КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

27 сентября 2018 г.
г. Екатеринбург

#CODEIB

АКТУАЛЬНЫЕ ВОПРОСЫ ОБРАБОБТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

КОНСТАНТИН САМАТОВ,

Руководитель направления в Аналитическом центре Уральского центра систем безопасности

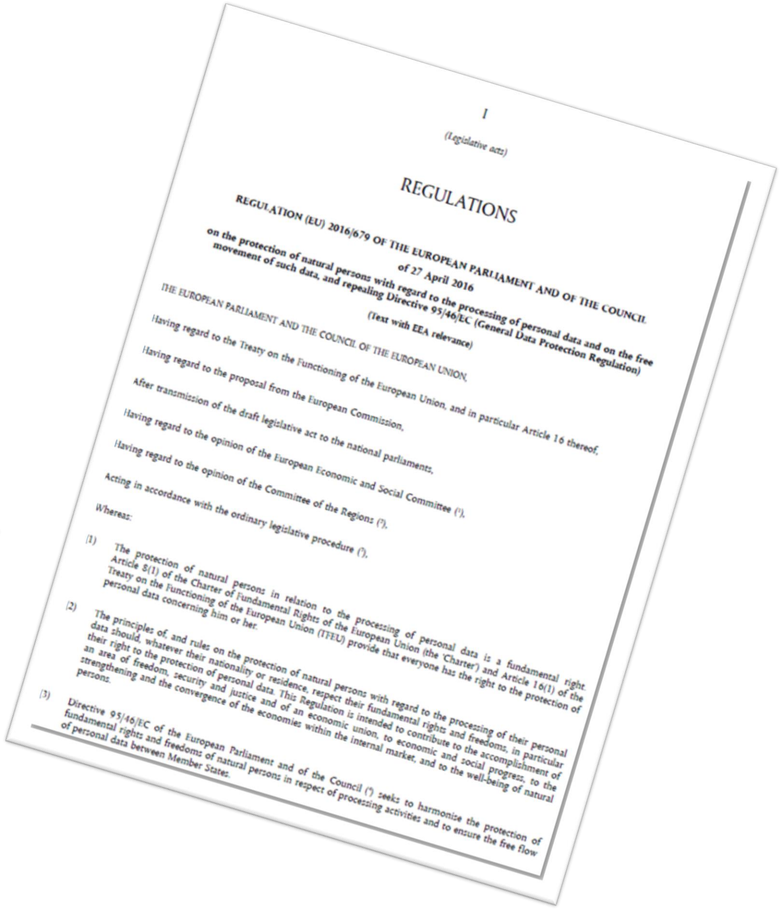
Член АРСИБ (Ассоциация руководителей служб информационной безопасности)

Преподаватель дисциплин информационной безопасности в УрГЭУ и УРТК им. А.С. Попова

О чем поговорим

1 ПРОБЛЕМНЫЕ ВОПРОСЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2 GDPR: ОБЛАСТИ ПРИМЕНЕНИЯ, ОСНОВНЫЕ ОТЛИЧИЯ ОТ ФЗ 152



I

(Legislative acts)

REGULATIONS

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 27 April 2016
on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee (1),

Having regard to the opinion of the Committee of the Regions (2),

Acting in accordance with the ordinary legislative procedure (3),

Whereas:

(1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.

(2) The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons.

(3) Directive 95/46/EC of the European Parliament and of the Council (4) seeks to harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to ensure the free flow of personal data between Member States.

Что такое персональные данные?

Любая информация, относящаяся к прямо или **косвенно** определенному или определяемому физическому лицу (субъекту персональных данных).

Проблемы:

1) непонимание операторов (организаций обрабатывающих персональные данные), что необходимо относить к персональным данным (в том числе при подготовке уведомления в РКН);

2) высокая вероятность быть привлеченным к ответственности за непредставление сведений об обработке персональных данных.

Относятся ли к ПДн:

Адрес электронной почты

IP адрес

Что считать биометрией?

Означает ли простановка галочки в SAPe или 1С напротив графы инвалидность что оператор обрабатывает специальные категории ПДн?

