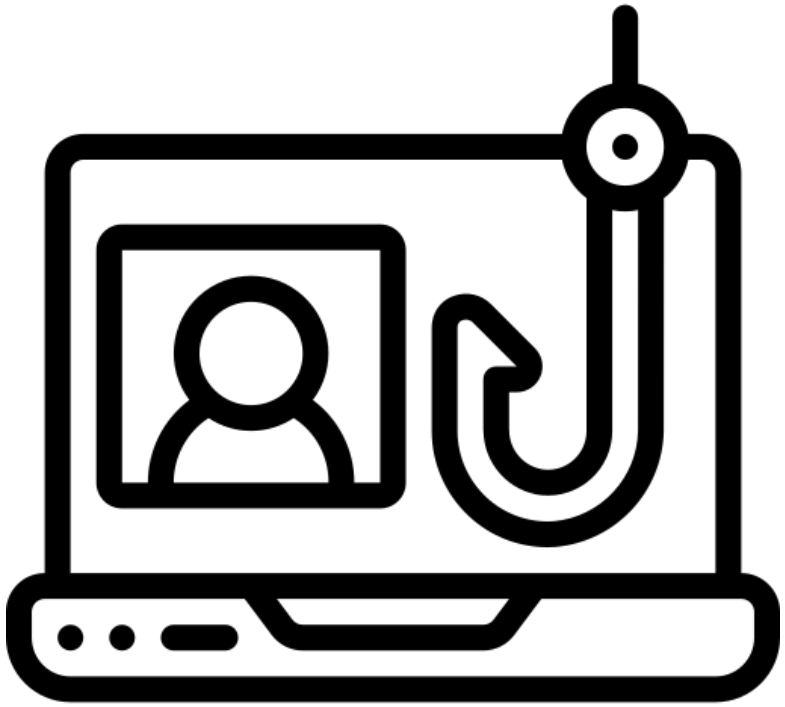
Белорусско-Российский университет
Кафедра «Программное обеспечение информационных технологий»

