Применение шифрования в качестве метода обезличивания персональных данных

Алексей Лукацкий
Бизнес-консультант по безопасности

22 марта 2017

Содержание

- В чем проблема?
- ФЗ-242 и неуёмное желание регулятора запретить все
- Что такое обезличивание?
- Как реализовать обезличивание?
- Может ли шифрование быть методом обезличивания?
- Что на эту тему думают в мире?
- Должно ли быть шифрование сертифицированным?

cisco

В чем проблема?

Как потребитель	Как поставщик/производитель
• Покупаете на Amazon • Посещаете EuroCrypt • Используете Gmail • Являетесь пользователем Facebook • Используете WhatsUp • Применяете iCloud • Арендуете автомобили в Hertz	• Пользуетесь Amazon AWS, Google.Docs • Имеете дочерние предприятия за пределами РФ, в том числе в ЕАЭС • Применяете общедоступные сервисы Web-аутентификации • Проводите конференцию в Белоруссии

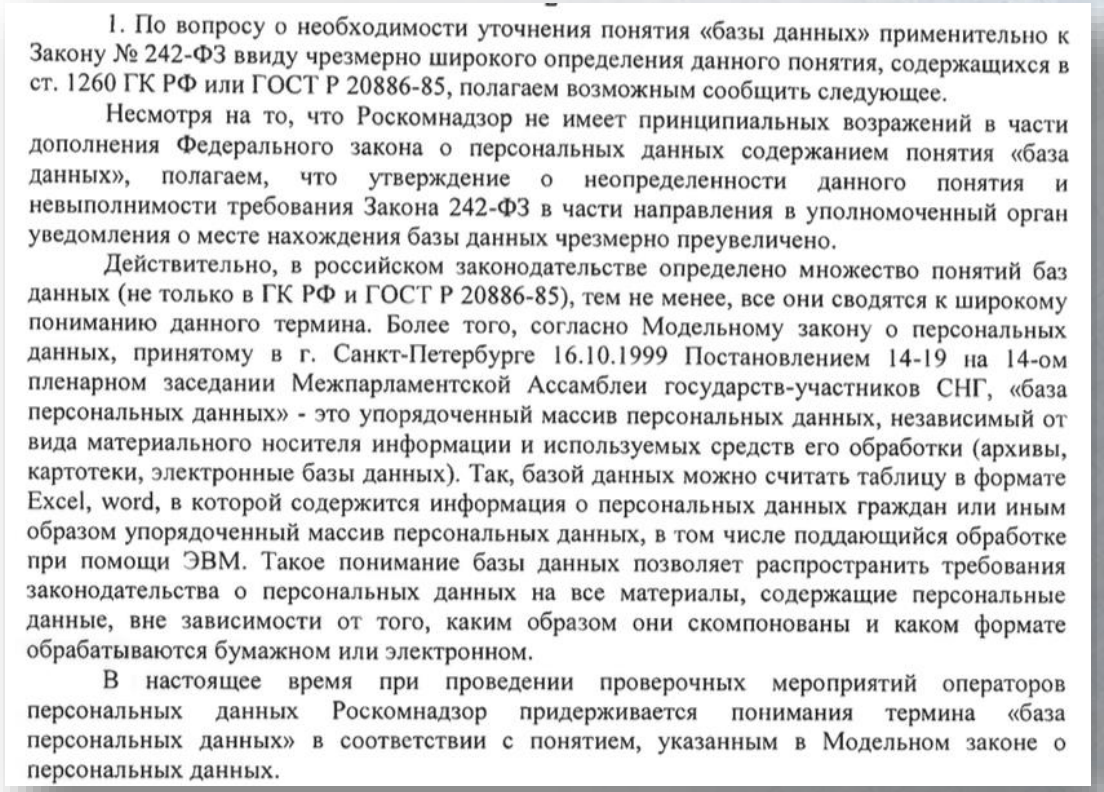
Что из этого следует?

- Реализация положений ФЗ-242 «о запрете хранения ПДн россиян за границей»
  - Базы ПДн, в которых происходит первичная регистрация и актуализация ПДн россиян, должны находится на территории РФ
  - Хотя слова «только» в законе нет, по сути вводится запрет хранения за пределами РФ
  - Наказание за нарушение
  - Выведение РКН из под действия 294-ФЗ
- Вступил в силу с 1 сентября 2015 года
- Первые нарушители уже заблокированы
  - Реальные нарушители, незаконно распространяющие ПДн с зарубежных сайтов

cisco

Разъяснение Роскомнадзора: что такое база данных?

- База данных - это упорядоченный массив данных, независимый от вида материального носителя информации и используемых средств его обработки (архивы, картотеки, электронные базы данных)
  - Таблицы в Excel, Word



1. По вопросу о необходимости уточнения понятия «базы данных» применительно к Закону № 242-ФЗ ввиду чрезмерно широкого определения данного понятия, содержащихся в ст. 1260 ГК РФ или ГОСТ Р 20886-85, полагаем возможным сообщить следующее.

Несмотря на то, что Роскомнадзор не имеет принципиальных возражений в части дополнения Федерального закона о персональных данных содержанием понятия «база данных», полагаем, что утверждение о неопределенности данного понятия и невыполнимости требования Закона 242-ФЗ в части направления в уполномоченный орган уведомления о месте нахождения базы данных чрезмерно преувеличено.

Действительно, в российском законодательстве определено множество понятий баз данных (не только в ГК РФ и ГОСТ Р 20886-85), тем не менее, все они сводятся к широкому пониманию данного термина. Более того, согласно Модельному закону о персональных данных, принятому в г. Санкт-Петербурге 16.10.1999 Постановлением 14-19 на 14-ом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ, «база персональных данных» - это упорядоченный массив персональных данных, независимый от вида материального носителя информации и используемых средств его обработки (архивы, картотеки, электронные базы данных). Так, базой данных можно считать таблицу в формате Excel, word, в которой содержится информация о персональных данных граждан или иным образом упорядоченный массив персональных данных, в том числе поддающийся обработке при помощи ЭВМ. Такое понимание базы данных позволяет распространить требования законодательства о персональных данных на все материалы, содержащие персональные данные, вне зависимости от того, каким образом они скомпонованы и каком формате обрабатываются бумажном или электронном.

В настоящее время при проведении проверочных мероприятий операторов персональных данных Роскомнадзор придерживается понимания термина «база персональных данных» в соответствии с понятием, указанным в Модельном законе о персональных данных.

Разъяснение Роскомнадзора: запрет зеркал и гражданство ПДн

Логический процесс, связанный с формированием и актуализацией базы данных, не позволяет осуществлять отдельные процедуры указанные в рассматриваемой норме, в том числе «хранение персональных данных» в базах данных на территории иностранного государства не нарушая при этом нормы Закона 242-ФЗ.