Адрес электронной почты является ПДн (см., например, Решение по делу № 12-253/2015 от 26.05.2015. Калининский районный суд (город Санкт-Петербург).

При этом стоит обратить внимание, что практика и мнение Роскомнадзора касательно отнесения электронной почты к категории ПДн неоднозначны. В ряде разъяснений Роскомнадзор указывает, что адрес электронной почты, содержащий ФИО, будет отнесен к категории ПДн, а в случае если адрес представляет собой набор символов (слов), его нельзя считать персональными данными.

Если можно идентифицировать субъекта – то ПДн

#CODEIB

IP адрес

Судебная практика однозначного решения не имеет. При этом одни суды IP-адрес к ПДн не относят (см., например, Постановление по делу № А56-75017/2014 от 01.06.2015. 13-й ААС), а другие, наоборот, признают (Решение по делу № А76-29008/2015 от 11.02.2016. АС Челябинской обл.).

Представляется, что статический IP-адрес справедливо относить к персональным данным, так как по нему можно идентифицировать пользователя.

Биометрические ПДн

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

Примеры Биометрических ПДн:

- фотографическое изображение и иные сведения, используемые для обеспечения однократного и/или многократного прохода на охраняемую территорию и установления личности гражданина.

- Фотографии в СКУД

Биометрические ПДн

вопрос вечера в палате - является ли скан жопы персональными данным?

Если можно однозначно идентифицировать субъекта, то да...

чота обсуждали, на кой икс поставили аж целых два считывателя для карточек, почему не захотели поставить сканер пальца

потом речь пошла про сканер глаза

и Маринка вспомнила, что отпечаток жопы тоже уникален

вопрос вечера - является ли скан жопы персональными данным?

в таком разрезе))))

Да. Причем биометрическими, ибо происходит удостоверение личности субъекта и его авторизация в системе контроля и управления доступом.

Не являются биометрическими ПДн

1) Фотографическое изображение, содержащееся в личном деле работника.

2) Подпись лица, наличие которой в различных договорных отношениях является обязательным требованием

3) Почерк, в том числе анализируемый уполномоченными органами в рамках почерковедческой экспертизы.

4) Материалы видеосъемки в публичных местах и на охраняемой территории, **до передачи** их **для установления личности** снятого человека.

Означает ли простановка галочки в SAPe или 1С напротив графы инвалидность, то что оператор обрабатывает специальные категории ПДн?

Инвалидность – это (в контексте 152-ФЗ):

1) Рассовая принадлежность
2) Национальная принадлежность
3) Политические взгляды
4) Религиозные убеждения
5) Философские убеждения
6) Состояние здоровья
7) Состояние интимной жизни
8) Социальный статус