Защита информации

Защита персональных данных

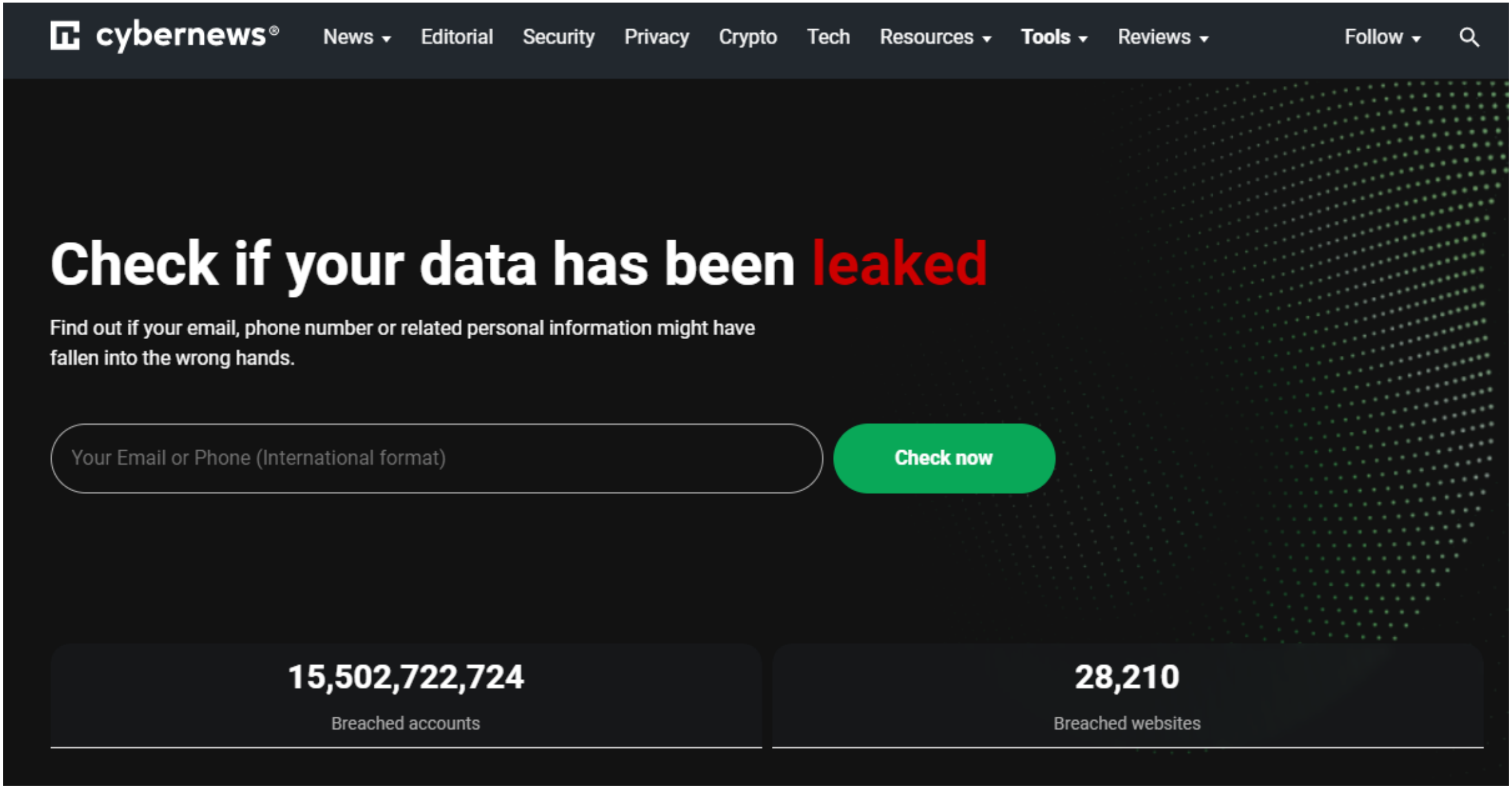
КУТУЗОВ Виктор Владимирович