Так, каждый случай, в котором при сборе данных будет осуществляться одновременное хранение базы данных на территории России и иностранного государства будет являться нарушением Закона 242-ФЗ, поскольку оператор при сборе персональных данных допустит их хранение в базе данных за пределами России. В том числе после сбора данных, то есть после формирования базы данных на территории России, недопустимо изменение условий ее хранения путем переноса базы данных на территорию иностранного государства.

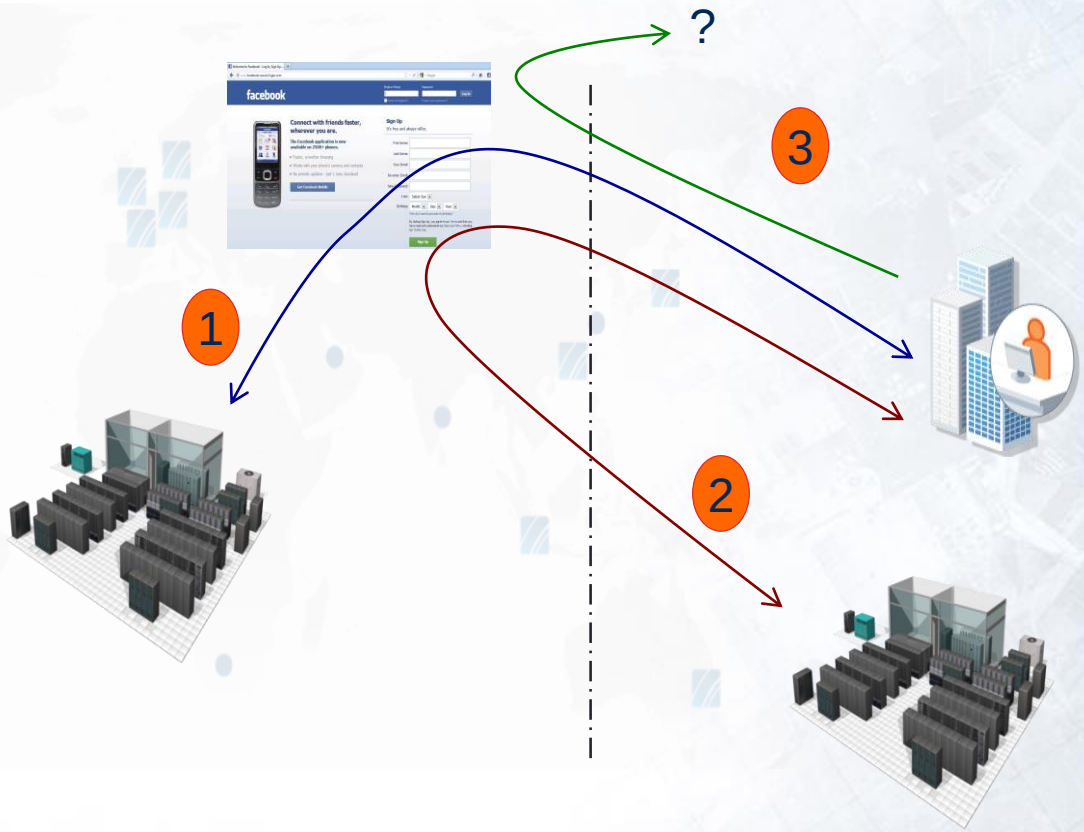
5. Относительно вопроса, о необходимости дополнительной регламентации процедуры установления гражданства субъекта персональных данных, в целях исполнения требований Закон № 242-ФЗ, полагаем возможным сообщить следующее.

Законодатель предоставил возможность операторам персональных данных самостоятельно определять указанную процедуру в соответствии со спецификой деятельности каждого юридического лица, осуществляющего сбор персональных данных граждан России. В связи с чем, полагаем, что дополнительного законодательного регулирования данный вопрос не требует.

Вместе с тем, в случае, если оператору персональных данных крайне затруднительно выделить среди множества субъектов персональных данных, тех в отношении кого необходимо осуществлять хранение данных на территории России, возможно применение принципа действия Закона на всей территории России. Так, в случае сбора данных на территории России, оператор персональных данных может осуществлять их хранение в базах данных, размещенных на технических средствах в Российской Федерации, вне зависимости от гражданства субъектов персональных данных.

Кого ФЗ-242 касается в первую очередь?

- Все иностранные компании, работающие в России
- Все иностранные компании, работающие для российских граждан
  - В том числе облачные сервисы и арендуемые за рубежом ЦОДы
- Все российские компании, работающие за рубежом
- Но только на операторов ПДн



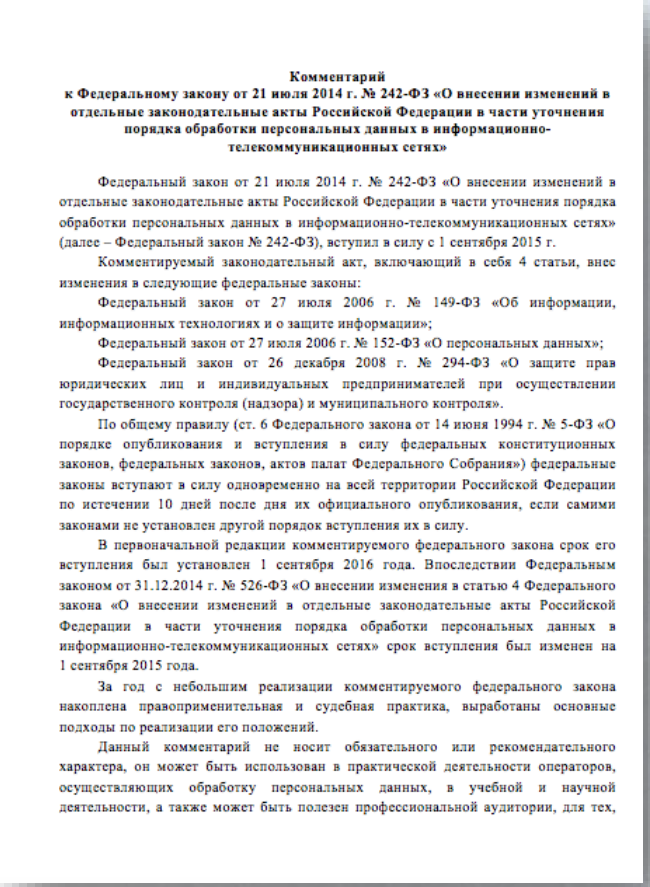
cisco

Потенциальные последствия за неисполнение ФЗ-242

- Блокирование доступа к зарубежным ресурсам, в которых ведется обработка ПДн российских граждан (сотрудников и клиентов)
- Блокирование доступа к зарубежным ресурсам и третьих фирм, в которых ведется обработка ПДн российских граждан (сотрудников и клиентов)
- Потенциальное снижение продаж решений и невозможность выполнения сервисных обязательств из-за потенциального блокирования основного сайта
- Репутационные риски
- Административная и уголовная ответственность отсутствует
  - Однако есть ответственность за невыполнение предписания РКН по результатам надзорных мероприятий

