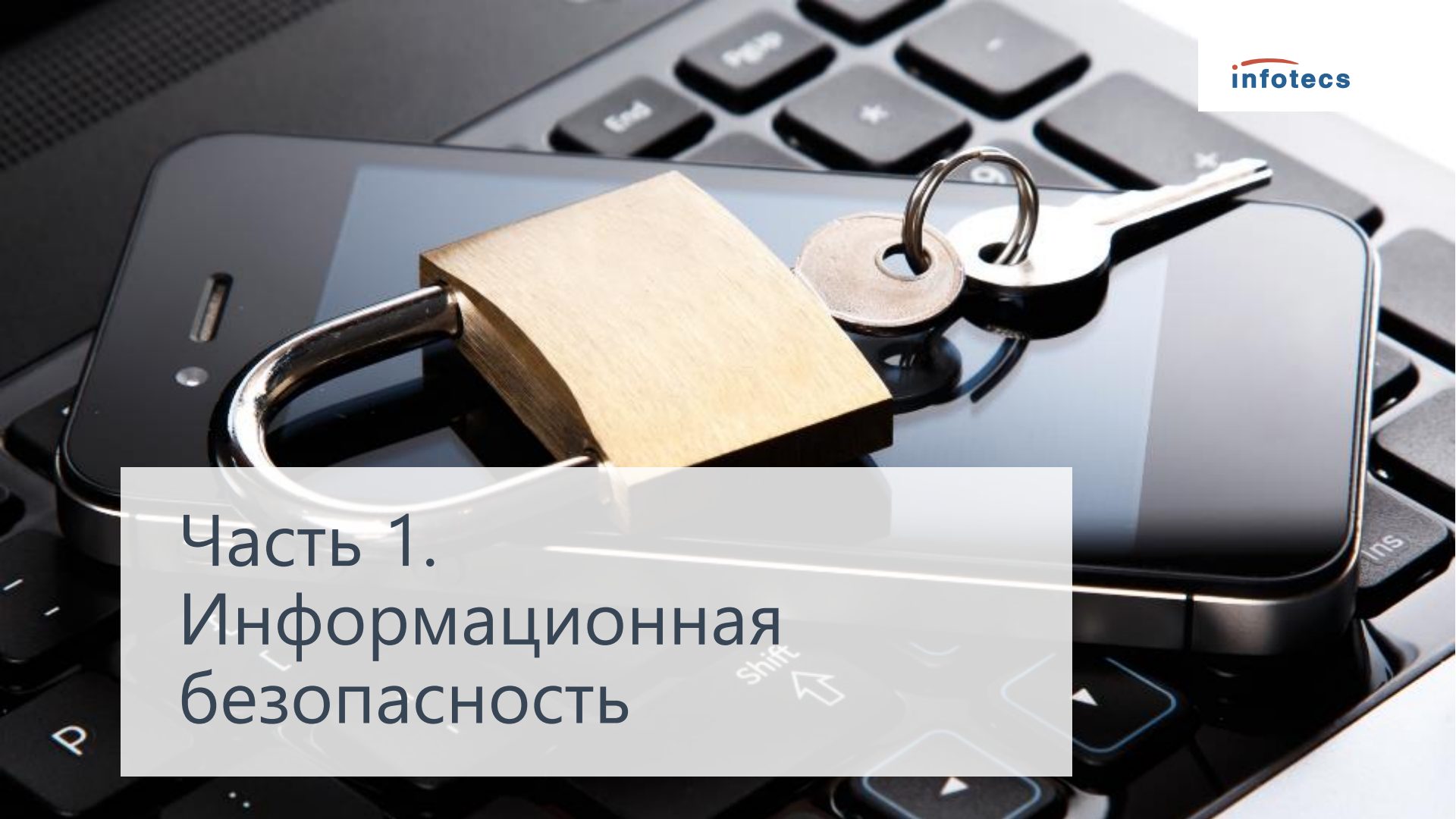
Информационная безопасность, персональные данные

ОАО «ИнфоТеКС», Москва
(495) 737-61-92
www.infotecs.ru
НОЧУ ДПО ЦПК «Учебный центр «ИнфоТеКС»
education@infotecs.ru

Олег Кузьмин
менеджер проектов НОЧУ ДПО ЦПК «Учебный центр «ИнфоТеКС»



Часть 1. Информационная безопасность

Что такое информация

Информация, это ресурс	▪ в современном мире информация является таким же ценным, а в ряде случаев и более ценным, ресурсом, как всем привычные природные ресурсы в виде различного рода полезных ископаемых, территориальных, человеческих и пищевых ресурсов
Информация, это товар, который подвержен как общепринятым нормам его передачи в виде дарения, купли-продажи, так и различными нелегальными и преступными способами завладения	▪ незаконное получение информации третьими лицами в целом приводит к материальному ущербу для ее собственника. Например, раскрытие технологии изготовления оригинального продукта приведет к появлению аналогичного продукта, но от другого производителя, и, как следствие, владелец технологии потеряет часть рынка и т.д.
Информация, это субъект управления, т.к. информационные ресурсы в современном мире непосредственно участвуют в организации управления всеми аспектами жизни человека и общества	▪ неправомерное изменение информации в процессе формирования управленческих воздействий может привести к нанесению морального, материального, физического ущерба для человека и к возникновению аварийных и катастрофических последствий для технических систем

Защита информации

ГОСТ 50922-2006 «Защита информации. Основные термины и определения»

- защита информации - деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию

Решение проблем информационной безопасности

- начинаются с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем. Это обусловлено тем, что для разных категорий субъектов характер решаемых задач может существенно различаться.

Важные выводы

- задачи по обеспечению информационной безопасности для разных категорий субъектов могут существенно различаться;
- информационная безопасность не сводится исключительно к защите от несанкционированного доступа к информации – это принципиально более широкое понятие.
- информационная безопасность есть составная часть информационных технологий – области, развивающейся беспрецедентно высокими темпами;
- в области информационной безопасности важны не столько отдельные решения (законы, знание основ работы с программным обеспечением, программно-технические изделия), находящиеся на современном уровне, сколько механизмы генерации новых решений, позволяющие, как минимум, адекватно реагировать на угрозы информационной безопасности или предвидеть новые угрозы и уметь им противостоять

Виды защиты информации согласно ГОСТ 50922-2006

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

Техническая защита информации – защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств

Криптографическая защита информации – защита информации с помощью ее криптографического преобразования.
Физическая защита информации – защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты

Эволюция понятия «информационная безопасность» в Российской Федерации

Первое упоминание без акцентирования внимания на определении понятия

- Закон РФ от 05.03.1992 г. № 2446-I «О безопасности» (утратил силу в связи с принятием Федерального закона от 28.12.2010 г. № 390-ФЗ «О безопасности»)

Первая формулировка понятия на законодательном уровне

- Федеральный закон от 04.07.1996 г. № 85-ФЗ «Об участии в международном информационном обмене» (утратил силу с принятием Федерального закона от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»)

Действующие законодательные и нормативные документы, где определено понятие «информационная безопасность»

- Указ Президента Российской Федерации от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;
- ГОСТ Р 53113.1-2008 «Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения»;
- ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»

Понятие «информационная безопасность» в законодательных и нормативных документах

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

- **информационная безопасность Российской Федерации** – состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства

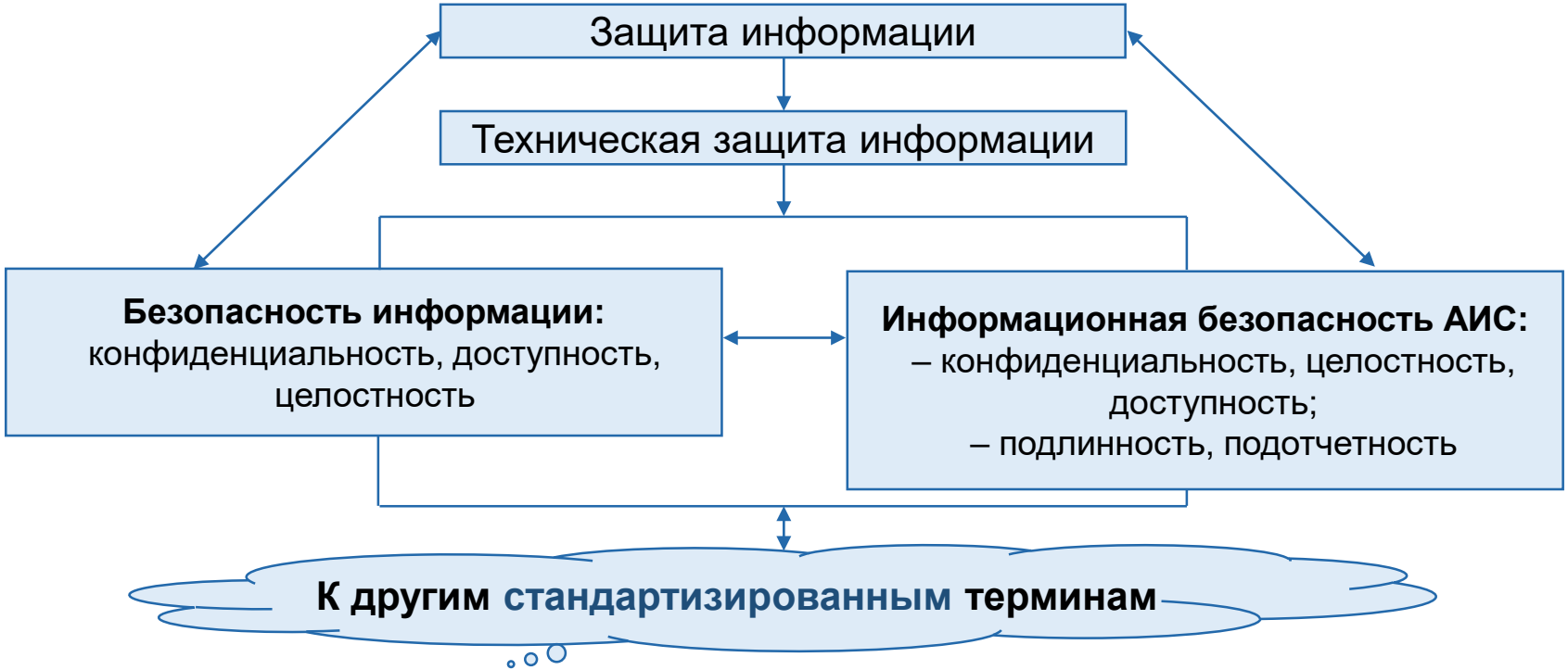
ГОСТ Р 53113.1-2008 «Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения»

- **информационная безопасность** - все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации или средств ее обработки

ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»

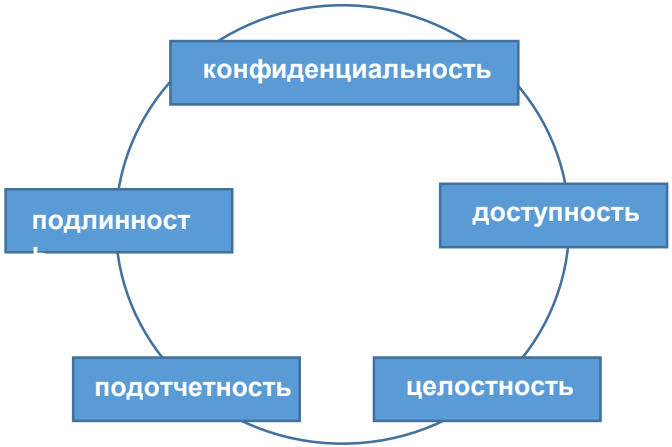
- **информационная безопасность** - свойство информации сохранять конфиденциальность, целостность и доступность. Кроме того, данное понятие может включать в себя также и свойство сохранять аутентичность, подотчетность, неотказуемость и надежность

