания нештатных режимов работы программных (программно-аппаратных) средств за счет преднамеренных изменений служебных данных, игнорирования, предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, искажения (модификации) самих данных и т.п. Такие угрозы могут возникнуть в случае использования нелицензионного или скомпрометированного аппаратного или программного обеспечения;
- угрозы внедрения вредоносных программ (программно-математического воздействия). Такие угрозы наиболее распространены и могут возникать при посещении сомнительных ресурсов (к примеру, не имеющих подтвержденного сертификата или использующих для доступа незащищенные протоколы связи), установки нелицензионного или скомпрометированного программного обеспечения;
- угрозы методами социальной инженерии. Данный вид угроз реализовывается злоумышленником целенаправленно в отношении

пользователя и/или третьих лиц. Вероятность возникновения угрозы данного типа возрастает при публикации персональных данных в открытых источниках в цифровой среде, а также при несоблюдении достаточных мер по защите своих персональных данных.

4. Базовая модель нарушителя

В качестве нарушителя рассматривается любое лицо или группа лиц, которое осуществляет, может осуществить или осуществило обработку персональных данных при отсутствии соответствующего разрешения или с нарушением условий такового. Нарушителем может являться как физическое лицо или группа лиц, так и организация, а также спецслужбы и органы власти (в том числе и зарубежные).

4.1. Общие положения

При организации защиты информации, в том числе при защите персональных данных организационными мерами, помимо модели угроз, необходимо учитывать модель нарушителя. Цель в разработке такой модели заключается в анализе возможностей, которым потенциально может обладать злоумышленник при организации попыток доступа к защищаемым персональным данным.

4.2. Классификация нарушителей

Среди потенциальных нарушителей можно выделить два типа:

- нарушителей с физическим доступом, реализующих угрозы безопасности персональных данных при непосредственном доступе к устройствам и системам, хранящим персональные данные;
- нарушителей с удаленным доступом, реализующих угрозы безопасности персональных данных через Интернет и прочими дистанционными способами.

Для получения доступа к персональным данным нарушитель с удаленным доступом может осуществлять перехват открытой и зашифрованной информации,

передаваемой по каналам связи сетям общего пользования и (или) сетям международного информационного обмена, а также по локальным сетям.

Любому нарушителю с физическим доступом необходим непосредственный контакт с устройством субъекта или оператора персональных данных.

Описанная модель нарушителя является базовой и может быть использована для разработки частной модели нарушителя.

5. Пути противодействия реализации актуальных информационных угроз

Базовая модель информационных угроз физического лица и Базовая модель нарушителя позволяют определить ключевые подходы к путям противодействия реализации актуальных информационных угроз. Предлагаемый вектор предполагает возможность осознанных действий лица с любым уровнем технических знаний, необходимость принятия решений в условиях неопределенности и контролируемость планируемых результатов.

С учетом указанных принципов основной акцент должен быть сделан на контроле физическим лицом производства персональных данных, в т.ч. и относящихся к третьим лицам. На следующем этапе должен быть определен алгоритм хранения, распространения и уничтожения указанных сведений. Во внимание должны быть приняты как содержательные, так и метаданные.

Перенося указанные выше вопросы, являющиеся одновременно и ограничениями, в плоскость реализации практических действий, целесообразно определить в качестве необходимого и минимально достаточного комплекс из 3 видов планомерной и взаимоувязанной деятельности:

- минимизация объема цифрового штампа физического лица;
- формирование стандартизированных цифровых следов;
- активное влияние на содержание цифровых теней.

Указывая, что цифровой штамп состоит из цифровых следов и цифровых теней, правомерно заметить, что в данном случае итоговая сумма больше

результата, получаемого при простом сложении частей из-за значительно более широких возможностей дальнейшего анализа сведенных воедино данных.