Республика Беларусь, Могилев, 2024

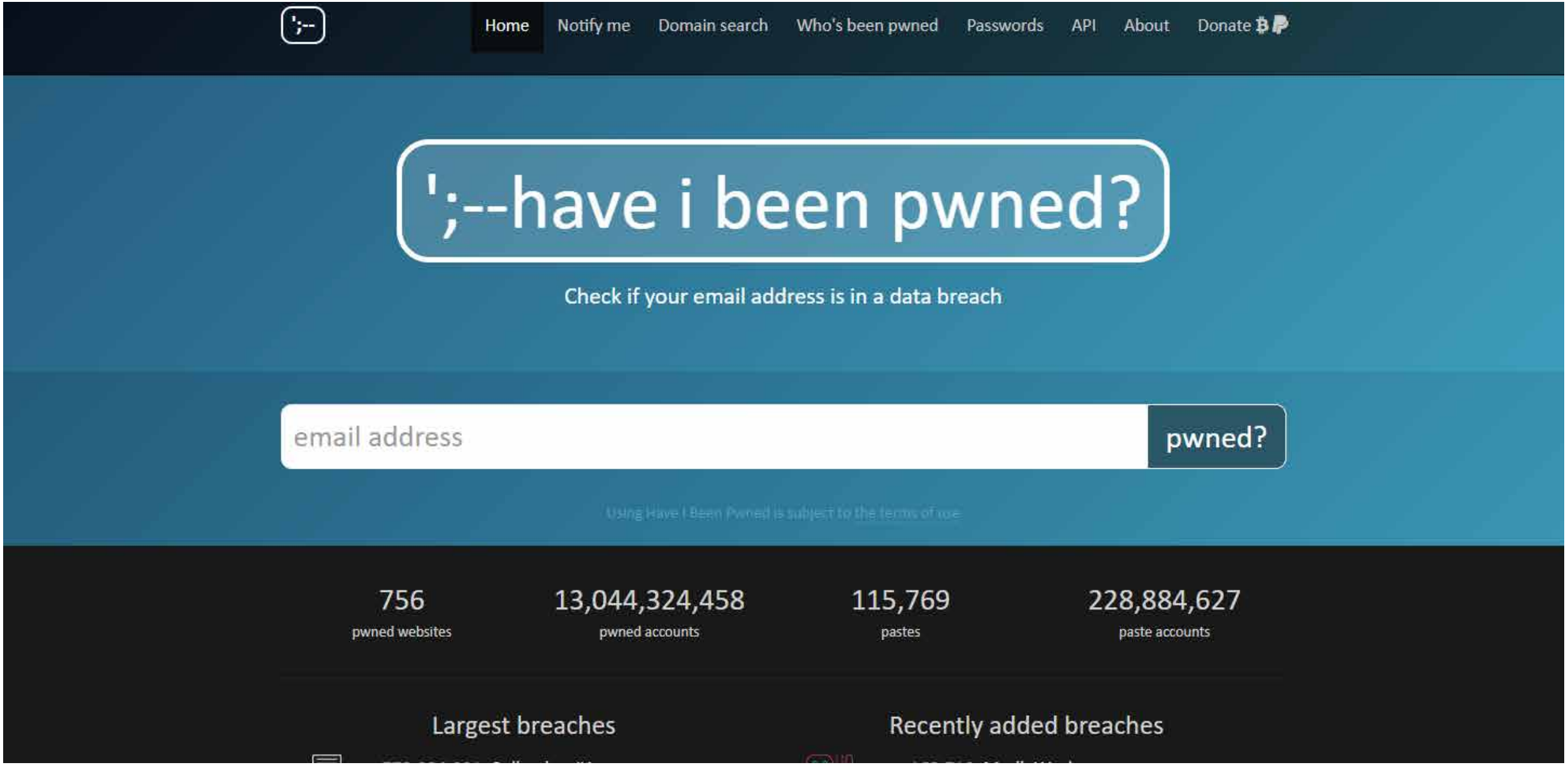


Прежде чем начинать тему **проверим ваши