Схема взаимосвязи стандартизированных элементов



Р 50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации

Схема взаимосвязи стандартизированных элементов



конфиденциальность информации – это состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право;
целостность информации – это состояние информации, при котором ее изменение осуществляется только преднамеренно субъектами, имеющими на него право;
доступность информации – это состояние информации, при котором субъекты, имеющие право доступа (т.е. право на чтение, изменение, копирование, уничтожение информации, а также права на изменение, использование, уничтожение ресурсов), могут реализовать их беспрепятственно;

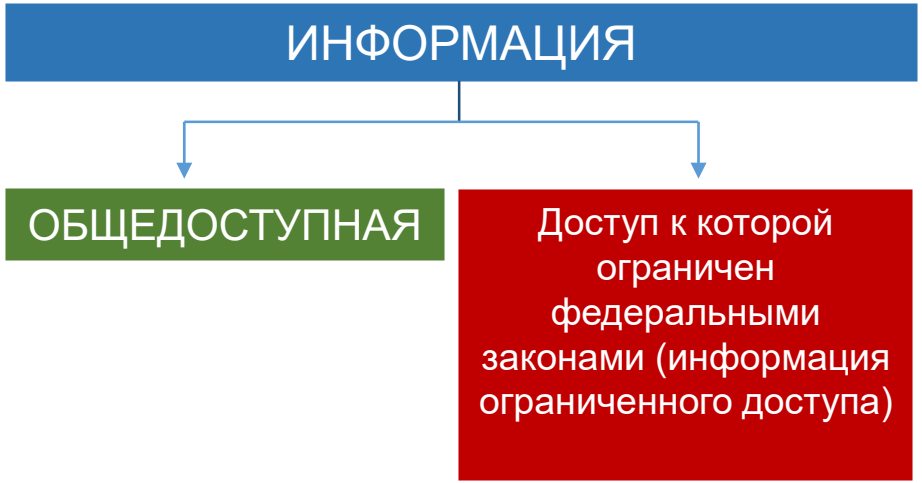
подотчетность информационных ресурсов АИС – это состояние информационных ресурсов, при котором обеспечиваются их идентификация и регистрация;
подлинность информационных ресурсов АИС – это состояние информационных ресурсов, при котором обеспечивается реализация информационной технологии с использованием именно тех ресурсов, к которым субъект, имеющий на это право, обращается.

Р 50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации

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

- Информация может являться объектом публичных, гражданских и иных правовых отношений.
- Информация может свободно использоваться любым лицом и передаваться одним лицом другому лицу, **если федеральными законами не установлены ограничения доступа к информации либо иные требования к порядку ее предоставления или распространения**.

Классификация информации по категории доступа



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

предоставление информации - действия, направленные на получение информации **определенным кругом лиц** или передачу информации **определенному кругу лиц**;

распространение информации - действия, направленные на получение информации **неопределенным кругом лиц** или передачу информации **неопределенному кругу лиц**;

Классификация информации в зависимости от порядка её предоставления или распространения

ИНФОРМАЦИЯ

- Информация, свободно распространяемая
- Информация, предоставляемая по соглашению лиц, участвующих в соответствующих отношениях
- Информация, распространение которой в РФ ограничивается или запрещается
- Информация, которая в соответствии с федеральными законами подлежит предоставлению или распространению

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

Обладатель информации

Права:

- разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;
- использовать информацию, в том числе распространять ее, по своему усмотрению;
- передавать информацию другим лицам по договору или на ином установленном законом основании;
- защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;
- осуществлять иные действия с информацией или разрешать осуществление таких действий.

Обязанности:

- соблюдать права и законные интересы иных лиц;
- принимать меры по защите информации;
- ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

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

- Граждане (физические лица) и организации (юридические лица) **вправе** осуществлять **поиск и получение любой информации** в любых формах и из любых источников при условии соблюдения требований, установленных настоящим Федеральным законом и другими федеральными законами.

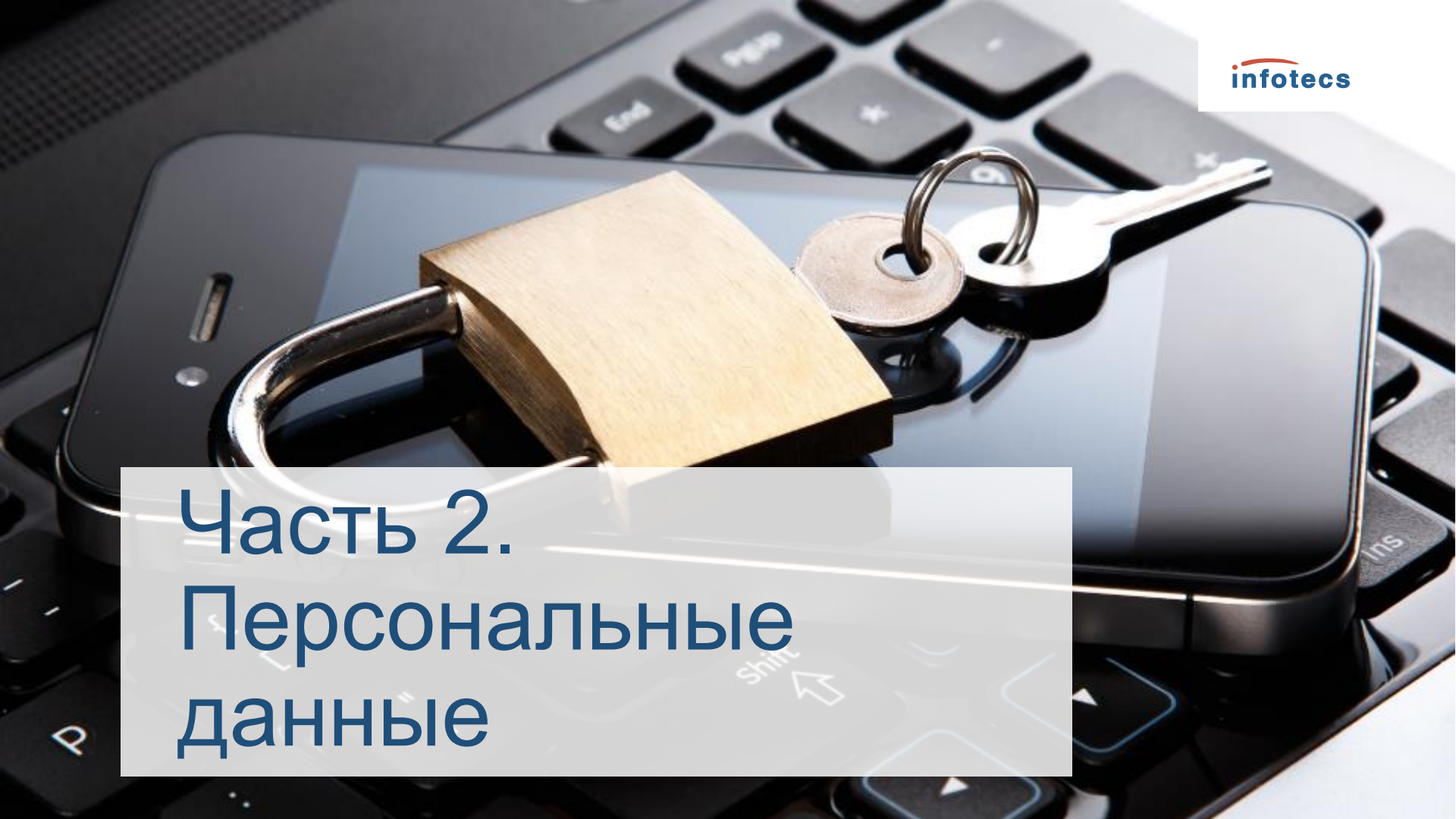
- Гражданин (физическое лицо) **имеет право** на получение от государственных органов, органов местного самоуправления, их должностных лиц в порядке, установленном законодательством Российской Федерации, информации, непосредственно затрагивающей его права и свободы.

- Организация **имеет право** на получение от государственных органов, органов местного самоуправления информации, непосредственно касающейся прав и обязанностей этой организации, а также информации, необходимой в связи с взаимодействием с указанными органами при осуществлении этой организацией своей уставной деятельности.

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

Не может быть ограничен доступ к:

1) **нормативным правовым актам**, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;
2) информации о состоянии **окружающей среды**;
3) информации **о деятельности государственных органов** и **органов местного самоуправления**, а также **об использовании бюджетных средств** (за исключением сведений, составляющих государственную или служебную тайну);
4) информации, накапливаемой **в открытых фондах** библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;
5) **иной информации**, недопустимость ограничения доступа к которой установлена федеральными законами.



Часть 2. Персональные данные

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

Статья 1. Сфера действия настоящего Федерального закона
Регулирует отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами, . . . физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным.

Статья 2. Цель настоящего Федерального закона
Целью настоящего ФЗ является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность **частной жизни, личную и семейную тайну**.

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

Статья 3. Основные понятия, используемые в настоящем Федеральном законе

В целях настоящего Федерального закона используются следующие основные понятия:

1. **персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
2. **оператор** - 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;
3. **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;

Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных (Страсбург, 28 января 1981 года)

Ратифицирована Федеральным законом от 19.12.2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»

Ограничения по применению в Российской Федерации:

1. Российская Федерация заявляет, что в соответствии с подпунктом «а» пункта 2 статьи 3 Конвенции не будет применять Конвенцию к персональным данным:

а) обрабатываемым физическими лицами **исключительно для личных и семейных нужд**;

б) отнесенным к **государственной тайне** в порядке, установленном законодательством Российской Федерации о государственной тайне;

2. Российская Федерация заявляет, что в соответствии с подпунктом «с» пункта 2 статьи 3 Конвенции будет применять Конвенцию к персональным данным, которые не подвергаются автоматизированной обработке, если применение Конвенции **соответствует характеру действий, совершаемых с персональными данными без использования средств автоматизации**;
3. Российская Федерация заявляет, что в соответствии с подпунктом «а» пункта 2 статьи 9 Конвенции оставляет за собой право устанавливать ограничения права субъекта персональных данных на доступ к персональным данным о себе **в целях защиты безопасности государства и общественного порядка**.

Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных (Страсбург, 28 января 1981 года)

Статья 1. Предмет и цель

Цель настоящей Конвенции состоит в обеспечении на территории каждой Стороны для **каждого физического лица**, независимо от его гражданства или местожительства, уважения его прав и основных свобод, и в частности его права на неприкосновенность частной жизни, в отношении автоматизированной обработки касающихся его персональных данных («защита данных»).