5.1. Минимизация объема цифрового штампа физического лица

Минимизация объема цифрового штампа физического лица, прежде всего, подразумевает принятия осознанного и информированного решения о том, какие данные, для каких целей и в каком объеме физическое лицо намерено производить. В данном контексте предполагается трактовать понятие персональных данных максимально широко и причислять к ним любую информацию, относящуюся к определенному или определяемому лицу – от транзакционных данных до перечня блюд в формуляре заказа завтрака в гостинице. Особенно важно учитывать, что при принятии решения об использовании какого либо цифрового прибора, сервиса или программы, в первую очередь, должно приниматься решение о готовности к производству персональных данных, а уже после этого – о полезности и удобствах, получаемых при использовании. Важно отметить, что в случае с абсолютным большинством видов оборудования и программных продуктов речь идет о производстве неконтролируемого физическим лицом и недекларированного объема персональных данных. На следующем этапе необходимо осуществление планомерной деятельности по распространению персональных данных в интересах достижения конкретных целей лица, что может быть как самостоятельным процессом (например, размещение фотографий в социальных сетях или резюме на сайте по подбору персонала), так и вспомогательным по отношению к главному (предоставление персональных данных для приобретения билетов, регистрация для получения доступа к публичной Wi-Fi сети и пр.). При этом стоит постоянно иметь в виду, что произведенные персональные данные в подавляющем большинстве случаев могут распространяться и вне зависимости от желания физического лица, например, перепостом в соцсетях или веб-сервисом по собственному решению.

Отдельное внимание необходимо уделить производству ваших персональных данных третьими лицами – смартфонами друзей, камерами городского видеонаблюдения, операторами баз данных и пр. Общим правилом может служить допущение, что в непрерывном режиме ведется сбор данных физического лица, во

многих случаях данный процесс является случайным, неосмысленным и не контролируемым. Полученные персональные данные широко вводятся в оборот, и контролировать их распространение физическим лицом практически невозможно. В связи с этим максимальное внимание целесообразно уделить именно процессу их производства и оказать на него все возможное влияние.

5.2. Формирование стандартизированных цифровых следов

Стандартизированные цифровые следы могут быть применены для осуществления и отражения в информационной среде регулярных процессов, необходимых человеку. Отработав механизм формирования следов необходимого содержания, физическое лицо получает дополнительные возможности в использовании сервисов и приборов (например, приобретение товаров по более низким ценам), создает желательное общественное мнение о себе, одновременно защищая частную жизнь.

5.3. Активное влияние на содержание цифровых теней

Активное влияние на содержание цифровых теней достижимо, в первую очередь, использованием системы самоограничений на деятельность в офлайн- и онлайн-режимах. Проработка необходимого формата теней, позволит смоделировать требуемое поведение и стандарты активности, позволяющие насколько возможно приблизиться к заданным параметрам отражения физического лица в цифровых тенях. Важное значение имеет настройка аппаратно-программного комплекса, используемого физическим лицом, с точки зрения предоставления минимально достаточной и выверенной информации, в т.ч. и метаданных, при взаимодействии с третьими лицами и информационными системами.

6. Цифровое присутствие

Цифровое присутствие на настоящем этапе развития технологий неоспоримо важно для эффективной деятельности каждого человека, а также эффективного общения с другими людьми вне зависимости от их места нахождения. Благодаря цифровому присутствию человек выстраивает свои социальные связи и повышает комфорт условий жизнедеятельности вслед за развитием прогресса. Для формирования полноценного цифрового присутствия необходимо предоставление человеком своих персональных данных. При этом следует учесть, что данная процедура может быть как контролируемой со стороны субъекта персональных данных, так и вынужденной, осуществляющейся без участия самого субъекта посредством деятельности и устройств третьих лиц. Результаты в этих двух случаях приводят к созданию в цифровой среде цифрового следа (контролируемого) и цифровой тени (вынужденной), которые вместе формируют цифровой штамп человека и определяют его цифровое присутствие.