Юрисдикций для РКН не существует

- ФЗ-242 «распространяет свое действие на лиц (операторов персональных данных), осуществляющих свою деятельность на территории Российской Федерации, то есть распространяется как на российские компании, так и на иностранные»
- «Закон определил необходимость исполнения нормы о локализации данных иностранными компаниями, в том числе которые осуществляют деятельность на территории России без образования официальных представительств или иных форм юридических лиц»



Комментарий
к Федеральному закону от 21 июля 2014 г. № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях»

Федеральный закон от 21 июля 2014 г. № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях» (далее – Федеральный закон № 242-ФЗ), вступил в силу с 1 сентября 2015 г.

Комментируемый законодательный акт, включающий в себя 4 статьи, внес изменения в следующие федеральные законы:

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

Федеральный закон от 26 декабря 2008 г. № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля».

По общему правилу (ст. 6 Федерального закона от 14 июня 1994 г. № 5-ФЗ «О порядке опубликования и вступления в силу федеральных конституционных законов, федеральных законов, актов палат Федерального Собрания») федеральные законы вступают в силу одновременно на всей территории Российской Федерации по истечении 10 дней после дня их официального опубликования, если самими законами не установлен другой порядок вступления их в силу.

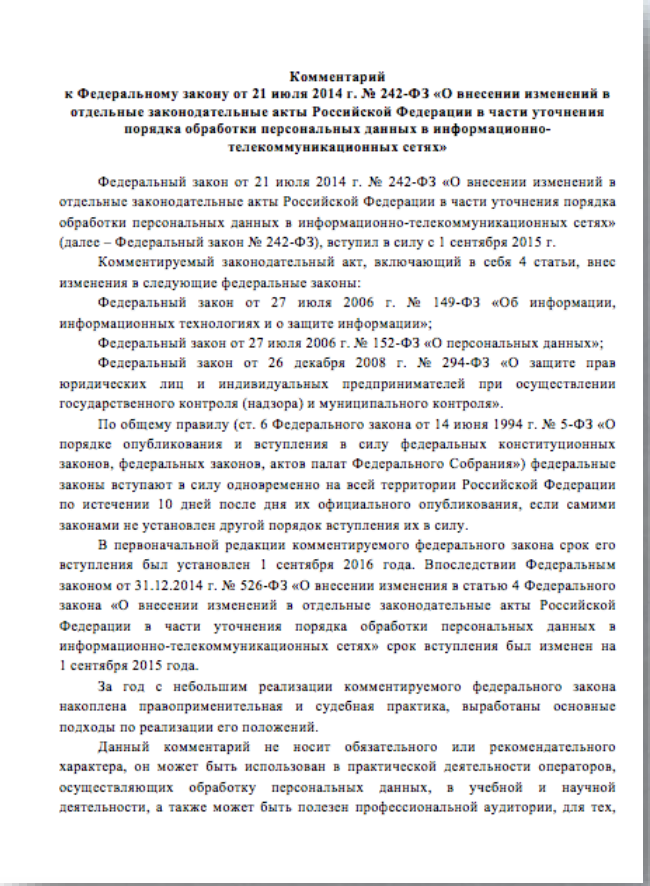
В первоначальной редакции комментируемого федерального закона срок его вступления был установлен 1 сентября 2016 года. Впоследствии Федеральным законом от 31.12.2014 г. № 526-ФЗ «О внесении изменения в статью 4 Федерального закона «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях» срок вступления был изменен на 1 сентября 2015 года.

За год с небольшим реализации комментируемого федерального закона накоплена правоприменительная и судебная практика, выработаны основные подходы по реализации его положений.

Данный комментарий не носит обязательного или рекомендательного характера, он может быть использован в практической деятельности операторов, осуществляющих обработку персональных данных, в учебной и научной деятельности, а также может быть полезен профессиональной аудитории, для тех,

Юрисдикций для РКН не существует

- Если Интернет-сайт
  - Использует домен .ru, .su, .рф
  - Имеет русскоязычную версию (даже с помощью плагина Google.Translate)
  - Исполняет договор на территории РФ (доставка товара, оказание услуги или пользование цифровым контентом)
- то сайт должен отвечать нормам ФЗ-242
- Обработка общедоступных ПДн не является исключением для выполнения ФЗ-242



Комментарий
к Федеральному закону от 21 июля 2014 г. № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях»

Федеральный закон от 21 июля 2014 г. № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях» (далее – Федеральный закон № 242-ФЗ), вступил в силу с 1 сентября 2015 г.

Комментируемый законодательный акт, включающий в себя 4 статьи, внес изменения в следующие федеральные законы:

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

Федеральный закон от 26 декабря 2008 г. № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля».

По общему правилу (ст. 6 Федерального закона от 14 июня 1994 г. № 5-ФЗ «О порядке опубликования и вступления в силу федеральных конституционных законов, федеральных законов, актов палат Федерального Собрания») федеральные законы вступают в силу одновременно на всей территории Российской Федерации по истечении 10 дней после дня их официального опубликования, если самими законами не установлен другой порядок вступления их в силу.

В первоначальной редакции комментируемого федерального закона срок его вступления был установлен 1 сентября 2016 года. Впоследствии Федеральным законом от 31.12.2014 г. № 526-ФЗ «О внесении изменения в статью 4 Федерального закона «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях» срок вступления был изменен на 1 сентября 2015 года.

За год с небольшим реализации комментируемого федерального закона накоплена правоприменительная и судебная практика, выработаны основные подходы по реализации его положений.

Данный комментарий не носит обязательного или рекомендательного характера, он может быть использован в практической деятельности операторов, осуществляющих обработку персональных данных, в учебной и научной деятельности, а также может быть полезен профессиональной аудитории, для тех,

cisco

Новая трактовка понятия «персональные данные»

- Под контроль попадают данные, которые сами по себе, без дополнительной информации, не могут быть соотнесены с конкретным субъектом
  - Сведения об активности анонимного пользователя в сети, IP- и MAC-адреса, файлы cookies, особенности поведения в интернете, геолокационные данные и т.п.
  - Эти сведения названы Большими пользовательскими данными (законопроект по ним уже пишется)
- Наличие «счетчиков» Google Analytics, Webtrends, Яндекс.Метрика требует по мнению РКН согласия на обработку ими персональных данных

LinkedIn

cisco

Как бороться с этим бредом?