Статья 2. Определения

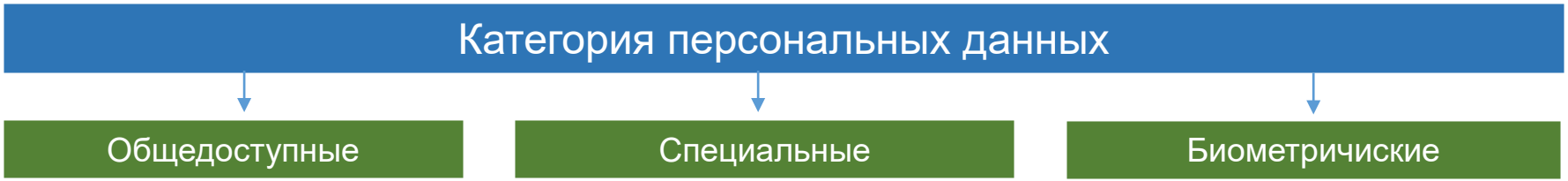
а) «персональные данные» означают любую информацию об определенном или поддающемся определению физическом лице («субъект данных»);

б) «автоматизированный файл данных» означает любой набор данных, подвергающийся автоматизированной обработке;

в) «автоматизированная обработка» включает в себя следующие операции, осуществляемые полностью или частично с помощью автоматизированных средств: хранение данных, осуществление логических и/или арифметических операций с этими данными, их изменение, уничтожение, поиск или распространение;

г) «контролер файла» означает физическое или юридическое лицо, орган государственной власти, учреждение или любой другой орган, компетентный в соответствии с внутренним законодательством **решать**, какова должна быть цель автоматизированного файла данных, какие категории персональных данных подлежат хранению или какие операции должны производиться с ними.

Классификация персональных данных исходя из правового режима

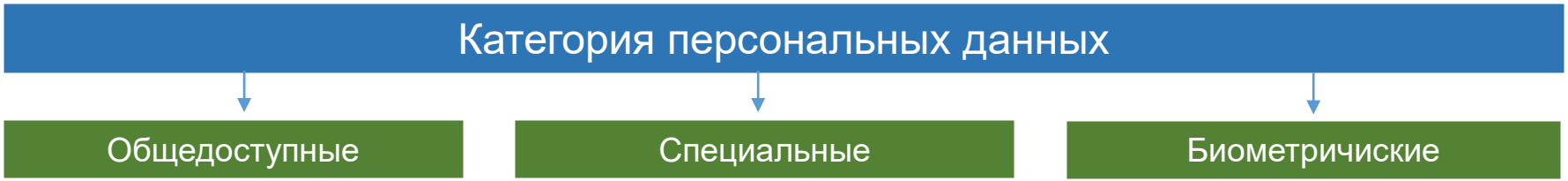


Статья 8. Общедоступные источники персональных данных

1. В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных.
2. Сведения о субъекте персональных данных 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.

Общедоступные источники персональных данных могут использоваться любыми лицами по их усмотрению при соблюдении установленных в **Статье 6. Условия обработки персональных данных** ограничений.

Классификация персональных данных исходя из правового режима



Статья 10. Специальные категории персональных данных
1. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, **НЕ ДОПУСКАЕТСЯ**, за исключением случаев, предусмотренных **частью 2** настоящей статьи.

Статья 11. Биометрические персональные данные
1. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных, могут обрабатываться **ТОЛЬКО** при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных **частью 2** настоящей статьи.

Классификация персональных данных по признаку свободы оборота

Группы персональных данных			
Свободно обращаемые	Ограниченно обращаемые	Обращаемые в специальных целях	Запрещенные к обороту

Свободно обращаемые персональные данные - это имя, фамилия, отчество и пол липа. В некоторых случаях к ним можно добавить возраст, образование, адрес места жительства, номер телефона, т. е. все те минимальные сведения, которые готов сообщить о себе субъект определённому кругу лиц и организаций, составляющих круг его каждодневного социального общения.

Как правило, несанкционированное использование этих сведений не может причинить субъекту какого-либо существенного вреда, поэтому применение мер ответственности возможно только в том случае, если нарушен порядок сбора и обработки этой информации (в частности, должностным лицом).

Например, Статья 22. Уведомление об обработке персональных данных
2. Оператор вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных:
4) сделанных субъектом персональных данных общедоступными;
5) включающих в себя только фамилии, имена и отчества субъектов персональных данных

Классификация персональных данных по признаку свободы оборота

Группы персональных данных			
Свободно обращаемые	Ограниченно обращаемые	Обращаемые в специальных целях	Запрещенные к обороту

Ограниченно обращаемые персональные данные - это различные виды персональных данных, в том числе и данные регистрационных номеров документов, сообщаемые субъектом (с его согласия) различным организациям и органам с целью совершения каких-либо действий или получения каких-либо услуг.

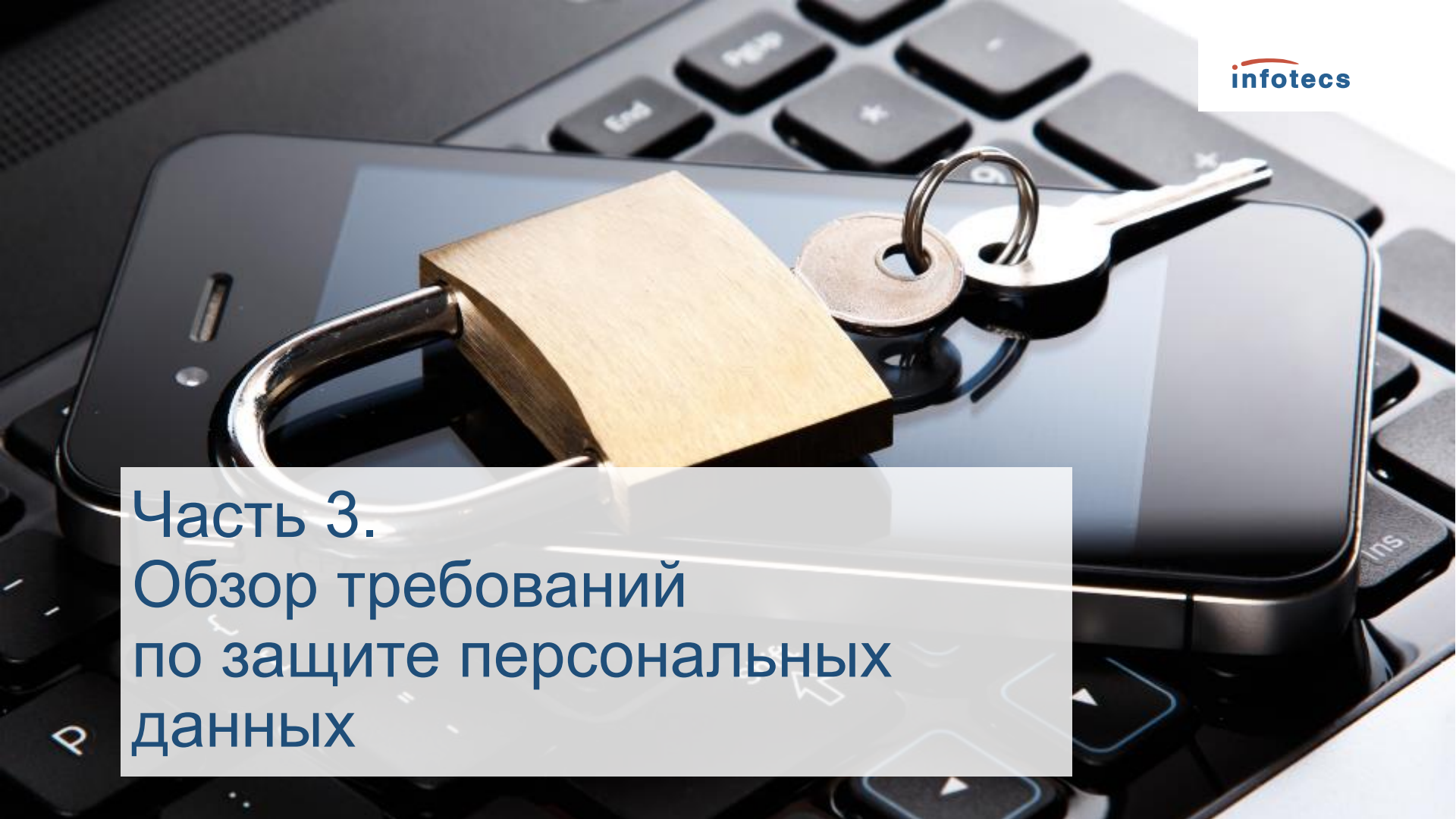
Например, для оформления потребительского кредита заёмщик должен сообщить помимо прочих данные о месте работы, должности, размере заработной платы, наличии движимого и недвижимого имущества и т. п. Разглашение или иное несанкционированное использование полученных персональных данных есть грубое нарушение неприкосновенности частной жизни субъекта персональных данных, способное причинить ему моральный и материальный ущерб. Субъектами мер ответственности в данном случае будут выступать преимущественно должностные лица, что может влиять на тяжесть применяемых мер ответственности.

Классификация персональных данных по признаку свободы оборота

Группы персональных данных			
Свободно обращаемые	Ограниченно обращаемые	Обращаемые в специальных целях	Запрещенные к обороту

Персональные данные, обращаемые в специальных целях - это те персональные данные, в том числе биометрические, которые собираются государственными, муниципальными и иными уполномоченными органами в рамках их полномочий в соответствии с законодательством. Согласие субъекта на сбор этих персональных данных требуется не всегда. К таким сведениям относится, например, информация об усыновлении. Разглашение и иное несанкционированное использование этих данных должно влечь за собой жёсткие меры ответственности.

Запрещённые к обороту персональные данные — это наиболее чувствительная информация, т. е. специальные категории персональных данных. За нарушения положений законодательства о защите специальных категорий персональных данных должны устанавливаться наиболее жёсткие меры ответственности.



Часть 3.
Обзор требований по защите персональных данных

Защита персональных данных работников

Согласно **п. 7 ст. 86 ТК РФ** защиту персональных данных работника от неправомерного их использования или утраты работодатель должен обеспечивать **за счёт своих средств**.

В соответствии со **ст. 87 ТК РФ** порядок хранения и использования персональных данных работников устанавливается работодателем, при этом необходимо учитывать, что для определённых носителей информации может устанавливаться особый порядок хранения и обращения (например, материальные носители биометрических персональных данных). Из данных норм следует, что работодатель должен **издать соответствующий локальный нормативный акт**, регулирующий вопросы хранения и использования персональных данных, а также обеспечивающий защиту последних от неправомерного их использования или утраты.

С соответствующим актом, а также со своими правами в сфере защиты персональных данных: работники должны быть ознакомлены под роспись.

Согласно **ст. 88 ТК РФ** работодатель должен не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных настоящим Кодексом или иными федеральными законами.

Разъяснения Роскомнадзора по защите персональных данных работников

Разъяснения Роскомнадзора от 14.12.2012 г. «Обработка ПДн работников, соискателей на замещение вакантных должностей, а также лиц, находящихся в кадровом резерве»

Работодатель вправе без соответствующего согласия осуществлять обработку персональных данных работника в случаях:
1. предусмотренных коллективным договором, в том числе правилами внутреннего трудового распорядка, являющимися, как правило, приложением к коллективному договору, соглашением, а также локальными актами работодателя, принятыми в порядке, установленном ст. 372 Трудового кодекса РФ.
2. обязанность по обработке, в том числе опубликованию и размещению персональных данных работников в сети Интернет, предусмотрена законодательством Российской Федерации (например):

п. 7 ч. 1 ст. 79 Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» медицинская организация обязана информировать граждан в доступной форме, в том числе с использованием сети Интернет, об осуществляемой медицинской деятельности и о **медицинских работниках, об уровне их образования и об их квалификации**.