Для реализации наиболее эффективной модели цифрового присутствия и обеспечения безопасности субъекта как в цифровой среде, так и реальном мире, необходимо тщательно контролировать создание цифровых следов и максимальным способом уменьшать количество оставляемых цифровых теней, которые могут привести к негативному результату.

6.1. Цели

Среди целей формирования цифрового присутствия можно выделить следующие пункты:

- формирование цифровыми средствами необходимого образа личности (необходимого профиля);
- ускорение процессов общения за счет цифровых средств коммуникации;
- применение цифровых методов управления;
- применение цифровых методов обеспечения жизнедеятельности.

6.2. Задачи

В процессе формирования цифрового присутствия возникают следующие задачи, решение которых необходимо:

- активное противодействие реализации актуальных информационных угроз;
- формирование необходимого цифрового штампа преимущественно за счет цифровых теней;
- поддержание передового аппаратно-программного комплекса;
- создание эффективной экосреды сервисов, программ и приложений;
- нивелирование возможных негативных последствий от негосударственных систем больших данных.

6.3. Принципы

Для обеспечения безопасности субъекта как в цифровой среде, так и реальном мире, необходимо придерживаться следующих принципов:

- контроль офлайн- и онлайн-присутствия;
- планомерная работа в сфере связей с общественностью;
- использование кастомизированного аппаратного комплекса;
- использование кастомизированного программного комплекса;
- использование кастомизированной экосреды сервисов и приложений;
- использование средств защиты приборов и информации.

7. Регламент (методы) цифрового присутствия

Данный регламент описывает основные принципы формирования эффективной модели цифрового присутствия с учетом необходимости тщательной защиты персональных данных человека.

7.1. Контролируемые зоны

Для реализации эффективной модели цифрового присутствия необходимо использование принципа контролируемых зон, заключающегося в разграничении

доступа к персональным данным в зависимости от текущей использующейся контролируемой зоны. Применение данного принципа важно для формирования культуры взаимодействия со своей цифровой личностью и обеспечения безопасности цифрового присутствия. Несмотря на название, данный принцип предусматривает некую гибкость, смещение рамок контролируемых зон в сторону ужесточения или смягчения накладываемых ограничений на основе решения субъекта.

Контролируемые зоны определяют доступность персональных данных субъекта в реальном мире. К примеру, в рабочей обстановке пользователь может использовать рабочий, общедоступный телефон для связи с общественностью, а на территории своего домохозяйства – личный телефон для связи с узким кругом близких и друзей.

Контролируемая зона определяется территорией субъекта персональных данных, на которой исключено пребывание лиц или объектов, не имеющих допуска. В таблице ниже продемонстрирован принцип формирования контролируемых зон.

Таблица 1. Концепция контролируемых зон

	Концепция контролируемых зон		
	Нулевая	Первая	Вторая
Присутствие недопущенных лиц	ДА	НЕТ	НЕТ
Наличие недоверенных подключенных/ неподключенных к Интернету приборов	ДА	ДА	НЕТ
Защита периметра	НЕТ	НЕТ	ДА

Как видно из таблицы, в условиях второй, самой защищенной контролируемой зоны, субъект персональных данных может ограничить присутствие посторонних лиц, отключить устройства от Интернета и при необходимости защитить параметр от утечек персональных данных с помощью сторонних аппаратных средств (например, от съема акустических колебаний стекол). Таким образом, субъект сможет находиться в безопасности, не опасаясь утечек персональных данных и нежелательных последствий, которые могут возникнуть впоследствии. Во второй контролируемой зоне под защитой специальных средств могут храниться финансовые сведения, сведения о здоровье, информация о частной жизни субъекта и т.п.

Для формирования цифрового присутствия субъект персональных данных может применить на практике контролируемую зону нулевого или первого уровня, в зависимости, требуется ли присутствие лиц, с которыми необходимо осуществлять социальное взаимодействие.