данные на наличие “утечек”**

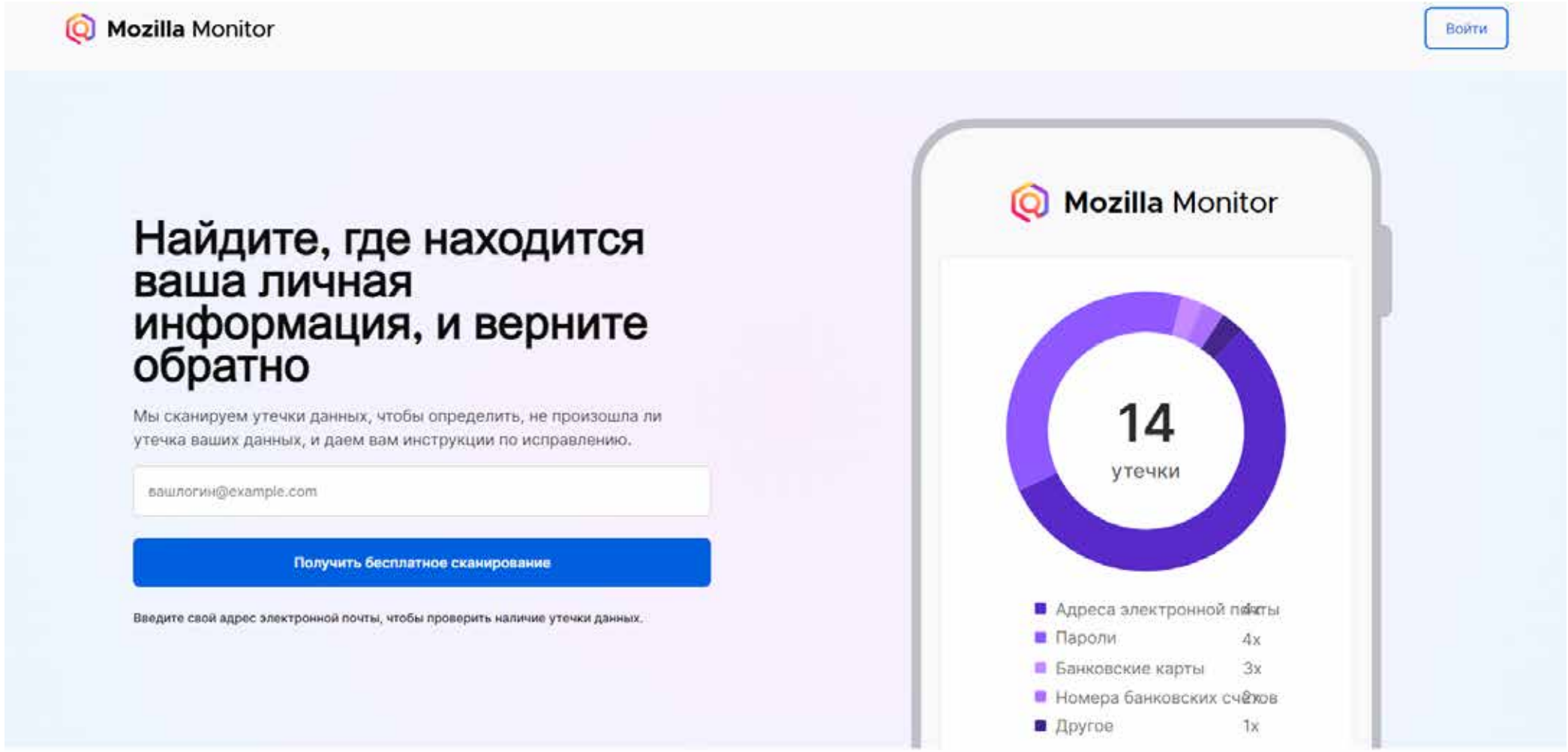
https://cybernews.com/personal-data-leak-check/