Разъяснения Роскомнадзора по защите персональных данных работников

Постановление Правительства Российской Федерации от 10.07.2013 № 582, образовательное учреждение должно размещать на своем официальном сайте в сети Интернет, в том числе информацию, содержащую следующие персональные данные:

- фамилия, имя, отчество руководителя образовательного учреждения, его место нахождения, график работы, адрес электронной почты, справочные телефоны
- фамилии, имена, отчества, должности руководителей структурных подразделений, включая филиалы и представительства, места их нахождения, графики работы, адреса электронной почты
- информация о персональном составе педагогических (научно-педагогических) работников, их фамилии, имена, отчества, занимаемые должности, их уровень образования, квалификация, наличие ученой степени, ученого звания.

Федеральный закон от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления», государственные органы и органы местного самоуправления обязаны обеспечить доступ к информации о своей деятельности, в том числе к сведениям о руководителях государственного органа, его структурных подразделений, территориальных органов и представительств за рубежом (при наличии), руководителях органа местного самоуправления, его структурных подразделений, руководителях подведомственных организаций (фамилии, имена, отчества, должности, рабочие телефоны). Иная информация может указываться только при согласии указанных лиц.

Разъяснения Роскомнадзора по распространению и обработке биометрических персональных данных

Разъяснения Роскомнадзора от 02.09.2013 «Отнесение фото- и видео- изображения, дактилоскопических данных и иной информации к биометрическим ПДн и особенности их обработки»
Исходя из определения, установленного Федеральным законом «О персональных данных» к биометрическим персональным данным относятся физиологические данные (дактилоскопические данные, радужная оболочка глаз, анализы ДНК, рост, вес и другие), а также иные физиологические или биологические характеристики человека, в том числе изображение человека (фотография и видеозапись), которые позволяют установить его личность и используются оператором для установления личности субъекта.

В соответствии со **ст. 152.1 ГК РФ**, обнародование и дальнейшее использование изображения гражданина (в том числе его фотографии, а также видеозаписи или произведения изобразительного искусства, в которых он изображен) допускаются только с согласия этого гражданина.
После смерти гражданина его изображение может использоваться только с согласия его законных представителей (супруги, дети, родители).

Разъяснения Роскомнадзора по распространению и обработке биометрических персональных данных

Такое согласие не требуется в случаях, когда:

1) использование изображения осуществляется в государственных, общественных или иных публичных интересах. (Согласно п. 25 постановления Пленума Верховного Суда Российской Федерации от 15 июня 2010 г. №16 к общественным интересам следует относить не любой интерес, проявляемый аудиторией, а, например, потребность общества в обнаружении и раскрытии угрозы демократическому правовому государству и гражданскому обществу, общественной безопасности, окружающей среде. К таким интересам, к примеру, относится информация, связанная с исполнением своих функций должностными лицами и общественными деятелями. **Соответственно, сообщение подробностей частной жизни лица, не занимающегося какой-либо публичной деятельностью, под данное исключение не подпадает**).

2) изображение гражданина получено при съемке, которая проводится в местах, открытых для свободного посещения, или на публичных мероприятиях (собраниях, съездах, конференциях, концертах, представлениях, спортивных соревнованиях и подобных мероприятиях), за исключением случаев, когда такое изображение является основным объектом использования;

3) гражданин позировал за плату.

Разъяснения Роскомнадзора по распространению и обработке биометрических персональных данных

Разъяснения Роскомнадзора от 02.09.2013 «Отнесение фото- и видео- изображения, дактилоскопических данных и иной информации к биометрическим ПДн и особенности их обработки»

Не являются биометрическими персональными данными фотографическое изображение, содержащиеся в личном деле работника, а также подпись лица, наличие которой в различных договорных отношениях является обязательным требованием, и почерк, в том числе анализируемый уполномоченными органами в рамках почерковедческой экспертизы. Все они **не могут рассматриваться как биометрические персональные данные**, поскольку действия с использованием указанных данных направлены на подтверждение их принадлежности **конкретному физическому лицу, чья личность уже определена и чьи персональные данные уже имеются в распоряжении оператора**.

Разъяснения Роскомнадзора по распространению и обработке биометрических персональных данных

Не являются биометрическим персональными данными рентгеновские или флюорографические снимки, характеризующие физиологические и биологические особенности человека, и находящиеся в истории болезни (медицинской карте) пациента (не имеет значения, бумажной или электронной), поскольку они **не используются оператором (медицинским учреждением) для установления личности пациента**. **Но в случае их передачи по запросу субъектов оперативно-розыскной деятельности, органов следствия и дознания в рамках проводимых ими мероприятий указанные сведения становятся биометрическими персональными данными, поскольку используются операторами — органами следствия и дознания в целях установления личности конкретного лица**.

Аналогичная позиция и с материалами видеосъемки в публичных местах и на охраняемой территории. **До передачи их для установления личности** снятого человека они **не являются биометрическим персональными данными**, обработка которых регулируется общими положениями Федерального закона «О персональных данных», поскольку не используются оператором (владельцем видеокамеры или лицом, организовавшим ее эксплуатацию) для установления личности. Однако, указанные материалы, используемые органами, осуществляющими оперативно-розыскную деятельность, дознание и следствие в рамках проводимых мероприятий, являются биометрическими персональными данными, в случае, если целью их обработки является установление личности конкретного физического лица.

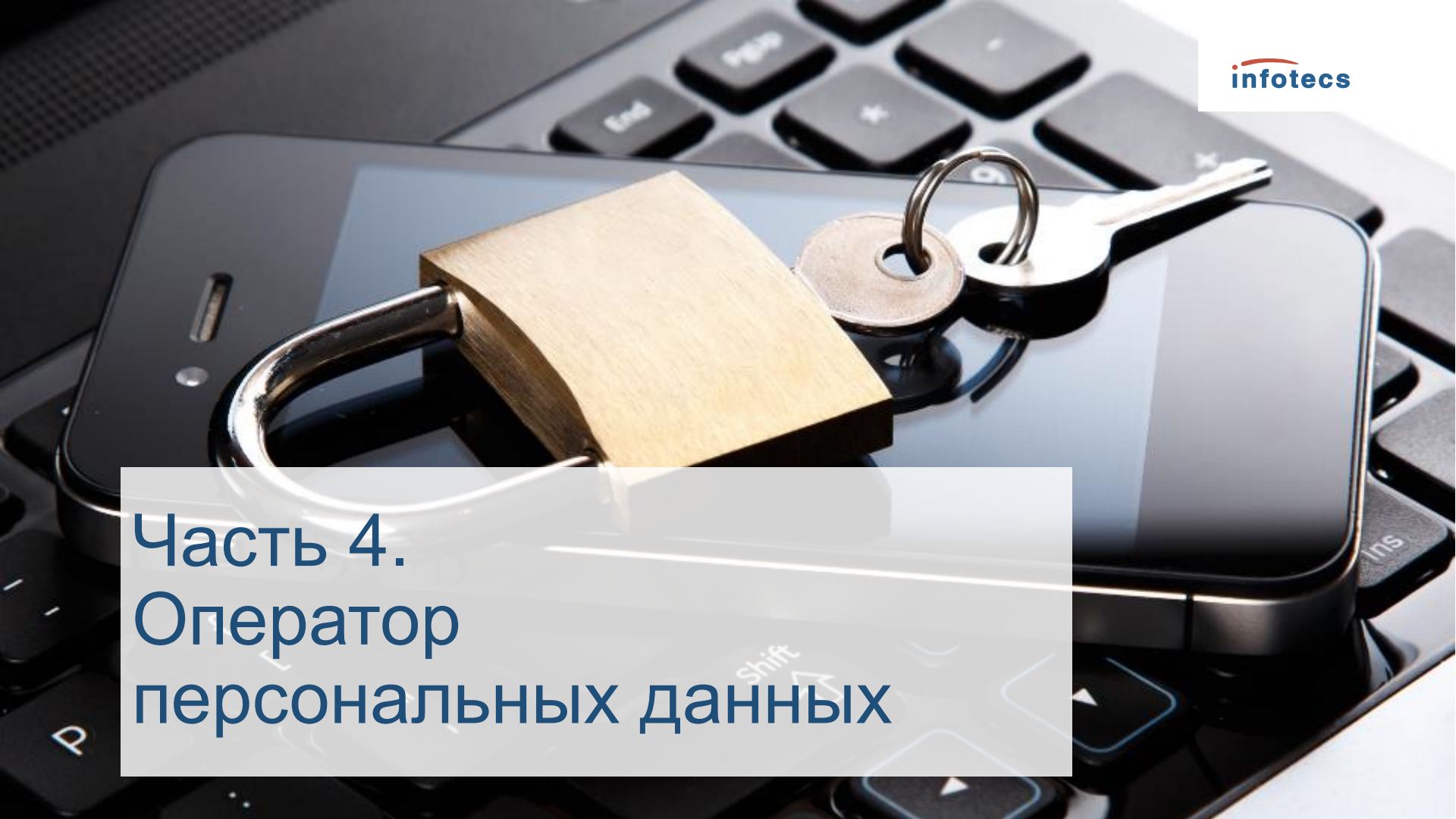
Разъяснения Роскомнадзора по распространению и обработке биометрических персональных данных

Разъяснения Роскомнадзора от 02.09.2013 «Отнесение фото- и видео- изображения, дактилоскопических данных и иной информации к биометрическим ПДн и особенности их обработки»

Обработка дактилоскопической информации в системе биометрической идентификации осуществляется путем преобразования изображения папиллярных узоров на промежуточной поверхности в цифровую форму и размещения полученных данных в базе данных в виде биометрического информационного шаблона.

Принимая во внимание, что **целью обработки указанных сведений** в системах биометрической идентификации является **установление личности конкретного лица**, а также тот факт, что данная информация, содержащаяся в шаблоне, **характеризует физиологические и биологические особенности человека** – субъекта персональных данных, то она относится к биометрическим персональным данным, обработка которых должна осуществляться в соответствии со ст. 11 Федерального закона «О персональных данных», а также Федеральным законом от 25.07.1998 № 128-ФЗ «О государственной дактилоскопической регистрации в Российской Федерации».

Ввиду изложенного, во всех случаях, не подпадающих под указанные в ч. 2 ст. 11 Федерального закона «О персональных данных», для использования дактилоскопической информации в системах идентификации, контроля и управления доступом необходимо получение от субъекта или его представителя **согласия в письменной форме** на обработку его биометрических персональных данных по правилам, установленным ч. 4 ст. 9 Федерального закона «О персональных данных».