Контролируемая зона предусматривает один или несколько периметров. Каждый из периметров отдельно может быть как охраняемым, так и не охраняемым, в зависимости от уровня существующей угрозы и модели правонарушителя. Физически могут существовать как периметр допуска на территорию организации, требующий одного уровня разрешения, а также внутренний периметр допуска в отдельные помещения, требующий дополнительное разрешение. В каждой контролируемой зоне применяются различные технические средства и способы защиты и контроля.

7.2. Профили

Информация, которую субъект персональных данных передает в цифровую среду, остается привязанной к источнику и идентифицирует его. Каждый "шаг" цифрового присутствия фиксируется, анализируется и позволяет определить субъекта, узнать новые сведения.

Каждый год появляются новые накопители и источники данных: датчики и носимые устройства, умная бытовая техника и др. Появляются новые сервисы и приложения, запрашивающие и собирающие данные о пользователях.

Но у размещения информации в Интернете две стороны. Так, публичное размещение геолокации в сообщении привлекает потенциальных злоумышленников: информирует об отсутствии пользователя в жилище, например. Но также позволяет быстро и удобно оформить заказ на сайте доставки.

Поэтому пользователю необходимо определять, кому и какие сведения о нем открыты, а для кого - закрыты. Описанная концепция профилей позволяет этого достичь.

Принцип профилей субъекта персональных данных в цифровой среде напоминает концепцию контрольных зон, как показано в таблице ниже.

Таблица 2. Концепция профилей с предоставлением данных по выбору пользователя

	ОСНОВНОЙ	**ПУБЛИЧНЫЙ**	**РАБОЧИЙ**	**ГОСУСЛУГИ**	**БАНКОВСКИЙ**	**ЛИЧНЫЙ**	**СЕРВИСНЫЙ**
ФИО (или псевдоним)							
Портрет							
Отпечатки пальцев							
Место работы							
Должность							
Звания, степени							
Домашний адрес							
Рабочий адрес							
Домашний телефон							
Рабочий телефон							
Мобильный телефон							
Специальный телефон							
Основной адрес электронной почты							
Дополнительный адрес электронной почты							
Рабочий адрес электронной почты							
Временный адрес электронной почты							

Мессенджер							
Сайт							
Авто							
Документ							
Банковская карта							

Пользователь формирует вокруг своей цифровой личности уникальные контролируемые зоны, которые отличаются набором доступных исходящих персональных данных и набором допущенных входящих сервисов, приложений и других лиц. В зависимости от используемого приложения/сервиса или устройства пользователь предоставляет только те данные, которые необходимы для эффективного взаимодействия с ним в цифровой среде (с учетом, что обеспечивается должная степень защиты персональных данных). В таблице выше приведен краткий вариант концепции, которая на самом деле гибка и имеет множество вариаций (контролируемых зон), зависящих от субъективных потребностей пользователя.

Приведенные поля являются именно примерами и могут регулироваться по потребностям пользователей.

Так, публичный профиль может подразумевать использование некоего обнародованного псевдонима, общедоступного аккаунта в социальной сети и номера телефона, по которому может дозвониться любой желающий. Личный профиль наоборот, предполагает применение личного телефонного номера, реального имени и личной закрытой страницы в социальной сети.

Представленная в таблице концепция профилей носит исключительно демонстрационный характер; количество профилей и данные, которые предоставляются в рамках каждого из них, регулируются самим субъектом персональных данных. При этом следует учитывать, что чем меньше персональных данных предоставляется, тем меньше вероятность их утечки и реализации угрозы безопасности в адрес субъекта.

7.3. Разрешения на обработку персональных данных

На данный момент времени должные меры по контролю за сбором, обработкой и хранением персональных данных обеспечиваются не в полной мере. В виду этого, для обеспечения максимальной степени защиты от потенциального воздействия угроз безопасности персональных данных, следует свести подтверждение разрешений к минимуму. В случае, если разрешение на обработку персональных данных для формирования эффективной модели цифрового присутствия необходимо, следует внимательно ознакомиться с текстом документа и предоставить минимальный набор персональных данных (если такое возможно), либо воспользоваться программой/услугой, не предусматривающей доступ к персональным данным пользователя (либо сводящей его к минимуму).