https://haveibeenpwned.com



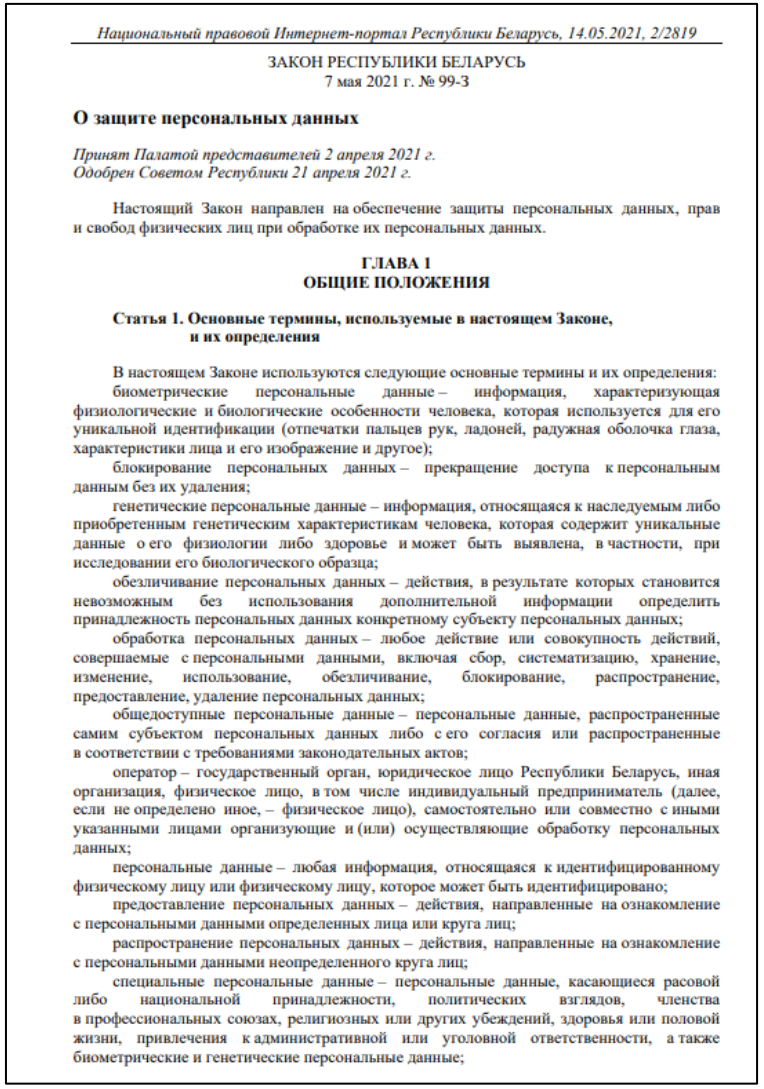
https://monitor.mozilla.org



Утечки данных происходят каждые 11 минут, раскрывая вашу личную информацию. Но не волнуйтесь, мы можем помочь.

Рекомендуемая литература по теме

Закон Республики Беларусь от 07.05.2021 № 99-З «О защите персональных данных»



Национальный правовой Интернет-портал Республики Беларусь, 14.05.2021, 2/2819

ЗАКОН РЕСПУБЛИКИ БЕЛАРУСЬ
7 мая 2021 г. № 99-З

О защите персональных данных

Принят Палатой представителей 2 апреля 2021 г.
Одобрен Советом Республики 21 апреля 2021 г.

Настоящий Закон направлен на обеспечение защиты персональных данных, прав и свобод физических лиц при обработке их персональных данных.

ГЛАВА 1
ОБЩИЕ ПОЛОЖЕНИЯ

Статья 1. Основные термины, используемые в настоящем Законе, и их определения

В настоящем Законе используются следующие основные термины и их определения:

биометрические персональные данные – информация, характеризующая физиологические и биологические особенности человека, которая используется для его уникальной идентификации (отпечатки пальцев рук, ладоней, радужная оболочка глаза, характеристики лица и его изображение и другое);

блокирование персональных данных – прекращение доступа к персональным данным без их удаления;

генетические персональные данные – информация, относящаяся к наследуемым либо приобретенным генетическим характеристикам человека, которая содержит уникальные данные о его физиологии либо здоровье и может быть выявлена, в частности, при исследовании его биологического образца;

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

обработка персональных данных – любое действие или совокупность действий, совершаемые с персональными данными, включая сбор, систематизацию, хранение, изменение, использование, обезличивание, блокирование, распространение, предоставление, удаление персональных данных;

общедоступные персональные данные – персональные данные, распространенные самим субъектом персональных данных либо с его согласия или распространенные в соответствии с требованиями законодательных актов;

оператор – государственный орган, юридическое лицо Республики Беларусь, иная организация, физическое лицо, в том числе индивидуальный предприниматель (далее, если не определено иное, – физическое лицо), самостоятельно или совместно с иными указанными лицами организующие и (или) осуществляющие обработку персональных данных;

персональные данные – любая информация, относящаяся к идентифицированному физическому лицу или физическому лицу, которое может быть идентифицировано;

предоставление персональных данных – действия, направленные на ознакомление с персональными данными определенных лица или круга лиц;

распространение персональных данных – действия, направленные на ознакомление с персональными данными неопределенного круга лиц;

специальные персональные данные – персональные данные, касающиеся расовой либо национальной принадлежности, политических взглядов, членства в профессиональных союзах, религиозных или других убеждений, здоровья или половой жизни, привлечения к административной или уголовной ответственности, а также биометрические и генетические персональные данные;