Часть 4. Оператор персональных данных

Оператор персональных данных

В каком случае НЕ НУЖНО регистрироваться как оператор персональных данных?
(ст. 22 п.2)

Оператор вправе осуществлять **без уведомления** уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных:
1) обрабатываемых в соответствии с трудовым законодательством;
2) полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные **не распространяются**, а также **не предоставляются третьим лицам без согласия субъекта персональных данных** и используются оператором **исключительно для исполнения** указанного договора и заключения договоров с субъектом персональных данных;
3) относящихся к членам (участникам) общественного объединения или религиозной организации и обрабатываемых соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, **для достижения законных целей**, предусмотренных их учредительными документами, при условии, что персональные данные **не будут распространяться или раскрываться третьим лицам без согласия в письменной форме субъектов персональных данных**

Оператор персональных данных

В каком случае НЕ НУЖНО регистрироваться как оператор персональных данных?
(ст. 22 п.2)

4) сделанных субъектом персональных данных **общедоступными**;
5) включающих в себя только **фамилии, имена и отчества** субъектов персональных данных;
6) необходимых в целях **однократного пропуска** субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях;
7) включенных в информационные системы персональных данных, имеющие в соответствии с федеральными законами **статус государственных автоматизированных информационных систем**, а также в государственные информационные системы персональных данных, созданные в целях **защиты безопасности государства и общественного порядка**;
8) обрабатываемых **без использования средств автоматизации** в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных;
9) обрабатываемых в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, **в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства**.

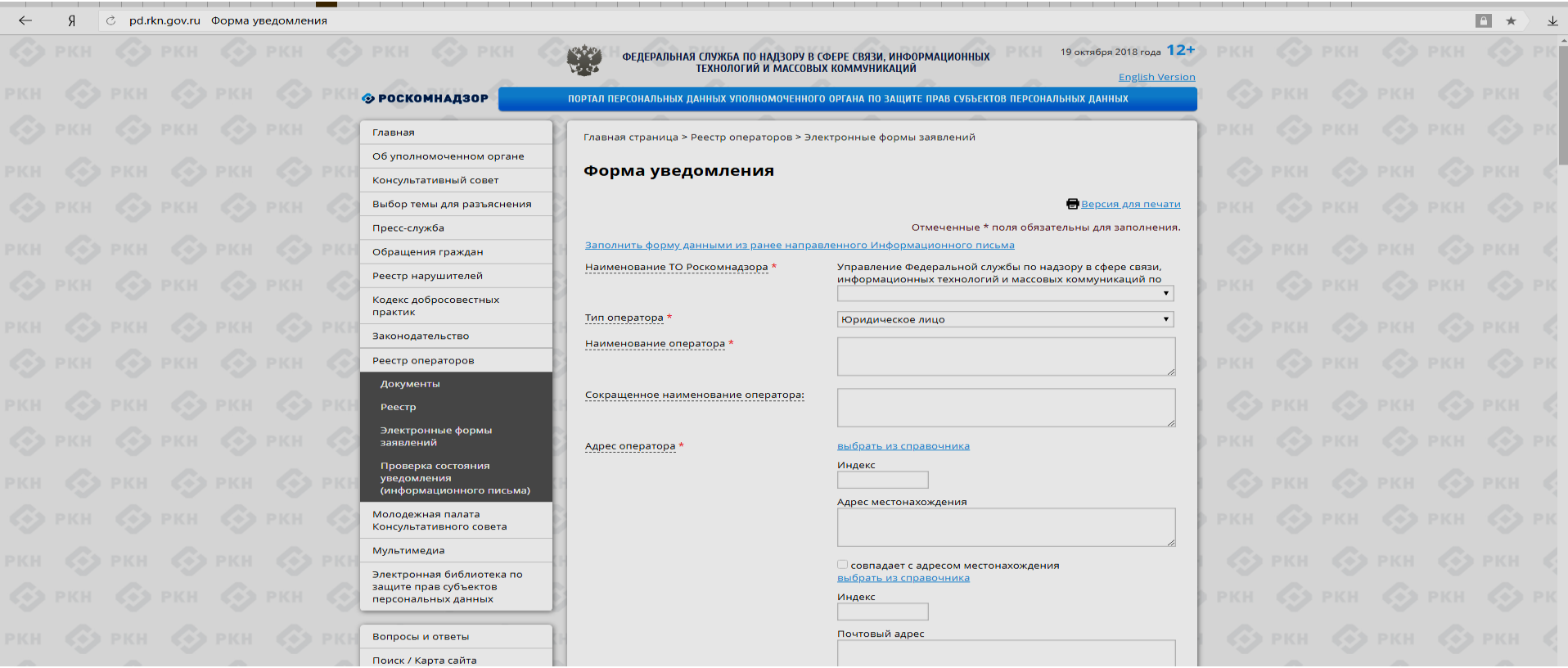
Оператор персональных данных

Ст. 22 Уведомление об обработке персональных данных
п.1 «Оператор до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных, за исключением случаев, предусмотренных **частью 2** настоящей статьи».

Уведомление должно быть направлено в письменной форме и подписано должностным лицом или направлено в электронной форме.

Образец формы уведомления об обработке персональных данных и методические рекомендации по его заполнению размещены на официальном сайте Роскомнадзора в информационно-телекоммуникационной сети «Интернет», www.pd.rkn.gov.ru

Оператор персональных данных



Оператор персональных данных

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ

19 октября 2018 года 12+

English Version

РОСКОМНАДЗОР

ПОРТАЛ ПЕРСОНАЛЬНЫХ ДАННЫХ УПОЛНОМОЧЕННОГО ОРГАНА ПО ЗАЩИТЕ ПРАВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

- Главная
- Об уполномоченном органе
- Консультативный совет
- Выбор темы для разъяснения
- Пресс-служба
- Обращения граждан
- Реестр нарушителей
- Кодекс добросовестных практик
- Законодательство
- Реестр операторов
  - Документы
  - Реестр
  - Электронные формы заявлений
  - Проверка состояния

Главная страница > Реестр операторов

Документы

1. Приказ Роскомнадзора от 30.05.2017 № 94 "Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения"
   TIF, 13.38 Mb
2. Приказ Минкомсвязи России от 20.07.2017 № 373 "О признании утратившими силу приказов Министерства связи и массовых коммуникаций Российской Федерации от 21.12.2011 № 346, от 28.08.2015 № 315 и пункта 9 приказа Министерства связи и массовых коммуникаций Российской Федерации от 24.11.2014 № 403"
   PDF, 83.05 Kb
3. Пример заполнения информационного письма
   DOC, 40.00 Kb
4. Пример заполнения уведомления
   , DOC, 53.00 Kb
5. Пример заполнения заявления о внесении в реестр операторов сведений о прекращении оператором обработки персональных данных
   DOC, 31.00 Kb
6. Пример заполнения заявления о предоставлении выписки из реестра операторов
   DOC, 30.50 Kb

Время публикации: 02.10.2009

Последнее изменение: 08.08.2018 14:25

Обязанности оператора персональных данных

ОБЯЗАННОСТИ ОПЕРАТОРА (152-ФЗ от 27.07.2006)

при сборе персональных данных (**статья 18**) по обеспечению безопасности персональных данных при их обработке (**статья 19**) при обращении к нему субъекта персональных данных либо при получении запроса субъекта персональных данных или его представителя, а также уполномоченного органа по защите прав субъектов персональных данных (**статья 20**) по устранению нарушений законодательства, допущенных при обработке персональных данных, по уточнению, блокированию и уничтожению персональных данных (**статья 21**)

Обязанности оператора персональных данных

предоставить субъекту персональных данных по его просьбе информацию, предусмотренную частью 7 статьи 14 настоящего Федерального закона (**ч. 1, ст. 18**)

1) подтверждение факта обработки персональных данных оператором;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые оператором способы обработки персональных данных;

4) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;

5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

Обязанности оператора персональных данных

предоставить субъекту персональных данных по его просьбе информацию, предусмотренную частью 7 статьи 14 настоящего Федерального закона (**ч. 1, ст. 18**)

6) сроки обработки персональных данных, в том числе сроки их хранения;

7) порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;

8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

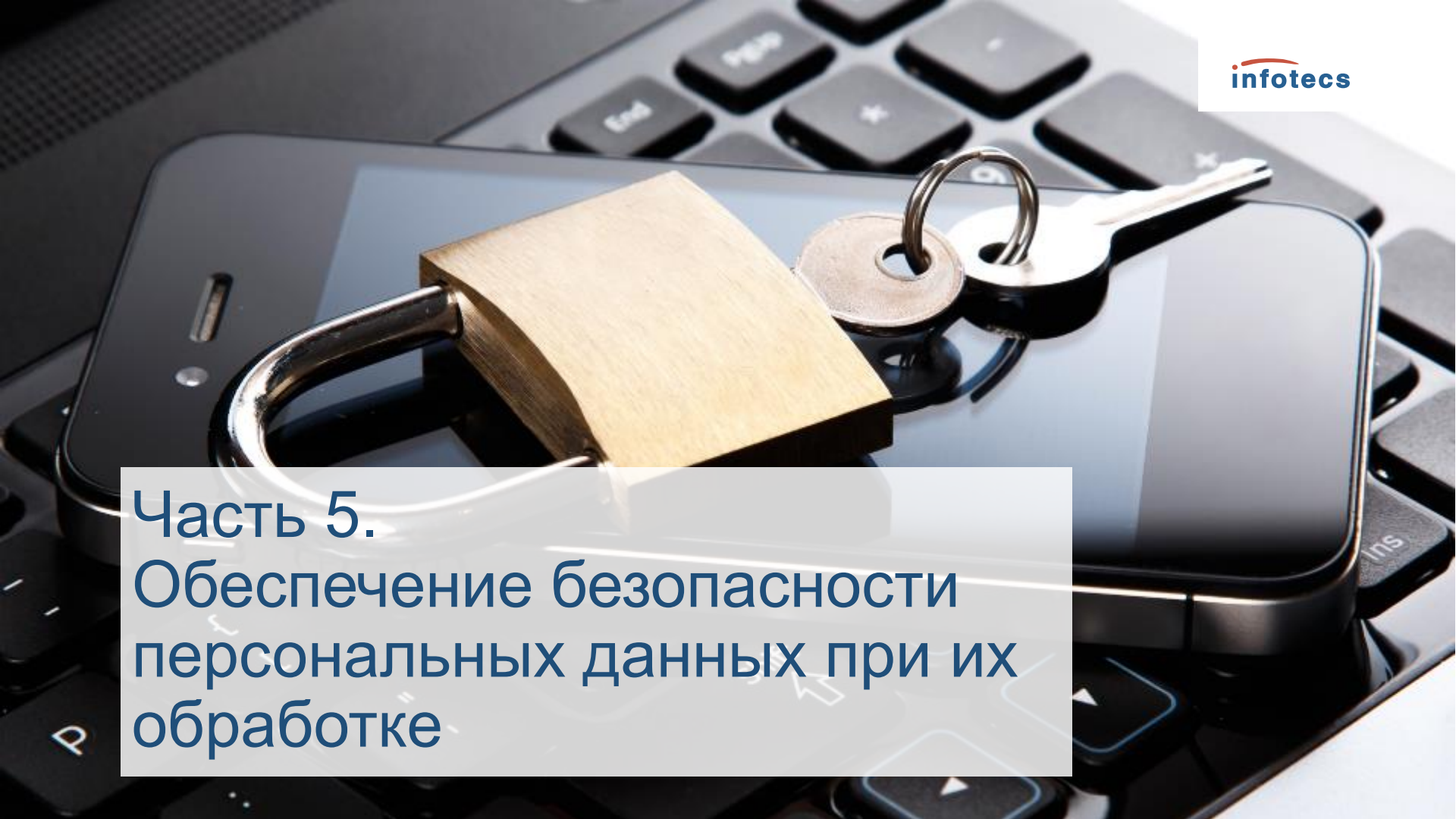
10) иные сведения, предусмотренные настоящим Федеральным законом или другими федеральными законами.