При наступлении момента прекращения использования программы/услуги, для которой разрешение на обработку персональных данных предоставлено, необходимо вручную отозвать разрешение и обязать соответствующего оператора персональных данных (со стороны разработчика программного обеспечения или владельца предоставляемой услуги) удалить персональные данные с целью предупреждения угрозы их несанкционированного использования.

7.4. Настройка аппаратно-программного комплекса

Так как в настоящее время культура цифрового присутствия только формируется и его участники не задумываются о рисках присутствия в цифровых средах, необходимо всеобъемлющее оповещение и обучение нормам безопасности. Данные нормы касаются не только контроля предоставляемых данных, но и максимально возможных мер по защите от угроз безопасности, способных повлечь несанкционированное раскрытие, уничтожение, изменение, блокирование, копирование, распространение персональных данных. Помимо профилирования цифрового присутствия и соблюдения принципа контролируемых зон, необходимо использовать нескомпрометированное аппаратное и программное обеспечение, а также конфигурировать его должным образом.

Важно отметить, что описываемые принципы настройки программного оборудования не гарантируют стопроцентной защиты от утечек персональных

данных, поэтому должны использоваться совместно с организацией офлайн- и онлайн-присутствия.

Аппаратное обеспечение

Необходимо тщательно подходить к вопросу выбора аппаратного обеспечения, по возможности ориентируясь на устройства без явных фактов дискредитации. Выбираемые устройства должны поддерживать последние разработки в плане защиты персональных данных и работать под управлением актуальных версий операционных систем с последними обновлениями, позволяющими закрыть известные бреши в системе безопасности.

Конфигурации устройств не должны поддерживать возможность несанкционированного доступа, как по сетевым каналам, так и с помощью внешних устройств и оптических дисков. Кроме того, не допускается использование стандартных (дефолтных) паролей для доступа к аппаратному обеспечению.

Носители информации в устройствах должны поддерживать и использовать шифрование данных.

При продаже или уничтожении устройств, хранящих данные (к примеру, оперативной памяти или жестких дисков), необходимо убедиться в тщательном удалении (уничтожении) данных на носителе и невозможности их восстановления. Для этого используются специальные программные или аппаратные инструменты.

Программное обеспечение

Практически все устройства находятся под управлением нескольких наиболее распространенных операционных систем. Среди этих устройств – смартфоны, телевизоры, настольные компьютеры и ноутбуки, планшетные компьютеры, автомобили и многое другое. Важно критически подходить к выбору операционной системы своего устройства – и не использовать те, о которых имеются сведения о дискредитации. Также необходимо учитывать важный аспект, касающийся использования только официальных версий систем. Версии, находящиеся во взломанном виде в открытом доступе, могут содержать зловредное программное

обеспечение. Пользователь должен обладать достаточным сетевым опытом и техническим бэкграундом, чтобы отличить безопасную сборку от небезопасной.

Необходимо опираться на следующие принципы, относящиеся как к операционным системам, так и к прикладному программному обеспечению:

1. Пользоваться лицензионными версиями программного обеспечения;
2. По возможности/при необходимости делать выбор в пользу защищенных операционных систем;
3. Скачивание приложений производить только через официальные источники;
4. Всегда проверять надежность производителя приложения (не ограничиваться исключительно рейтингами других пользователей и отзывами) и официальность сборки (проверять хэш-сумму загруженного файла и другие методы);
5. Устанавливать только минимум нужных приложений и своевременно удалять неиспользуемые программы. Особенно это касается уязвимого программного обеспечения, такого Java и Flash;
6. Отдавать предпочтение программному обеспечению, которое обладает функционалом защиты от утечек персональных данных;
7. Внимательно и осознанно предоставлять доступ к персональным данным при появлении запросов от устанавливаемого программного обеспечения;
8. Внимательно анализировать лицензионные соглашения на предмет обязанностей пользователя и разработчика;
9. Своевременно обновлять программное обеспечение и драйверы используемых устройств
10. В случае подключения к точкам доступа Wi-Fi, Bluetooth, а также базовым станциям оператора сотовой связи по возможности удостоверяться в надежности устройства связи. Не осуществлять подключение к публичным (открытым) точкам доступа к цифровой среде. Отключать неиспользуемые интерфейсы связи;
11. Использовать надежные парольные политики. Не допускать использование стандартных (дефолтных) паролей для доступа (а также открытого доступа) к программному обеспечению. По возможности следует использовать