Что такое обезличивание ПДн?

- Обезличивание - действия, в результате которых невозможно без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн
  - ст.3 ФЗ-152 «О персональных данных»
  - Обезличивание приводит к тому, что персональные данные перестают быть персональными и требования ФЗ к ним уже неприменимы

cisco

Позиция регулятора (РКН)

области, поясняем:

Вопрос 1. При анализе персональных данных обрабатываемых в организации возник следующий вопрос.

Из определений ст. 3 152-ФЗ «О персональных данных» следует, что:

а) 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, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

б) обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;

Можно ли на основании данных определений сделать вывод, что при обезличивании персональных данных эти данные перестают быть персональными, поскольку нельзя установить их принадлежность к субъекту и в этом случае вопросы, связанные с обработкой таких данных выходят за сферу действия 152-ФЗ?

Ответ: В соответствии со ст. 7 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» операторы и третьи лица, получающие доступ к персональным данным, должны обеспечивать их конфиденциальность. В данном Законе также разъясняется, что конфиденциальность персональных данных представляет собой обязательное требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

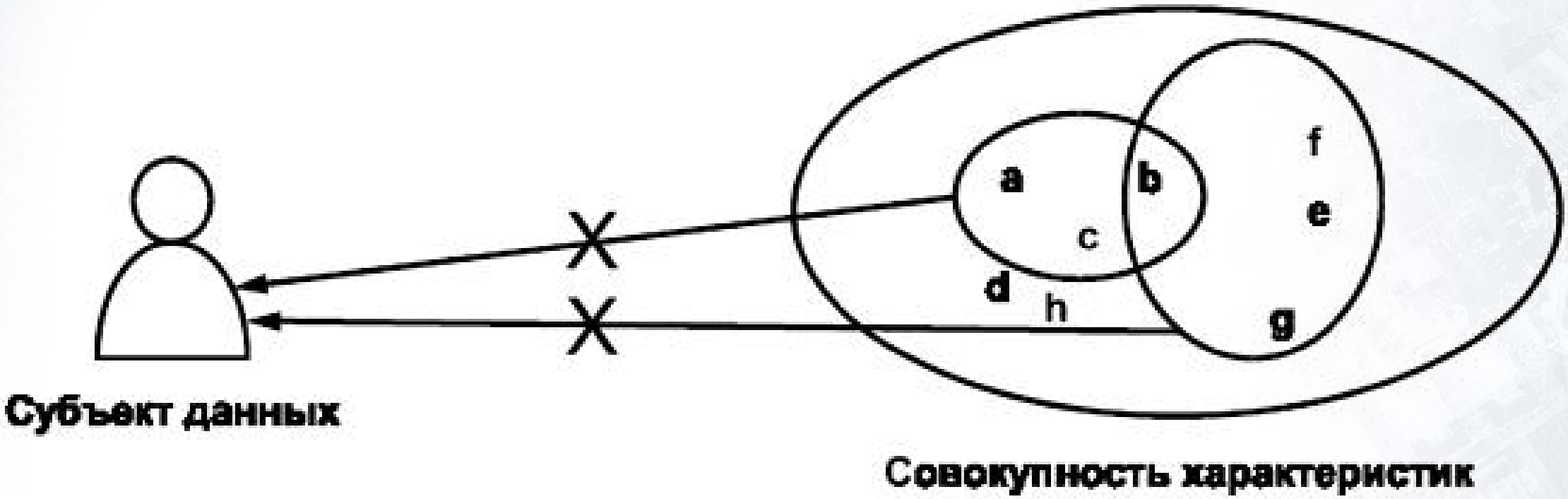
Не требуется обеспечивать конфиденциальность персональных данных:

- В случае обезличивания персональных данных. Под обезличиванием персональных данных понимаются действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту.

Следовательно, при обезличивании персональных данных, эти данные перестают быть персональными, поскольку нельзя установить их принадлежность к субъекту персональных данных, в этом случае, вопросы, связанные с обработкой обезличенных персональных данных, выходят за сферу действия Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

Вопрос 2. При выделении информационных систем персональных данных и классификации

Как обеспечить обезличивание?



Два основных метода обезличивания

- Обезличивание представляет собой процесс удаления связи между идентифицирующей совокупностью характеристик и субъектом данных
- Оно может быть осуществлено двумя разными способами
  - с помощью удаления или преобразования характеристик, при котором связь между характеристиками и субъектом данных либо прекращается, либо перестает быть уникальной и указывает на несколько субъектов данных
  - путем увеличения популяции субъектов данных, при котором связь между совокупностью характеристик и субъектом данных перестает быть уникальной

Методы обезличивания по NIST SP800-122

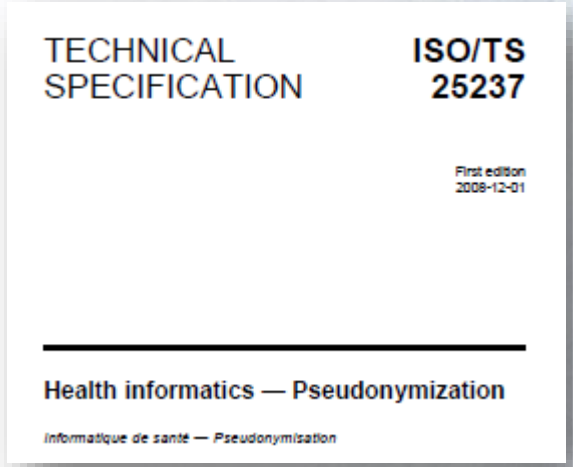
- Абстрагирование ПДн – сделать их менее точными
  - Например, путем группирования общих или непрерывных характеристик
- Скрытие ПДн – удалить всю или часть записи ПДн
  - ПДн не должны быть избыточными по отношению к цели
- Внесение шума в ПДн – добавить небольшое количество посторонней информации в ПДн
- Замена ПДн – переставить поля одной записи ПДн с теми же самыми полями другой аналогичной записи
- Замена данных средним значением – заменить выбранные данные средним значением для группы ПДн

Методы обезличивания по NIST SP800-122

- Разделение ПДн на части – использование таблиц перекрестных ссылок
  - Например, две таблицы – одна с ФИО и идентификатором субъекта ПДн, вторая – с тем же идентификатором субъекта ПДн и остальной частью ПДн
- Использование специальных алгоритмов
  - Например, маскирование ПДн или подмена отдельных символов другими
  - Идеальным вариантом является использование алгоритмов криптографического преобразования (шифрование или хеширование)

Обезличивание по стандартам ISO

- Стандарт ISO 25237-2008: Health informatics – Pseudonymization
- Псевдонимизация – специфичный тип обезличивания, который удаляет ассоциацию с субъектом ПДн и добавляет ассоциацию между набором особенностей, касающихся субъекта ПДн и одним или более псевдонимами