Обязанности оператора персональных данных

Если предоставление персональных данных является обязательным в соответствии с федеральным законом, оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные (**ч. 2, ст. 18**)

Если персональные данные получены не от субъекта персональных данных, оператор, за исключением случаев, предусмотренных частью 4 настоящей статьи, до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию (**ч. 3, ст. 18**)

1) наименование либо фамилия, имя, отчество и адрес оператора или его представителя;
2) цель обработки персональных данных и ее правовое основание;
3) предполагаемые пользователи персональных данных;
4) установленные настоящим Федеральным законом права субъекта персональных данных;
5) источник получения персональных данных.



Часть 5. Обеспечение безопасности персональных данных при их обработке

Обеспечение безопасности персональных данных при их обработке

Нормативно-правовое регулирование

Федеральный закон № 152-ФЗ от 27.07.2006 «О персональных данных» (статья 19)

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

Постановление Правительства РФ от 06.07.2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»

Постановление Правительства РФ от 18.09.2012 г. N 940 «Об утверждении Правил согласования проектов решений ассоциаций, союзов и иных объединений операторов об определении дополнительных угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности членами таких ассоциаций, союзов и иных объединений операторов, с Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю»

Обеспечение безопасности персональных данных при их обработке

Нормативно-правовое регулирование

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

Приказ ФСТЭК России от 11.02.2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»
«Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. ФСТЭК РФ 14.02.2008)

«Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (Выписка) (утв. ФСТЭК РФ 15.02.2008)

Специальные требования и рекомендации по технической защите конфиденциальной информации(СТР-К) (утв. решением Коллегии Гостехкомиссии России № 7.2/02.03.2001 г.)

Обеспечение безопасности персональных данных при их обработке

Нормативно-правовое регулирование

Приказ ФСБ России от 10.07.2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»

«Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности» (утв. ФСБ России 31.03.2015 N 149/7/2/6-432)

Постановление Правительства РФ от 1 ноября 2012 г. № 1119

Четыре типа ИСПДн в зависимости от категории ПДн (**абз. 1-4 ст. 5**):

1. **ИСПДн-С -** ИСПДн, обрабатывающая **специальные категории ПДн**, если в ней обрабатываются ПДн, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных.
2. **ИСПДн-Б** - ИСПДн, обрабатывающая **биометрические ПДн**, если в ней обрабатываются 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, и не обрабатываются сведения, относящиеся к специальным категориям персональных данных.
3. **ИСПДн-О** - ИСПДн, обрабатывающая **общедоступные ПДн**, если, если в ней обрабатываются персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей 8 Федерального закона «О персональных данных».
4. **ИСПДн-И** - ИСПДн, обрабатывающая **иные категории ПДн**.

Постановление Правительства РФ от 1 ноября 2012 г. № 1119

Каждая ИСПДн делится на **два подтипа** (**абз. 5 ст. 5**):

1) **ИСПДн-сотрудников**, обрабатывающей ПДн сотрудников оператора, если в ней обрабатываются ПДн только указанных сотрудников.
2) **ИСПДн- не сотрудников** (в остальных случаях), обрабатывающей ПДн субъектов ПДн, не являющихся сотрудниками оператора.

Вводится **три типа актуальных угроз безопасности ПДн -** совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия (ст. 5):

Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе **актуальны угрозы, связанные с наличием НДВ в системном ПО**, используемом в информационной системе.

Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе **актуальны угрозы**, **связанные с наличием НДВ в прикладном ПО**, используемом в информационной системе.

Угрозы 3-го типа актуальны для информационной системы, если для нее **актуальны угрозы**, **не связанные с наличием НДВ в системном ПО и прикладном ПО**, используемом в информационной системе.

Определение типа угроз безопасности ПДн, актуальных для ИСПДн, производится оператором с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18 Федерального закона «О персональных данных», и в соответствии с нормативными правовыми актами, принятыми во исполнение части 5 статьи 19 Федерального закона «О персональных данных» (**ст. 7**).

Постановление Правительства РФ от 1 ноября 2012 г. № 1119

При обработке ПДн в ИСПДн устанавливаются **4 уровня защищенности ПДн** (**УЗ**) (**ст. 8 – ст. 12**):

УЗ 1, УЗ 2, УЗ 3, УЗ 4.

УЗ 1 - максимальные требования к уровню защищенности,

УЗ 4 – минимальные требования к уровню защищенности.

Уровень защищенности ПДн при их обработке в ИСПДн **определяется в зависимости от** следующих параметров:

- типа ИСПДн (ИСПДн-С, ИСПДн-Б, ИСПДн-О),
- подтипа ИСПДн (ИСПДн-сотрудников, ИСПДн-не_сотрудников),
- количества субъектов (более 100 000, менее чем 100 000)
- типа актуальных угроз (1й, 2й, 3й).

Выбор средств защиты для СЗПДн **осуществляется оператором** в соответствии с нормативными правовыми актами ФСТЭК России и ФСБ России (**п. Г ст. 13**).

Постановление Правительства РФ от 1 ноября 2012 г. № 1119

Определение уровня защищенности ИСПДн

Тип ИСПДн	Категории субъектов	Количество субъектов	Тип актуальных угроз		
			1 тип	2 тип	3 тип
ИСПДн-С	Не сотрудников	Более 100 000	УЗ 1	УЗ 1	УЗ 2
		Менее чем 100 000	УЗ 1	УЗ 2	УЗ 3
	Сотрудников	Более 100 000	УЗ 1	УЗ 2	УЗ 3
		Менее чем 100 000	УЗ 1	УЗ 2	УЗ 3
ИСПДн-Б	Не сотрудников	Более 100 000	УЗ 1	УЗ 2	УЗ 3
		Менее чем 100 000	УЗ 1	УЗ 2	УЗ 3
	Сотрудников	Более 100 000	УЗ 1	УЗ 2	УЗ 3
		Менее чем 100 000	УЗ 1	УЗ 2	УЗ 3
ИСПДн-И	Не сотрудников	Более 100 000	УЗ 1	УЗ 2	УЗ 3
		Менее чем 100 000	УЗ 1	УЗ 3	УЗ 4
	Сотрудников	Более 100 000	УЗ 1	УЗ 3	УЗ 4
		Менее чем 100 000	УЗ 1	УЗ 3	УЗ 4
ИСПДн-О	Не сотрудников	Более 100 000	УЗ 2	УЗ 2	УЗ 4
		Менее чем 100 000	УЗ 2	УЗ 3	УЗ 4
	Сотрудников	Более 100 000	УЗ 2	УЗ 3	УЗ 4
		Менее чем 100 000	УЗ 2	УЗ 3	УЗ 4

Постановление Правительства РФ от 1 ноября 2012 г. № 1119

Общие требования по обеспечению уровня защищенности

Требования к защите ПДн в зависимости от уровня защиты	УЗ 4	УЗ 3	УЗ 2	УЗ 1
Технические средства защиты				
Применение СЗИ в соответствии с нормативно-правовыми актами, принятыми ФСТЭК и ФСБ России (**ст. 4**)	+	+	+	+
Использование СЗИ, прошедших процедуру оценки соответствия требованиям законодательства РФ в области обеспечения безопасности информации, в случае, **когда применение таких средств необходимо для нейтрализации актуальных угроз** (**пункт Г ст. 13**)	+	+	+	+
Организационные и другие технические меры				
Организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения (**пункт А ст. 13**)	+	+	+	+
Обеспечение сохранности носителей персональных данных (**пункт Б ст. 13**)	+	+	+	+
Утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к ПДн, обрабатываемым в ИС, необходим для выполнения ими служебных (трудовых) обязанностей (**пункт В ст. 13**)	+	+	+	+
Назначение должностного лица (работника), ответственного за обеспечение безопасности ПДн в информационной системе (**ст. 14**)	-	+	+	+
Обеспечение доступа к содержанию электронного журнала сообщений исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей (**ст. 15**)	-	-	+	+
Обеспечение автоматической регистрации в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к ПДн, содержащимся в информационной системе (**пункт А ст. 16**)	-	-	-	+
Создание структурного подразделения, ответственного за обеспечение безопасности ПДн в информационной системе, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности (**пункт Б ст. 16**)	-	-	-	+

Постановление Правительства РФ от 1 ноября 2012 г. № 1119

Выводы по Требованиям ПП № 1119 от 01.11.2012 г.:

Представлена классификация ИСПДн – утверждены четыре типа ИСПДн (+два подтипа в каждой).

Утверждены определения актуальности угроз (три типа – 1й, 2й, 3й) в зависимости от актуальности угрозы НДВ в СПО и ППО.

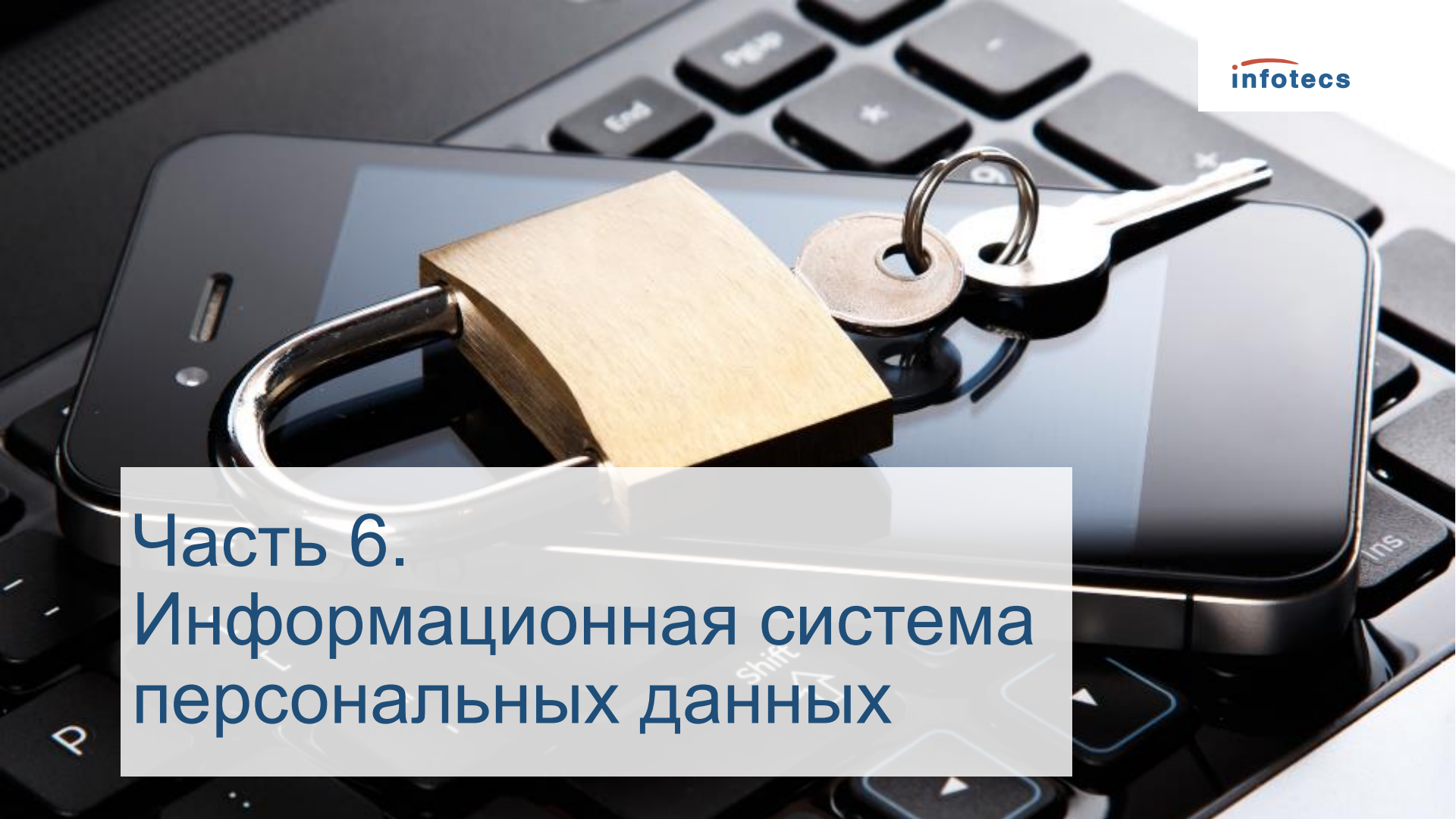
Утверждены 4 уровня защищенности ПДн при их обработке в ИСПДн (УЗ 1 - максимальные требования, УЗ 4 - минимальные).