- Закон Республики Беларусь от 07.05.2021 № 99-З **О защите персональных данных**

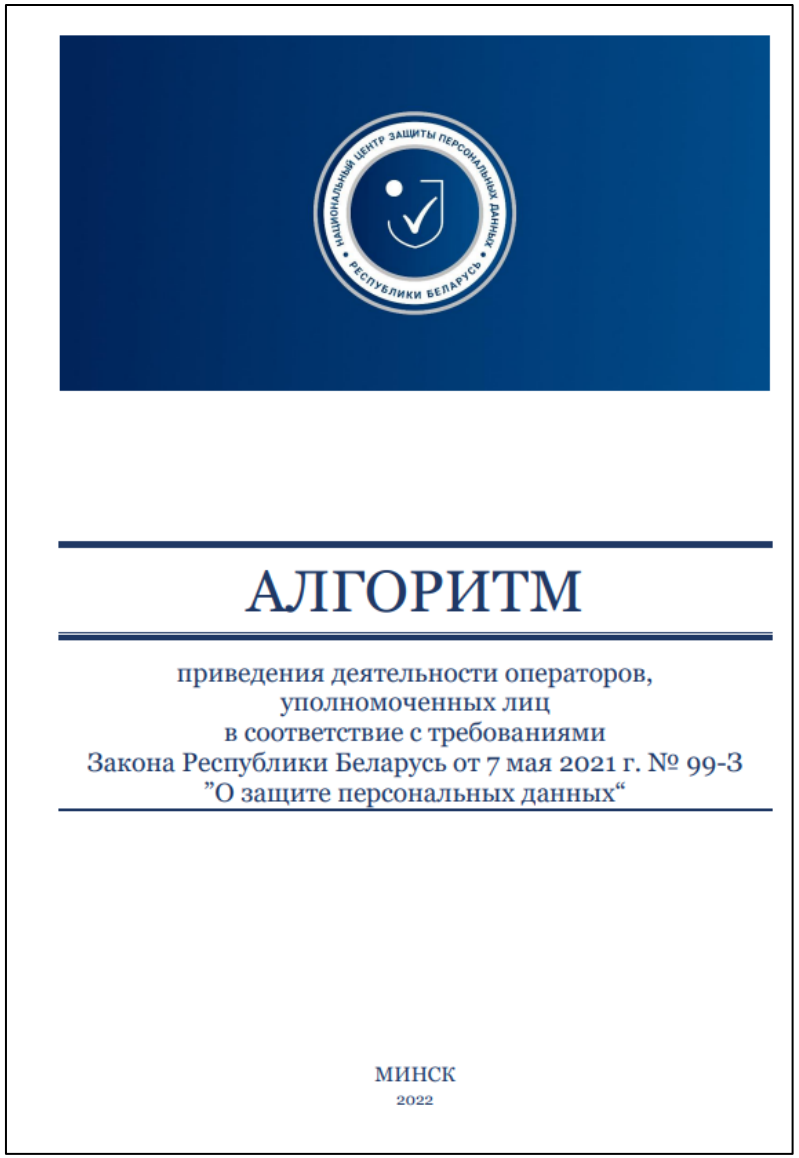
- https://pravo.by/upload/docs/op/H12100099_1620939600.pdf

Постатейный комментарий к Закону

- **Постатейный комментарий к Закону Республики Беларусь "О защите персональных данных"** – Минск : Национальный центр защиты персональных данных, 2023 – 202 с.