системы многофакторной аутентификации с помощью нескомпрометированных устройств;

12. Применять средства антивирусной и антифишинговой защиты.

Также недопустимо относиться к личным портативным устройствам как публичным, доступным для обмена с другими пользователями, возможными для временного использования другими лицами. Такое поведение упрощает доступ к операционной системе со стороны недоверенных лиц и нарушает конфиденциальность данных.

Отдельно стоит обращать внимание на браузерные приложения – им после операционных систем доступен наиболее обширный пласт данных о пользователе. Как и в случае с прочим программным обеспечением, следует делать выбор в сторону программ, акцентирующих внимание на отсутствие элементов отслеживания действий пользователя и предоставляющих дополнительные меры по защите от угроз безопасности персональных данных.

При выборе любого другого программного обеспечения следует руководствоваться теми же принципами, а также не допускать возможности установки программного обеспечения недоверенными лицами.

Превентивные меры

В вопросах информационной безопасности, как и любых сферах предупреждения рисков, важно предпринимать меры, предупреждающие риск. Деятельность по устранению последствий, по сути своей, не является направленной на поддержание безопасности.

Поэтому пользователь должен осознавать связь пользования устройством с угрозами такого использования, учитывая рост информационных рисков.

В большинстве полноценных сервисов пользователи используют учетные записи. Учетная запись используется для сохранения настроек, авторизации и для синхронизации между устройствами.

Рекомендуемой практикой является создание не менее двух учетных записей. Одна из которых предоставляет права администратора, а другая – права обычного пользователя. При работе в условиях повышенного риска следует использовать

запись с ограниченными правами. Даже если запись пользователя будет взломана, без прав администратора злоумышленник не сможет нанести серьезного вреда.

Также необходимо использовать разные учетные записи на разных устройствах и не синхронизировать их между собой, по крайней мере, в автоматическом режиме.

Между тем, пользователь должен предпринимать шаги на случай своей ошибки или на случай обхода злоумышленников мер безопасности. Поэтому пользователю необходимо через определенные промежутки времени создавать резервные копии чувствительных данных и хранить их на нескомпрометированном устройстве в безопасном месте.

Принятие превентивных мер позволит существенно снизить уровень информационных угроз в обществе.

7.5. Организация онлайн и офлайн присутствия

Наиболее важным элементом безопасности является контроль своего поведения и отражение его в аппаратных и программных средствах путем конфигурирования, добавлением инструментов, обеспечивающих дополнительный уровень защиты, или отказом от тех или иных функций.

К таким элементам контроля следует отнести необходимость защиты всех устройств с помощью сложных парольных фраз, применению защищенных каналов связи типа VPN и отключение потенциально небезопасных функций, таких, как геолокация, в случае отсутствия необходимости использования (к примеру, в смартфоне при одновременном использовании отдельного навигационного устройства).

При этом, по возможности, необходимо использовать различные технологии защищенных каналов связи.

Учет своего поведения и настройки устройств в соответствующем своему поведению виде позволит свести угрозы информационной безопасности к минимуму, повысить качество доверия в информационной среде и защитить пользователя.

Формировать свои привычки поведения с учетом цифрового присутствия следует по принципам непрерывной слежки, постоянного риска утечки персональных данных и понимания, что переданные в цифровую среду данные остаются там навсегда.