TECHNICAL SPECIFICATION

ISO/TS 25237

First edition 2008-12-01

Health informatics — Pseudonymization

Informatique de santé — Pseudonymisation

Обезличивание по ГОСТу

- Стандарт ГОСТ Р 55036-2012 «Информатизация здоровья. Псевдонимизация»
- Обезличивание - действия, в результате которых удаляется связь между совокупностью идентифицирующих данных и субъектом данных
- Псевдонимизация - особый случай обезличивания, при котором помимо удаления прямой связи с субъектом данных создается связь между конкретной совокупностью характеристик этого субъекта и одним или несколькими псевдонимами

ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 55036 — 2012 ISO/TS 25237:2008

Информатизация здоровья

ПСЕВДОНИМИЗАЦИЯ

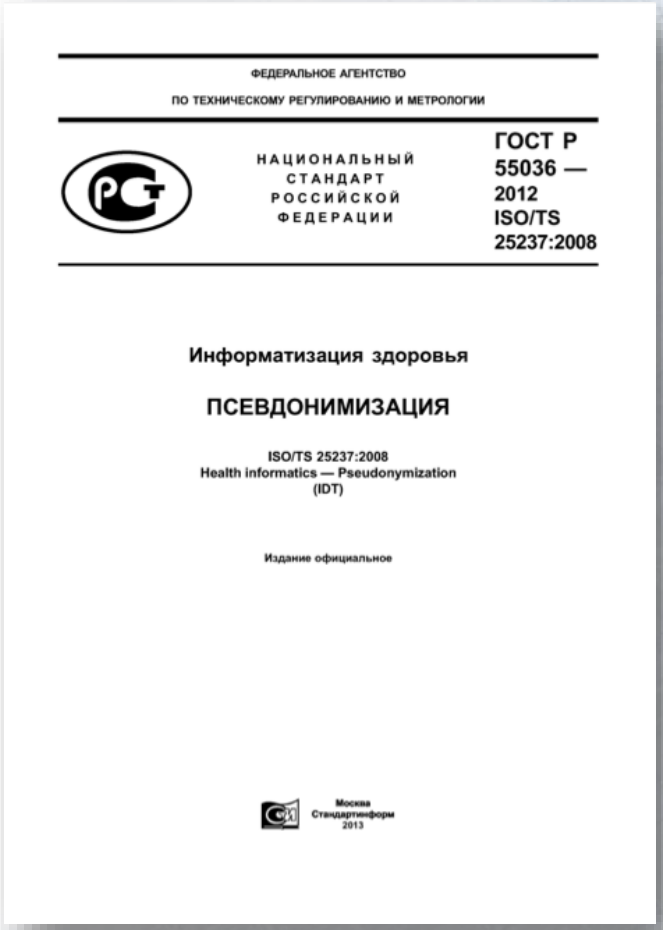
ISO/TS 25237:2008
Health informatics — Pseudonymization
(IDT)

Издание официальное

Москва
Стандартинформ
2013

Обезличивание по ГОСТу

- В защите персональных данных выделяются две задачи
  - первая - защита оперативного доступа к персональным данным (например, в веб-приложениях),
  - вторая - защита персональных данных, хранящихся в базах данных
- Стандарт ГОСТ Р 55036-2012 «Информатизация здоровья. Псевдонимизация» посвящен последней задаче


ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 55036 — 2012 ISO/TS 25237:2008

Информатизация здоровья

ПСЕВДОНИМИЗАЦИЯ

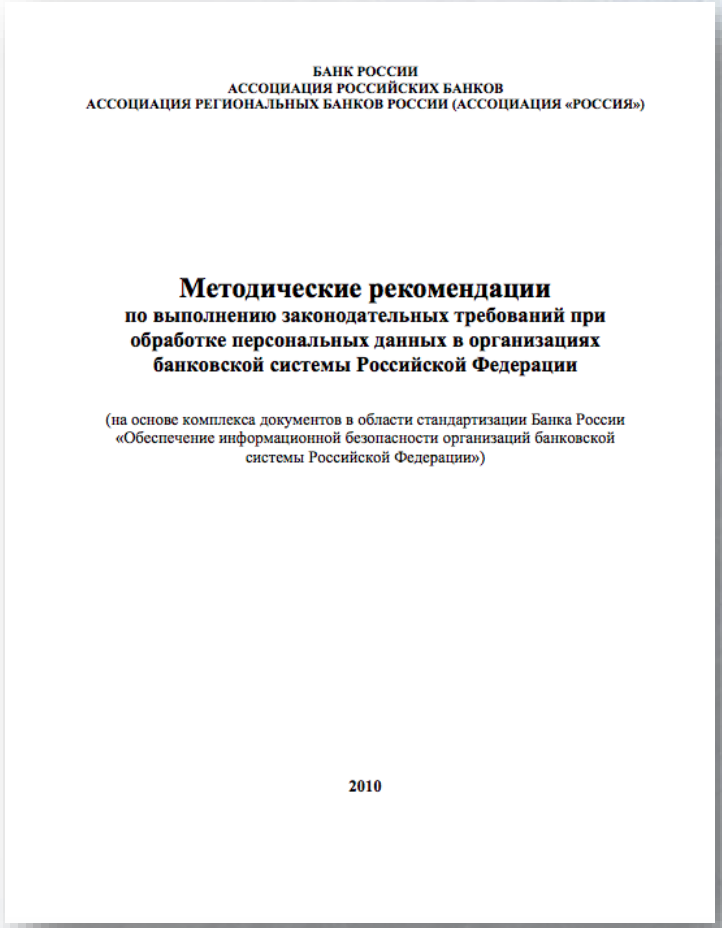
ISO/TS 25237:2008
Health informatics — Pseudonymization
(IDT)

Издание официальное

Москва
Стандартинформ
2013

Рекомендации ЦБ по обезличиванию

- Методические рекомендации разработаны Ассоциацией российских банков и Ассоциацией региональных банков России (Ассоциацией «Россия») совместно с Банком России для обеспечения методической поддержки применения организациями БС РФ Комплекса БР ИББС



БАНК РОССИИ
АССОЦИАЦИЯ РОССИЙСКИХ БАНКОВ
АССОЦИАЦИЯ РЕГИОНАЛЬНЫХ БАНКОВ РОССИИ (АССОЦИАЦИЯ «РОССИЯ»)

Методические рекомендации
по выполнению законодательных требований при обработке персональных данных в организациях банковской системы Российской Федерации

(на основе комплекса документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации»)

2010

Рекомендации ЦБ по обезличиванию

- Персональные данные, обрабатываемые в ИСПДн, можно обезличить с целью понижения уровня требований по обеспечению безопасности
- Полностью обезличить все персональные данные невозможно – в информационных системах всегда будут присутствовать технические средства, на которых будет происходить процесс, обратный обезличиванию