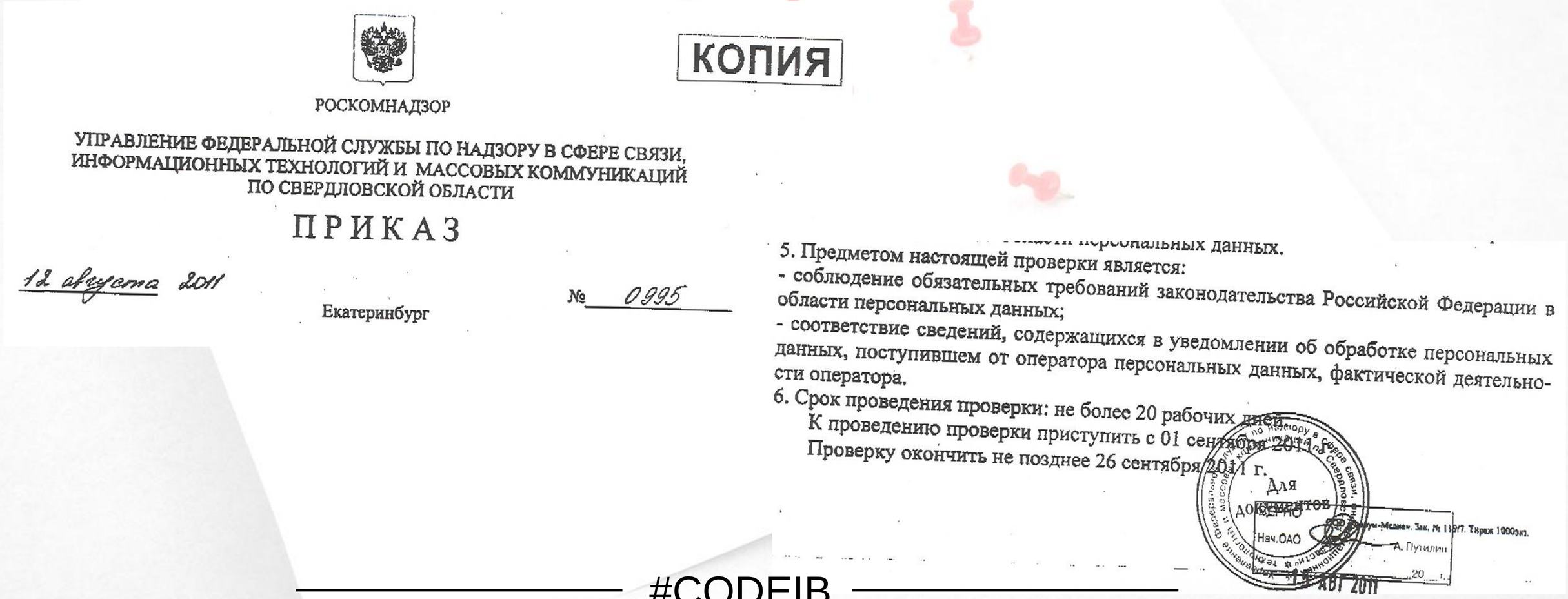
Что такое ПДн?

Фамилия имя отчество, дата рождения, серия и номер паспорта – ДА!

Остальное - ?

Санкции Регуляторов

Высокая вероятность быть привлеченным к ответственности за непредставление сведений об обработке персональных данных.



КОПИЯ

РОСКОМНАДЗОР

УПРАВЛЕНИЕ ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ ПО СВЕРДЛОВСКОЙ ОБЛАСТИ

ПРИКАЗ

12 августа 2011 № 0995

Екатеринбург

5. Предметом настоящей проверки является:
- соблюдение обязательных требований законодательства Российской Федерации в области персональных данных;
- соответствие сведений, содержащихся в уведомлении об обработке персональных данных, поступившем от оператора персональных данных, фактической деятельности оператора.

6. Срок проведения проверки: не более 20 рабочих дней.
К проведению проверки приступить с 01 сентября 2011 г.
Проверку окончить не позднее 26 сентября 2011 г.

Для документов
ДОВЕРЕНО
Нач.ОАО
А. Пугалин

Санкции Регуляторов

ПРЕДПИСАНИЕ

об устранении выявленного нарушения

«26» сентября 2011 г. № П-66-0234/06

Наименование проверяемого лица (юридического лица, индивидуального предпринимателя): Наименование оператора удалено автором

Номер лицензии (при наличии): нет
Наименование вида деятельности (услуги): обработка персональных данных
Дата и номер акта проверки: «26» сентября 2011г. № А-66-0610/06
Содержание нарушения:
- ч. 7 ст.22 Федерального закона от 27 июля 2006г. № 152-ФЗ «О персональных данных». Непредставление в уполномоченный орган сведений об изменении информации, содержащейся в уведомлении об обработке персональных данных, в определенный законодательством срок.

Основание выдачи предписания: статья 17 Федерального закона от 26.12.2008 № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля».
Срок устранения нарушения: 26 октября 2011 г.
Срок сообщения об устранении нарушения: 27 октября 2011г.
Подписи лиц, проводивших проверку:

В чем суть?

В уведомлении оператора не в полном объеме указаны категории обрабатываемых персональных данных. Уведомление не содержит следующих категорий обрабатываемых персональных данных: гражданство; ИНН; данные полиса ОМС; фактический адрес проживания; контактный телефон; номер истории болезни; код медико-экономического стандарта (МЭС); код международной классификации болезней (МКБ); код посещения медицинской организации; сведения, содержащиеся в трудовой книжке; сведения о воинском учете; сведения, содержащиеся в документах, подтверждающих право на дополнительные гарантии и компенсации по определенным основаниям, предусмотренным законодательством.