При использовании программных средств и Интернет-сервисов следует делать выбор в пользу тех, которые:

1. Не дискредитированы;
2. Запрашивают разрешение на минимальный набор персональных данных (либо не запрашивают вовсе);
3. Обладают средствами сквозного шифрования персональных данных в цифровом периметре и доказали эффективность этих средств исследованиями соответствующих органов и организаций;
4. Реализуют дополнительные меры защиты персональных данных (к примеру, не допуская их хранение или осуществляя удаление через короткое или определенное время) пользователей; а также допускающих подключение через защищенные протоколы связи;
5. Допускают удаление персональных данных автоматически или вручную (очистка истории посещений в браузере, удаление журнала использования программы и т.п.).

Аналогичными мерами можно воспользоваться и в реальной жизни:

1. Пользоваться для общения помещениями и местами открытого пространства, исключающими несанкционированный сбор информации (отсутствуют посторонние лица, не установлены устройства сбора информации и т.п.);
2. При общении через Интернет или телефонные сети указывать минимальное количество персональных данных. Помнить о возможности посреднической атаки, при которой невидимый собеседник может быть скомпрометирован;
3. При общении через Интернет или телефонные сети использовать кодовые фразы и прочие ассоциации с целевой информацией, предоставляя ее в открытом виде собеседнику только при личном контакте в безопасной контролируемой зоне;

4. По возможности, не использовать физические объекты для хранения конфиденциальной информации (не хранить пароли на бумажных носителях на рабочем столе), либо хранить такие объекты в местах, исключающих доступ посторонних лиц (к примеру, сейфах);
5. Удалять данные о себе, если необходимость в них отсутствует.

Описанные меры хотя и не позволяют достичь стопроцентной гарантии безопасности цифрового и нецифрового присутствия, дают возможность уменьшить риск утечки персональных данных и нанесения потенциального ущерба субъекту персональных данных.

8. Заключительные положения

Как уже говорилось ранее, цифровое присутствие каждого человека получает все большее распространение и становится необходимым фактором обеспечения производственной деятельности и эффективного общения. При этом цифровое присутствие может быть как контролируемым, так и вынужденным, то есть осуществляющимся без участия самого субъекта за счет деятельности и устройств третьих лиц.

Несмотря на все положительные моменты цифрового присутствия и его необходимость в жизни каждого человека, в данной сфере всплывает один очень существенный недостаток – а именно риск утечки персональных данных и риск использования "утекших" данных против их субъекта.

Данный риск возникает не только по причине бесконтрольного распространения своих персональных данных физическими лицами, но и по вине недобросовестных операторов персональных данных, не принимающих должные меры по защите хранящийся и обрабатываемой на их устройствах информации, а также по причине неправильно сконфигурированных устройств и/или устройств, имеющих изъяны в программном и аппаратном обеспечении.

Цель данного документа – обратить внимание на проблему защиты (охраны) цифрового присутствия человека от целенаправленных и случайных попыток получения доступа к его персональным данным, попытаться сформировать свод

общих концепций по безопасному использованию цифровых устройств и услуг в эпоху удобной и одновременно представляющей угрозу частной жизни технологии больших данных (BigData).

Предложенные концепции могут быть использованы для совершенствования механизмов регулирования цифровой экономики, в первую очередь, сферы персональных данных.

Документ разработан рабочей группой
по вопросам организационной защиты персональных данных
Консультативного совета при уполномоченном органе
по защите прав субъектов персональных данных
под общей редакцией:
Алехиной И.Г., Председателя Консультативного совета при уполномоченном органе по защите прав субъектов персональных данных, ученого секретаря Центра инженерного образования Российской академии образования - Российского государственного университета нефти и газа (НИУ) имени И.М. Губкина
Понявина А.В., Директора Исполкома Национального Дельфийского совета России;
Черникова С.В., аналитика, автора книг по информационной безопасности.