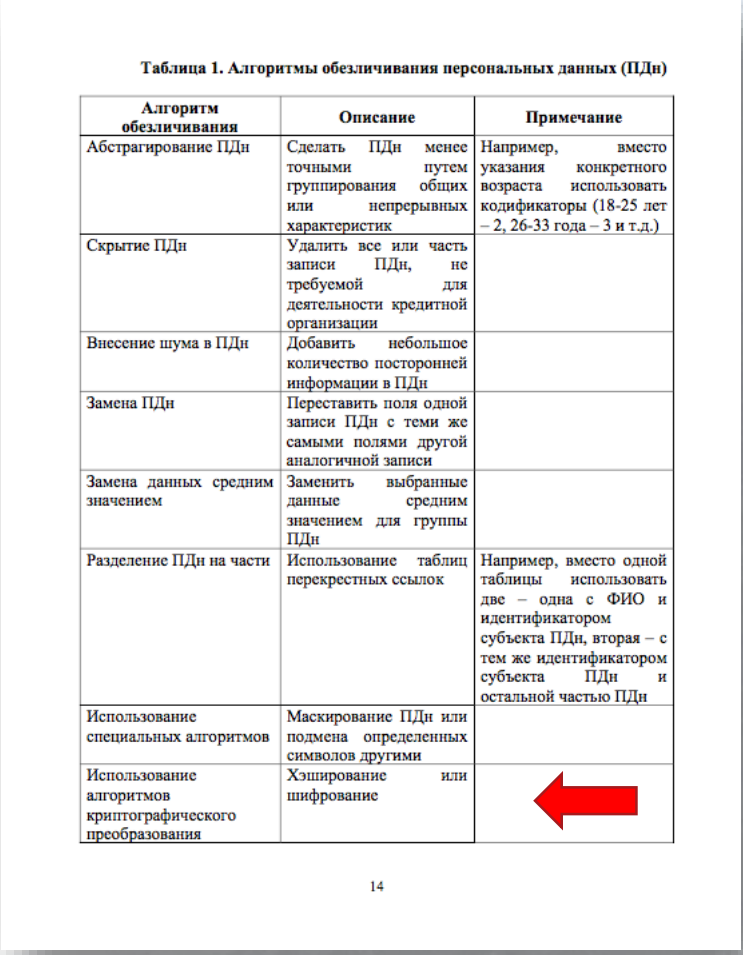


Таблица 1. Алгоритмы обезличивания персональных данных (ПДн)

Алгоритм обезличивания	Описание	Примечание
Абстрагирование ПДн	Сделать ПДн менее точными путем группирования общих или непрерывных характеристик	Например, вместо указания конкретного возраста использовать кодификаторы (18-25 лет – 2, 26-33 года – 3 и т.д.)
Скрытие ПДн	Удалить все или часть записи ПДн, не требуемой для деятельности кредитной организации	
Внесение шума в ПДн	Добавить небольшое количество посторонней информации в ПДн	
Замена ПДн	Переставить поля одной записи ПДн с теми же самыми полями другой аналогичной записи	
Замена данных средним значением	Заменить выбранные данные средним значением для группы ПДн	
Разделение ПДн на части	Использование таблиц перекрестных ссылок	Например, вместо одной таблицы использовать две – одна с ФИО и идентификатором субъекта ПДн, вторая – с тем же идентификатором субъекта ПДн и остальной частью ПДн
Использование специальных алгоритмов	Маскирование ПДн или подмена определенных символов другими	
Использование алгоритмов криптографического преобразования	Хэширование или шифрование	

14

NIST, ISO, ГОСТ и рекомендации Банка России допускают применение криптографии как метода обезличивания

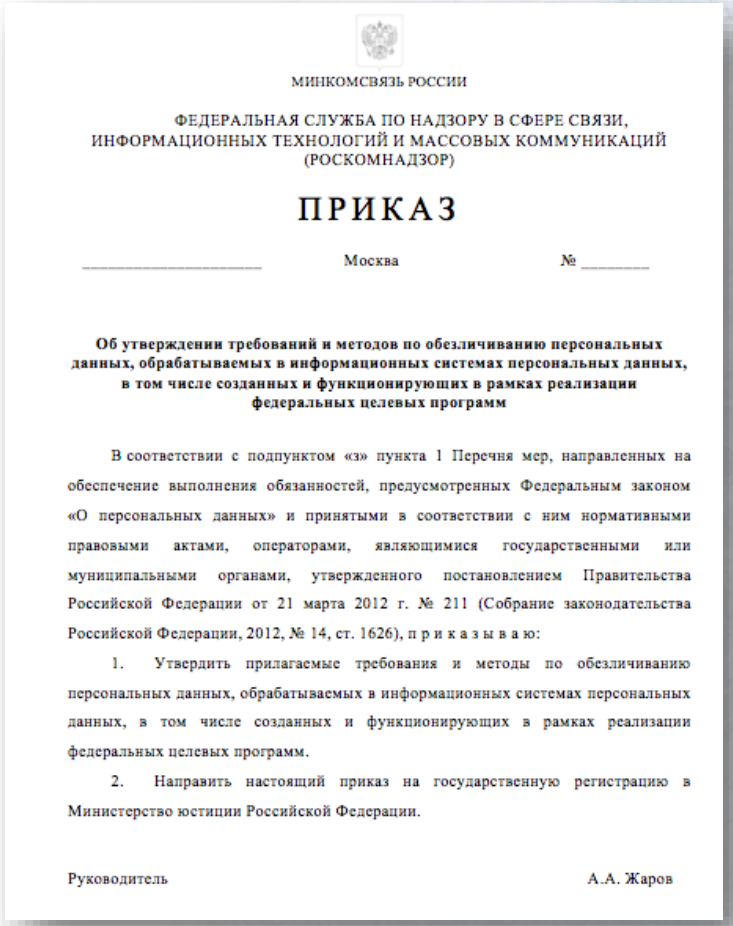
Криптография как метод обезличивания

- Обезличивание на основе криптографических алгоритмов использует цепочку базовых криптографических и сопутствующих алгоритмов
  - Хеширование
  - Генерацию случайных чисел
  - Генерацию ключей
  - Шифрование
  - Базовые функции логического преобразования битовых строк

Требований к криптографическим алгоритмам, стойкости и сертификации не предъявляется

Что думает основной регулятор про обезличивание?