В чем суть?

Перечень категорий персональных данных субъектов, а также самих субъектов ставших известными оператору, не соответствует перечню, заявленному в уведомлении оператора об обработке персональных данных. Тем самым, оператор нарушил требование, предусмотренное ч.7 ст. 22 Закона.

Оператор персональных данных не представил в Уполномоченный орган информацию об изменении категорий обрабатываемых персональных данных, категориях субъектов персональных данных, целях обработки.

General Data Protection Regulation

- Вступил в силу 25.05.2018
- Отменяет Директиву 95/46/EC (англ. Data Protection Directive 95/46/EC)

Кто должен соблюдать в России?

1. Компании, учреждённые в ЕС*

Например:

Имеются дочерние предприятия в ЕС*

Есть представительства в ЕС*

Филиалы расположены на территории государства – члена ЕС*

* Или странах, следующих законодательству ЕС, на основании международных договоров (напр. Исландия, Лихтенштейн, Норвегия)

Кто должен соблюдать в России?

2. Компания осуществляет деятельность, связанную с ЕС

- Намерение к предложению
- Упоминание потребителей или пользователей в ЕС

Предложение товаров/услуг в ЕС

- Отслеживание в Интернете
- Анализ активности пользователя
- Ведение статистики и т.п.

Основные отличия от 152-ФЗ

GDPR

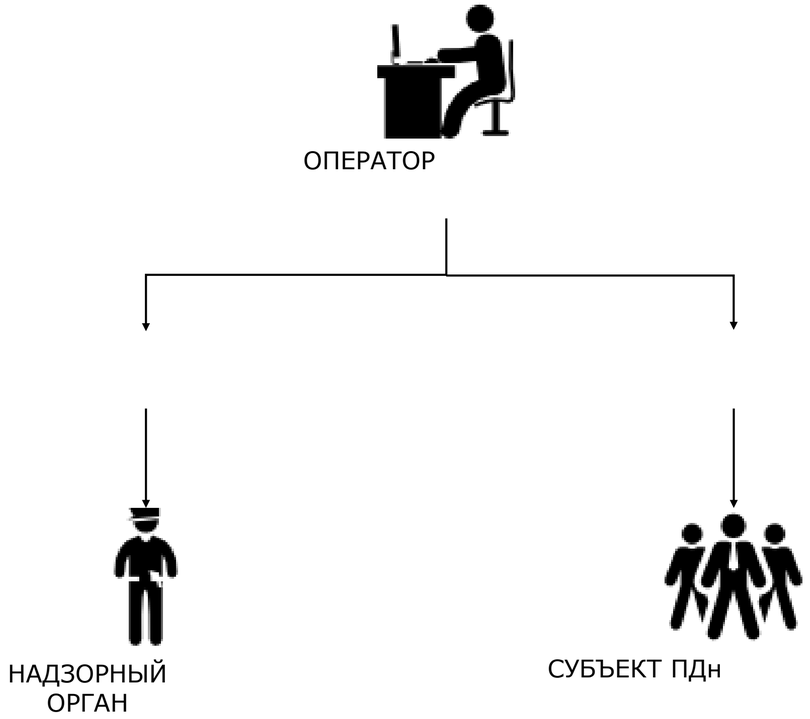
Оценка воздействия на защиту данных

Data
Protection
Impact
Assessment

- Описание предусмотренных операций по обработке ПДн.
- Оценка необходимости и соразмерности операций обработки по отношению к заявленным целым обработки.
- Оценка рисков для прав и свобод субъектов ПДн.
- Меры по обеспечению защиты ПДн.

GDPR

Уведомления об утечках



В случаях утечки ПДн, оператор обязан **сообщить о происшествии** надзорному органу, за исключением случаев, когда эта утечка ПДн едва ли обернется рисками для прав и свобод лиц.