Определена процедура выбора уровня защищенности ПДн при их обработке в ИСПДн (в зависимости от типа и подтипа ИСПДн, количества субъектов > 100 000 или <100 000, типа актуальных угроз).

Перечислены основные требования по обеспечению уровней защищенности ПДн в ИСПДн.

Контроль выполнения требований отдан в компетенцию Оператора или уполномоченного лица (не регулятора) (**ст. 17**).

Средства защиты ПДн определяет Оператор в соответствии с нормативно-правовыми актами, принятыми ФСТЭК России и ФСБ России.



Часть 6. Информационная система персональных данных

АЛГОРИТМ ФОРМИРОВАНИЯ ИСПДн

1. Определение области внедрения ИСПДн
Должны быть определены **объекты** (территории, офисы, филиалы, представительства), **структурные подразделения, автоматизированные системы** и **процессы**, в границах которых будут осуществляться мероприятия по реализации требований закона к порядку обработки персональных данных.

2. Назначение ответственных
Должно быть определено **структурное подразделение** или **должностное лицо**, ответственное за обеспечение безопасности ПДн.

3. Разработка и утверждение перечня персональных данных
Необходимо определить **состав обрабатываемых ПДн, цели и условия обработки, сроки хранения ПДн** различных категорий. Перечень обрабатываемых в ИСПДн персональных данных должен быть утверждён **приказом руководителя организации.**

4. Установление необходимого уровня правоотношений между оператором и субъектом персональных данных
Согласие субъекта на обработку его ПДн должно быть **при необходимости** получено, в том числе и в письменной форме. В целях обеспечения максимальной юридической чистоты в вопросах соблюдения прав субъектов персональных данных и во избежание инцидентов, связанных с нарушением этих прав, порядок реагирования на запросы со стороны субъектов персональных данных, внесения изменений в ПДн, а также условия прекращения обработки ПДн должны быть также **определены документально** в соответствующих приказах, инструкциях и процедурах, определяющих, в том числе, **степень участия должностных лиц в обработке ПДн** и **характер их взаимодействия между собой**.

АЛГОРИТМ ФОРМИРОВАНИЯ ИСПДн

5. Выделение и классификация ИСПДн
ИСПДн, подлежащие защите, должны быть **однозначно идентифицированы** как совокупности конкретных технических средств, размещенных внутри конкретных контролируемых зон и предназначенных для обработки конкретных категорий ПДн с конкретными целями. Должна быть проведена их **классификация**. На **каждую ИСПДн** должен быть оформлен **отдельный Акт классификации.**

6. Разработка модели угроз и требований к системе защиты
Разработка модели угроз входит в состав **мероприятий по обеспечению безопасности ПДн при их обработке в информационных системах**, предусмотрена **методическими документами ФСТЭК и ФСБ** в качестве обязательной меры для **специальных** ИСПДн. Модель угроз разрабатывается в соответствии с **методическими документами ФСТЭК и ФСБ**. При этом в зависимости от характеристик конкретной ИСПДн применяются **документы либо одного, либо обоих ведомств.** Требования по обеспечению безопасности ПДн разрабатываются на основе модели угроз с учётом **установленного класса ИСПДн** и включаются в техническое (частное техническое) задание на разработку СЗПДн.

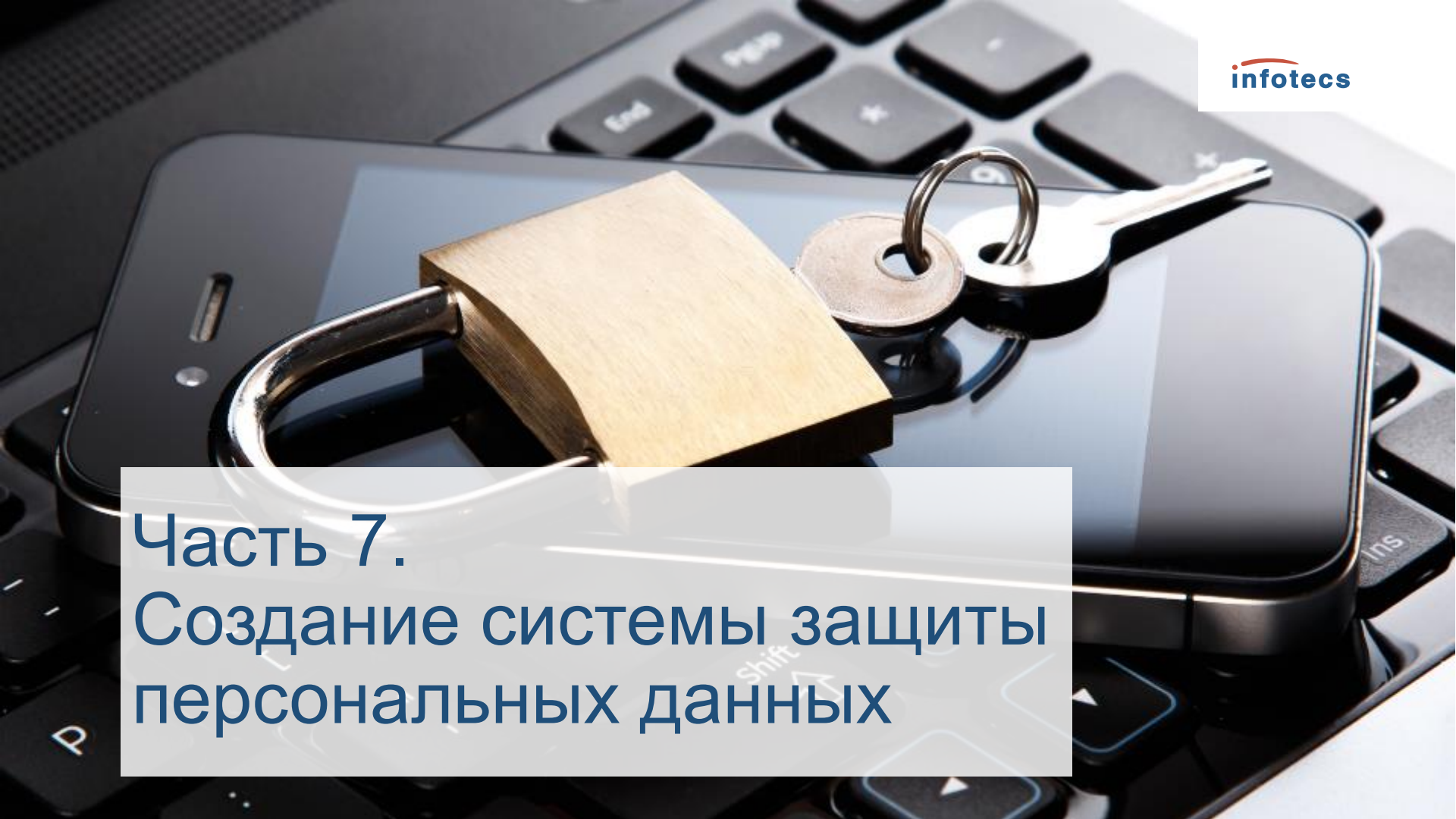
7. Проектирование и создание ИСПДн (СЗПДн)
В каждой информационной системе, предназначенной для обработки ПДн, должна быть **спроектирована и создана система защиты персональных данных**, соответствующая требованиям руководящих и нормативно-методических документов ФСТЭК и ФСБ по защите информации. Порядок проектирования определяется рядом **государственных стандартов и руководящих документов ФСТЭК России.**

АЛГОРИТМ ФОРМИРОВАНИЯ ИСПДн

8. Контроль над обеспечением уровня защищённости ПДн
Должно быть обеспечено выполнение **всех требований** по защите при эксплуатации СЗПДн. С этой целью в организации организовывается и проводится **периодический контроль** эффективности применяемых мер защиты, в том числе с применением специальных сертифицированных средств контроля.

9. Получение лицензий ФСТЭК и ФСБ (при необходимости)
В ряде **предусмотренных федеральным законодательством случаев** организация, осуществляющая деятельность, связанную с использованием **сертифицированных средств криптографической защиты информации**, либо деятельность в области **технической защиты конфиденциальной информации** должна получить соответствующие лицензии.

10. Выполнение прочих требований закона
ФЗ «О персональных данных» и подзаконными актами установлен ряд других норм и требований, которые могут иметь отношение **не ко всем операторам** и которые должны исполняться теми из них, для кого это является **производственной необходимостью**. Это и обработка биометрических персональных данных, и вопросы трансграничной передачи ПДн, и учёт особенностей обработки ПДн без использования средств автоматизации. При наличии таких оснований требуется выработка специальных мер, разработка процедур и издание **внутренних организационно-распорядительных документов**, регулирующих данные процессы.



Часть 7. Создание системы защиты персональных данных

СТАДИИ СОЗДАНИЯ СИСТЕМЫ ЗАЩИТЫ ПДн

Согласно СТР-К, «Специальные требования и рекомендации по технической защите конфиденциальной информации». Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282 (для служебного пользования) и **ГОСТ Р 51583-2014** «Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Основные положения»

Создание СЗПДн должно включать следующие стадии и этапы:

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

ПРЕДПРОЕКТНАЯ СТАДИЯ СОЗДАНИЯ СЗПДн

В ходе предпроектного обследования ИСПДн:

- определяется перечень ПДн, обрабатываемых в ИСПДн, и в них выделяется совокупность ПДн, подлежащих защите;
- определяются условия размещения технических средств ИСПДн относительно контролируемой зоны и доступа к ним;
- определяются конфигурация и топология ИСПДн, физические, функциональные и технологические связи как внутри ИСПДн, так и с другими системами;
- определяются технические средства и системы, составляющие ИСПДн, используемые общесистемные и прикладные программные средства;
- определяются режимы обработки ПДн в ИСПДн в целом и в отдельных компонентах;
- определяется класс ИСПДн;
- уточняется степень участия должностных лиц в обработке ПДн, характер их взаимодействия между собой;
- определяются (уточняются) угрозы безопасности ПДн применительно к конкретным условиям функционирования ИСПДн, разрабатывается модель угроз.