- Приказ от 5.09.2013 №996
- Разработан во исполнение Постановления Правительства от 21.03.2012 №211
- Носит рекомендательный характер
- Не требует необратимости ПДн



МИНКОМСВЯЗЬ РОССИИ

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

ПРИКАЗ

_____ Москва № _____

Об утверждении требований и методов по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ

В соответствии с подпунктом «з» пункта 1 Перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами, утвержденного постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211 (Собрание законодательства Российской Федерации, 2012, № 14, ст. 1626), п р и к а з ы в а ю:

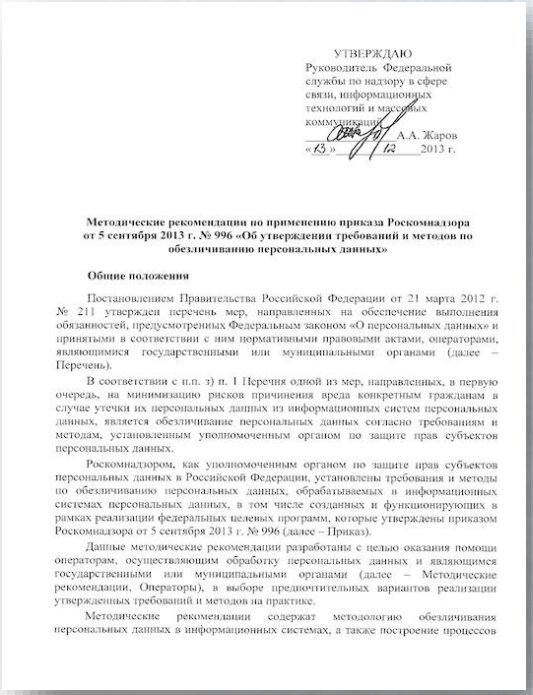
1. Утвердить прилагаемые требования и методы по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ.

2. Направить настоящий приказ на государственную регистрацию в Министерство юстиции Российской Федерации.

Руководитель А.А. Жаров

Методические рекомендации РКН по обезличиванию

- Методические рекомендации по применению приказа по обезличиванию
- Предлагают для разных сценариев обработки ПДн альтернативы, описывают их преимущества и недостатки, дают примеры применения
- Приведена таблица соответствия методов обезличивания свойствам обезличенных данных, рассмотрены вопросы организации обработки обезличенных данных, даны правила и рекомендации по работе с обезличенными данными



УТВЕРЖДАЮ
Руководитель Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций
А.А. Жаров
«13» 12 2013 г.

Методические рекомендации по применению приказа Роскомнадзора от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»

Общие положения

Постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211 утвержден перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами (далее – Перечень).

В соответствии с п.п. з) п. 1 Перечня одной из мер, направленных, в первую очередь, на минимизацию рисков причинения вреда конкретным гражданам в случае утечки их персональных данных из информационных систем персональных данных, является обезличивание персональных данных согласно требованиям и методам, установленным уполномоченным органом по защите прав субъектов персональных данных.

Роскомнадзором, как уполномоченным органом по защите прав субъектов персональных данных в Российской Федерации, установлены требования и методы по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ, которые утверждены приказом Роскомнадзора от 5 сентября 2013 г. № 996 (далее – Приказ).

Данные методические рекомендации разработаны с целью оказания помощи операторам, осуществляющим обработку персональных данных и являющимся государственными или муниципальными органами (далее – Методические рекомендации, Операторы), в выборе предпочтительных вариантов реализации утвержденных требований и методов на практике.

Методические рекомендации содержат методологию обезличивания персональных данных в информационных системах, а также построение процессов

Приказ РКН по обезличиванию

- Определяет свойства обезличенных ПДн, свойства методов обезличивания, требования к свойствам обезличенных данных, требования к методам обезличивания
- Не устанавливает жестких требований к используемым методам, но при этом рекомендует 4 метода
  - Метод введения идентификаторов
  - Метод изменения состава или семантики ПДн путем замены результатами статистической обработки, обобщения или удаления записей
  - Метод декомпозиции (разбиения на подмножества с последующим хранением)
  - Метод перемешивания (перестановки отдельных записей)
  - ~~**Криптографический метод**~~

cisco

Допускает ли приказ РКН применение криптографии?

- Методы обезличивания должны обеспечивать требуемые свойства обезличенных данных, соответствовать предъявляемым требованиям к их характеристикам (свойствам), быть практически реализуемыми в различных программных средах и позволять решать поставленные задачи обработки персональных данных
- К требованиям к свойствам метода обезличивания относятся:
  - обратимость (возможность проведения деобезличивания)
  - возможность обеспечения заданного уровня анонимности
  - увеличение стойкости при увеличении объема обезличиваемых персональных данных

Допускает ли приказ РКН применение криптографии?

- К требованиям к свойствам получаемых обезличенных данных относятся:
  - сохранение полноты (состав обезличенных данных должен полностью соответствовать составу обезличиваемых персональных данных)
  - сохранение структурированности обезличиваемых персональных данных
  - сохранение семантической целостности обезличиваемых персональных данных
  - анонимность отдельных данных не ниже заданного уровня

Методические рекомендации РКН по обезличиванию

- Все методы хороши, выбирай на вкус ☺

Свойства обезличенных данных \ Метод обезличивания	Метод введения идентификаторов	Метод изменения состава или семантики	Метод декомпозиции	Метод перемешивания
Полнота	+	+/-	+	+
Структурированность	+	+	+	+
Релевантность	+/-	+	+	+
Семантическая целостность	+	+/–	+	+
Применимость	+	+	+	+
Анонимность	+/-	+	+/-	+

\+ безусловное наличие свойства
+/- условное наличие свойства, см. описание метода