- ✓ Компания должна документировать любые утечки ПДн, их последствия, а также предпринятые меры по устранению последствий.
- ✓ По возможности сообщить субъекту персональных данных, в разумный срок

Штрафы

GDPR

До 10 млн. Евро или до 2 % оборота компании

До 20 млн. Евро или до 4 % оборота компании

Сферы нарушения обязательств:

- Обработка ПДн ребёнка
- Защита by design и by default
- Совместная обработка с др. компаниями
- Не назначение представителя в ЕС
- Отчётные записи по обработке
- Обеспечение безопасности ПДн
- Уведомления об утечках
- Предварительная оценка влияния на защиту ПДн
- Требования к Офицеру по защите данных

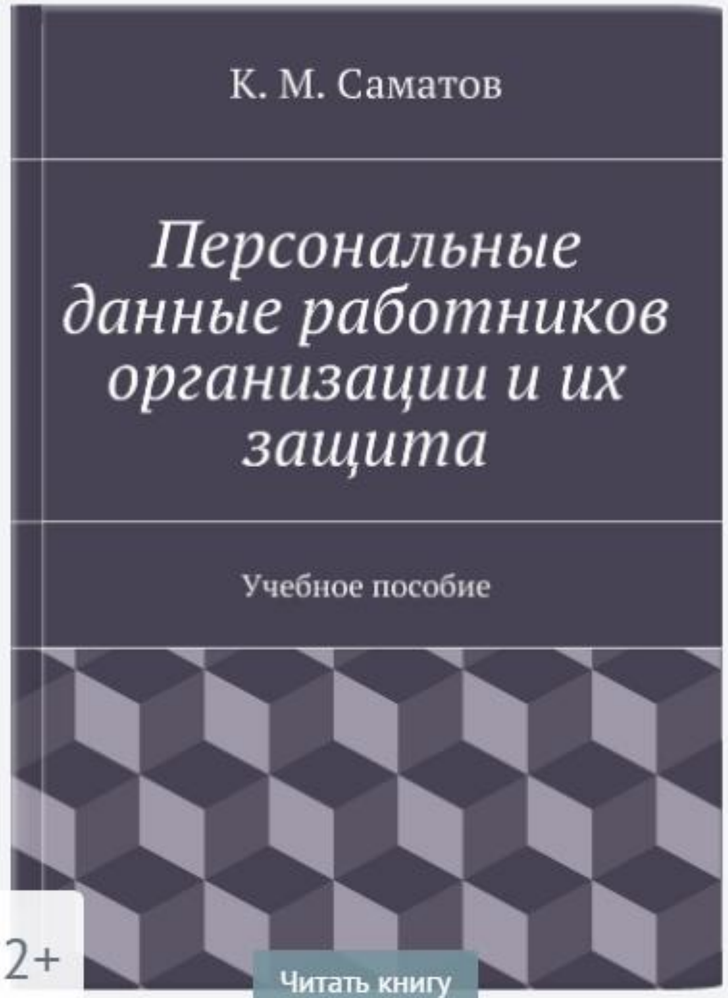
Нарушения основополагающих правил:

- Принципы обработки ПДн
- Правомерность обработки ПДн
- Правила согласия
- Обработка спец.категорий ПДн

Нарушение прав субъектов ПДн

Трансграничная передача ПДн

Подробнее про ПДн



14.06.2018

Рады сообщить, что книга размещена в открытом доступе для свободного скачивания.

Предлагаемое учебное пособие, первоначально предназначавшееся для работников кадровых служб организаций, получило широкую популярность среди руководителей служб безопасности, а также у специалистов по безопасности занимающихся частной практикой.

Книга была написана членом АРСИБ Константином Саматовым в 2016 году. В ней рассматриваются вопросы обработки персональных данных работников организации и построения системы их защиты. Уделено внимание вопросам прохождения операторами персональных данных контрольно-надзорных мероприятий со стороны государственных органов.

Скачать материал можно по ссылке. http://aciso.ru/news/3902/

СПАСИБО ЗА ВНИМАНИЕ!

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

27 Сентября 2018 г.
г. Екатеринбург

#CODEIB

КОНСТАНТИН САМАТОВ,

Руководитель направления в Аналитическом центре Уральского центра систем безопасности

Член АРСИБ (Ассоциация руководителей служб информационной безопасности)

Преподаватель дисциплин информационной безопасности в УрГЭУ и УРТК им. А.С. Попова

EMAIL: K.SAMATOV@GMAIL.COM

FACEBOOK: K.SAMATOV