- https://cpd.by/storage/2023/02/NPK-22.02.2023.pdf

Алгоритм



- **Алгоритм приведения деятельности операторов, уполномоченных лиц в соответствие с требованиями Закона** Республики Беларусь от 7 мая 2021 г. № 99-З ”О защите персональных данных“

- https://cpd.by/storage/2022/05/algoritm_dejstvij_operatora_razjasnenie.pdf

Национальный центр защиты персональных данных Республики Беларусь

Нормативные правовые акты

1. **Конституция Республики Беларусь**
2. **Закон** Республики Беларусь от 7 мая 2021 г. № 99-З "**О защите персональных данных**"
3. **Указ** Президента Республики Беларусь от 28 октября 2021 г. № 422 "**О мерах по совершенствованию защиты персональных данных**"
4. **Закон** Республики Беларусь от 10 ноября 2008 г. № 455-З "**Об информации, информатизации и защите информации**"
5. **Закон** Республики Беларусь от 21 июля 2008 г. № 418-З "**О регистре населения**"
6. **Трудовой кодекс Республики Беларусь** (статья 47)
7. **Кодекс Республики Беларусь об административных правонарушениях** (статья 23.7)
8. **Уголовный кодекс Республики Беларусь** (статьи 203-1, 203-2)
9. **Приказ** Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 "О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449"
10. **Приказ** Оперативно-аналитического центра при Президенте Республики Беларусь от 12 ноября 2021 г. № 194 "**Об обучении по вопросам защиты персональных данных**"
11. **Приказ** Оперативно-аналитического центра при Президенте Республики Беларусь от 12 ноября 2021 г. № 195 **"О технической и криптографической защите персональных данных"**
12. **Приказ** Оперативно-аналитического центра при Президенте Республики Беларусь от 1 июня 2022 г. № 94 "О государственном информационном ресурсе "**Реестр операторов персональных данных**"
13. **Приказ** Оперативно-аналитического центра при Президенте Республики Беларусь от 23 ноября 2023 г. № 218 "Об изменении приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 12 ноября 2021 г. № 194"

Правовые акты

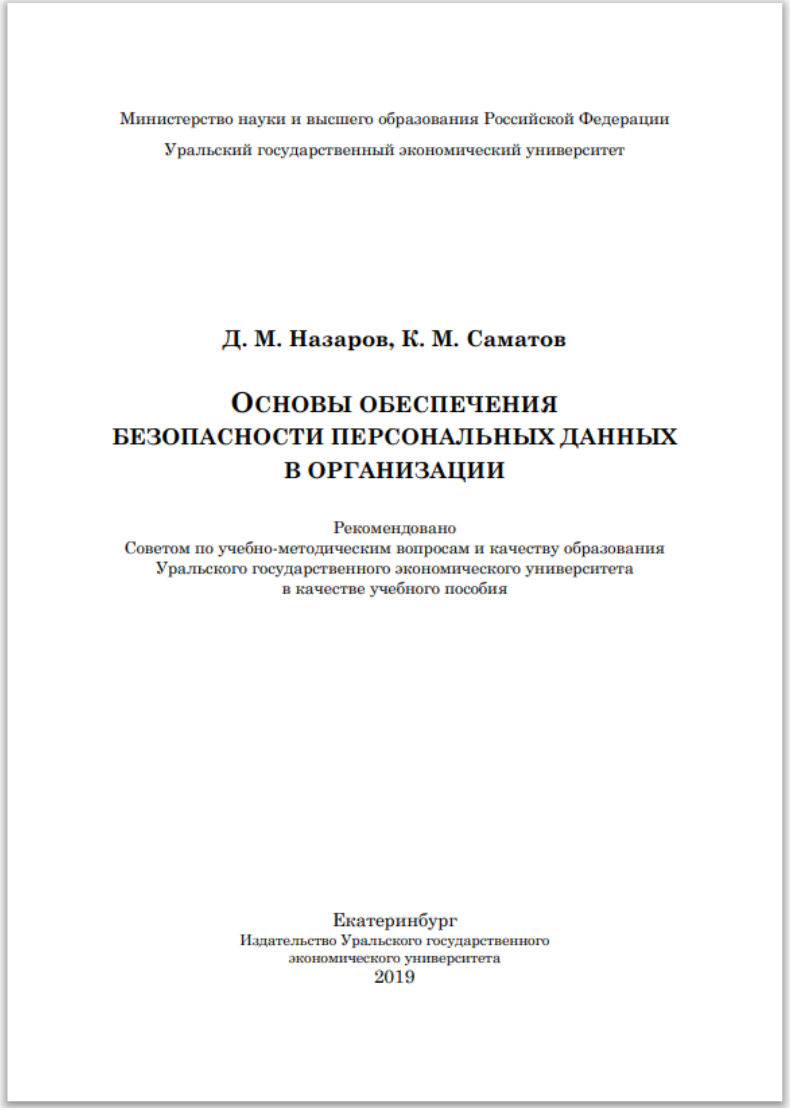
1. **Приказ** директора Национального центра защиты персональных данных Республики Беларусь от 15 ноября 2021 г. № 12 "**О классификации информационных ресурсов (систем)**"
2. **Приказ** директора Национального центра защиты персональных данных Республики Беларусь от 15 ноября 2021 г. № 13 "**Об уведомлении о нарушениях систем защиты персональных данных**"
3. **Приказ** директора Национального центра защиты персональных данных Республики Беларусь от 15 ноября 2021 г. № 14 "**О трансграничной передаче персональных данных**"
4. **Приказ** директора Национального центра защиты персональных данных Республики Беларусь от 26 декабря 2022 г. № 114 "Об изменении приказа директора Национального центра защиты персональных данных Республики Беларусь от 15 ноября 2021 г. № 14"