cisco

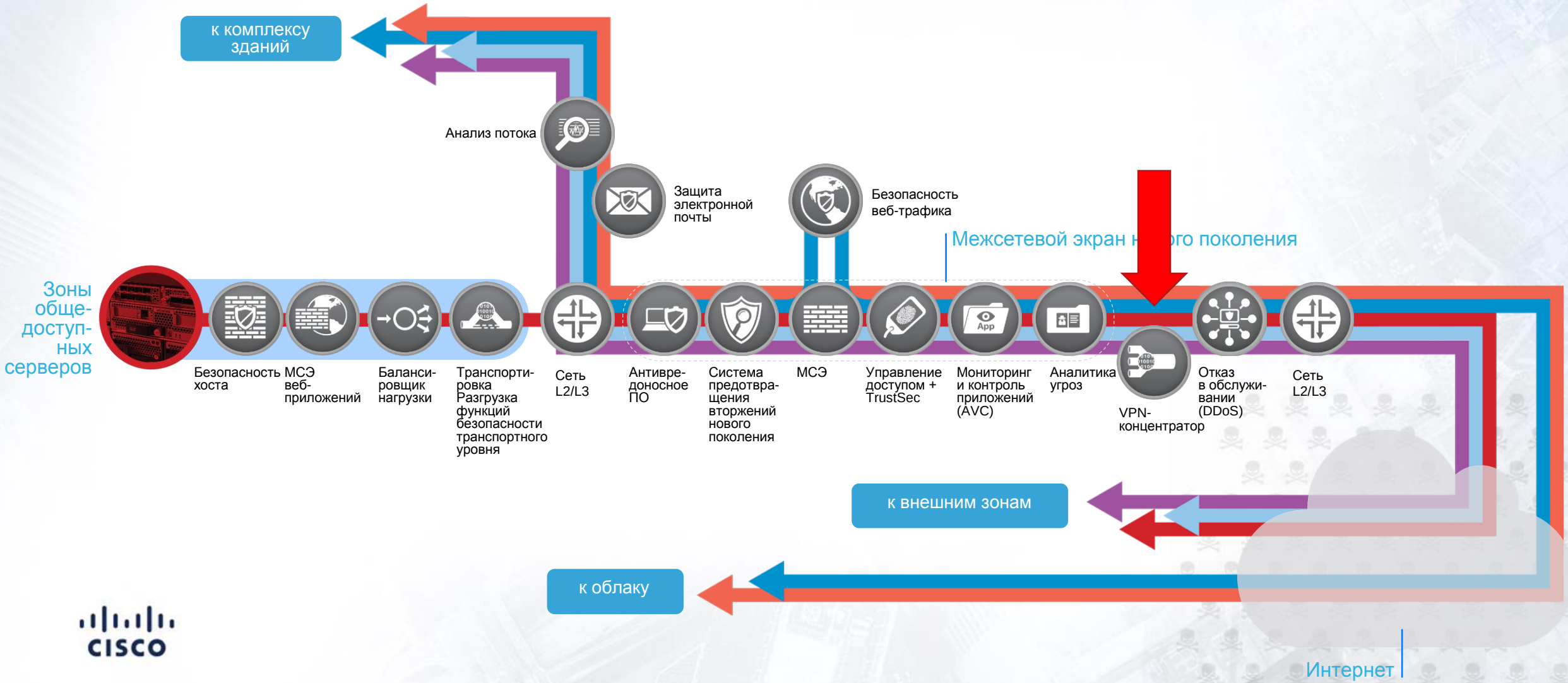
Что с сертификацией криптографии для обезличивания?

- Во всех существующих в России нормативных актах используется термин «криптографическая защита информации» и логическая связка «шифрование = защита информации»
  - В этом случае необходимо применение сертифицированных СКЗИ (хотя не всегда)
- Но обезличивание – это не защита информации
- Если шифрование/хеширование использовать для обезличивания, то вопрос применения сертифицированных СКЗИ на повестке дня не стоит

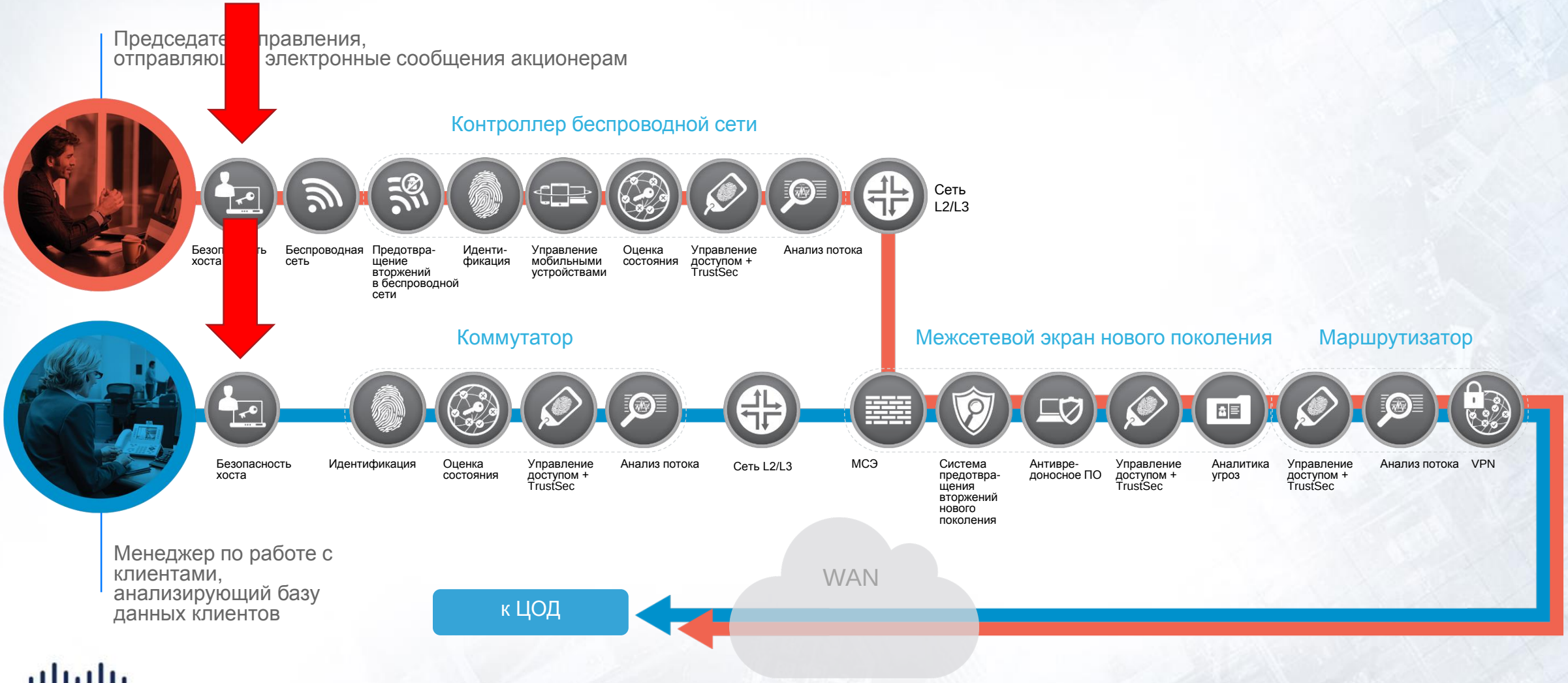
В качестве резюме

- Полное изолирование хранения персональных данных россиян на территории России сегодня не представляется возможным
  - Также как и перенос баз данных персональных данных на территорию России
- РКН активно проводит проверки выполнения ФЗ-242
- Обезличивание является способом решения стоящей задачи, так как выводит обезличенные данные из под действия ФЗ-152
- Криптография (шифрование и хеширование) могут быть использованы в качестве метода обезличивания
  - В т.ч. и с точки зрения существующих нормативных правовых актов

Где реализовать обезличивание? Периметр!



Где реализовать обезличивание? Хост!



Где реализовать обезличивание? ЦОД!

Спасибо!

alukatsk@cisco.com