По результатам предпроектного обследования разрабатывается техническое (частное техническое) задание на разработку СЗПДн, в которое включаются конкретные требования по обеспечению безопасности ПДн при их обработке в ИСПДн.

СТАДИЯ ПРОЕКТИРОВАНИЯ И РЕАЛИЗАЦИИ СЗПДн

включает разработку СЗПДн в составе ИСПДн. На данной стадии в соответствии с требованиями ТЗ (ЧТЗ) на разработку СЗПДн:

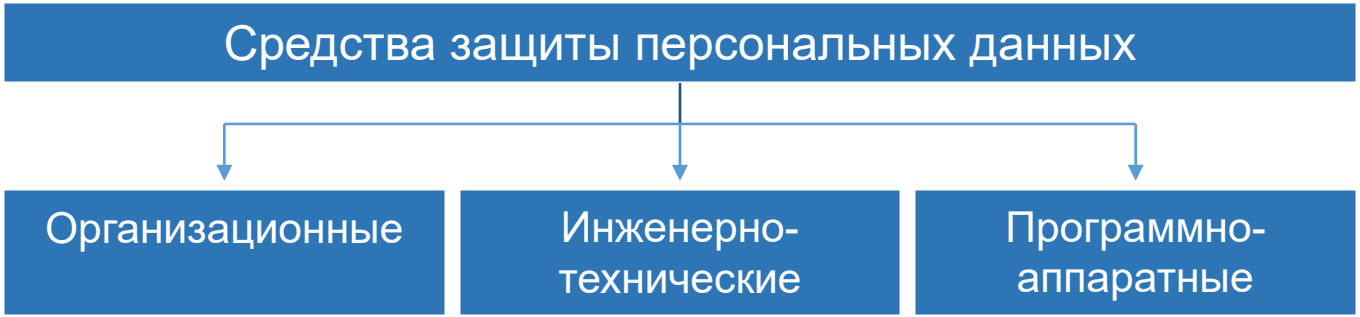
- разрабатывается задание на проведение работ, и выполняются работы в соответствии с проектной документацией;
- разрабатываются мероприятия по защите информации в соответствии с предъявляемыми требованиями;
- проводится обоснование состава и закупка технических средств защиты ИСПДн и сертифицированных средств защиты информации и их установка;
- разработка эксплуатационной и организационно-распорядительной документации на ИСПДн по обеспечению режима информационной безопасности при обработке ПДн и разрешительной системы доступа пользователей к обрабатываемой в ИСПДн информации;
- выполняются другие мероприятия, характерные для конкретных ИСПДн и направлений обеспечения безопасности ПДн.

СТАДИЯ ВВОДА В ДЕЙСТВИЕ СЗПДн

На стадии ввода в действие СЗПДн осуществляются:

- опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПДн;
- приемо-сдаточные испытания СЗПДн по результатам опытной эксплуатации;
- оценка соответствия ИСПДн требованиям по безопасности ПДн.

СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ В ИСПДн (СЗПДн)

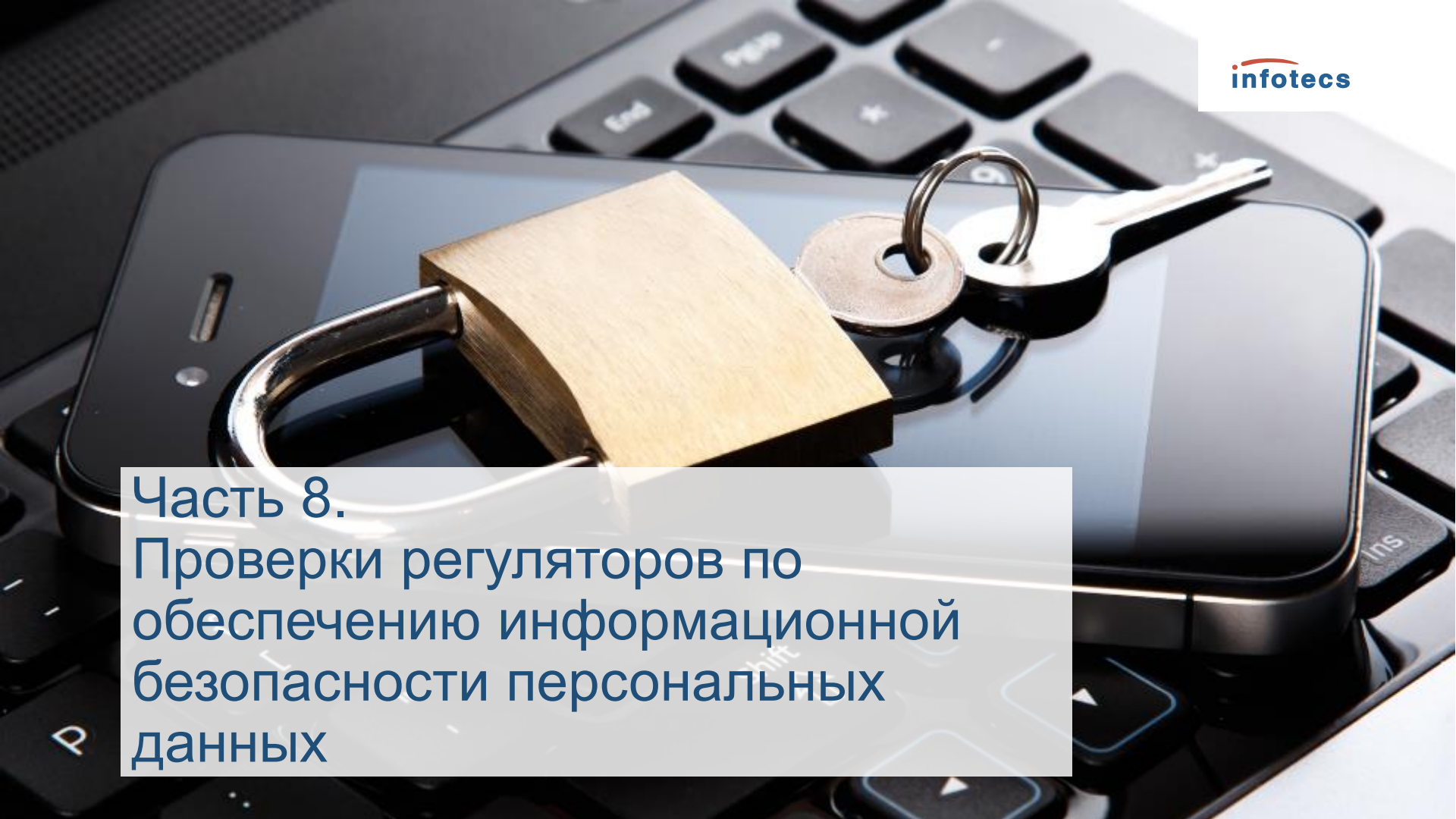


ОБЩИЕ ВЫВОДЫ ПО СОЗДАНИЮ И ПРОЕКТИРОВАНИЮ ИСПДн (СЗПДн)

Проектирование и создание СЗПДн должно осуществляться в соответствии с руководящими и нормативно-методическим документами регуляторов - ФСТЭК России и ФСБ России.

И прежде всего - ФСТЭК России, поскольку общие вопросы построения систем защиты регулируются именно этим органом. Именно научно-исследовательскими организациями ФСТЭК России разработаны соответствующие государственные стандарты для автоматизированных систем в защищённом исполнении.

Методические документы ФСБ России не содержат рекомендаций по порядку проектирования систем защиты и предназначены для применения лишь в случае использования СКЗИ для защиты ПДн.



Часть 8. Проверки регуляторов по обеспечению информационной безопасности персональных данных

Виды предусмотренных законодательством проверок

Роскомнадзор:

- по обращению субъекта персональных данных о соответствии содержания персональных данных и способов их обработки целям их обработки (федеральный закон № 152-ФЗ от 27.07.2006 «О персональных данных»)
- проверка сведений, содержащихся в уведомлении об обработке персональных данных (федеральный закон № 152-ФЗ от 27.07.2006 «О персональных данных»)
- внеплановые проверки по контролю нарушений обязательных требований (федеральный закон № 294-ФЗ от 26.12.2008 «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля»)

Виды предусмотренных законодательством проверок

ФСТЭК России:

- надзор за деятельностью лицензиата ФСТЭК России (постановление Правительства РФ от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации»)
- по обращению Роскомнадзора (федеральный закон № 152-ФЗ от 27.07.2006 «О персональных данных»)
- внеплановые проверки по контролю нарушений обязательных требований (федеральный закон № 294-ФЗ от 26.12.2008 «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля»)

Виды предусмотренных законодательством проверок

ФСБ России:

- контроль за соблюдением правил пользования средств криптографической защиты информации (приказ ФСБ России № 66 от 09.02.2005 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации – (Положение ПКЗ-2005))

- надзор за деятельностью лицензиата ФСБ России (постановление Правительства РФ от 29.12.2007 № 957 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами»)

- по обращению Роскомнадзора (федеральный закон № 152-ФЗ от 27.07.2006 «О персональных данных»)

- внеплановые проверки по контролю нарушений обязательных требований (федеральный закон № 294-ФЗ от 26.12.2008 г. «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля»)

ОТВЕТСТВЕННОСТЬ ЗА НЕВЫПОЛНЕНИЕ ЗАКОННЫХ ТРЕБОВАНИЙ ОРГАНОВ КОНТРОЛЯ

КоАП Статья 19.5. Невыполнение в срок законного предписания (постановления, представления, решения) органа (должностного лица), осуществляющего государственный надзор (контроль)
1. Невыполнение в установленный срок законного предписания (постановления, представления, решения) органа (должностного лица), осуществляющего государственный надзор (контроль), об устранении нарушений законодательства - влечет наложение административного штрафа:

- на граждан в размере от **трехсот до пятисот** рублей;
- на должностных лиц - от **одной тысячи до двух тысяч** рублей или **дисквалификацию** на срок **до трех лет**;
- на юридических лиц - от **десяти тысяч до двадцати тысяч** рублей.

2. Невыполнение в установленный срок законного предписания, решения органа, уполномоченного в области экспортного контроля, его территориального органа - влечет наложение административного штрафа:

- на должностных лиц в размере от **пяти тысяч до десяти тысяч** рублей или **дисквалификацию** на срок **до трех лет**;
- на юридических лиц - от **двухсот тысяч до пятисот тысяч** рублей.

Спасибо за внимание!

Олег Кузьмин
менеджер проектов НОЧУ ДПО ЦПК
«Учебный центр «ИнфоТеКС»

ОАО «ИнфоТеКС», Москва
(495) 737-61-92
www.infotecs.ru
НОЧУ ДПО ЦПК «Учебный центр «ИнфоТеКС»
education@infotecs.ru