Рекомендуемая литература по теме

Шаблинский, И. Г. **Правовое регулирование информационных отношений в сфере обработки персональных данных** : учебное пособие для вузов / И. Г. Шаблинский ; под редакцией М. А. Федотова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 52 с.

https://urait.ru/bcode/544886

Рекомендуемая литература по теме


Министерство науки и высшего образования Российской Федерации
Уральский государственный экономический университет

Д. М. Назаров, К. М. Саматов

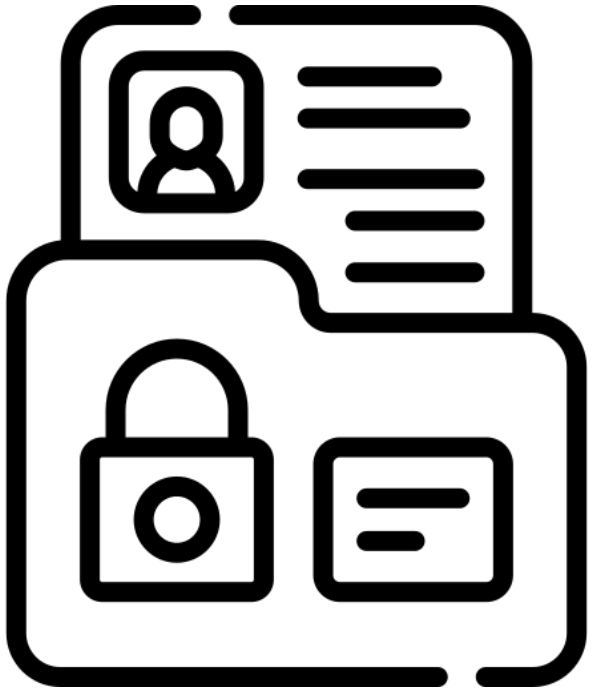
ОСНОВЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОРГАНИЗАЦИИ

Рекомендовано
Советом по учебно-методическим вопросам и качеству образования
Уральского государственного экономического университета
в качестве учебного пособия

Екатеринбург
Издательство Уральского государственного
экономического университета
2019

Назаров, Д. М. **Основы обеспечения безопасности персональных данных в организации** : учеб. пособие / Д. М. Назаров, К. М. Саматов ; М-во науки и высш. образования Рос. Федерации, Урал. гос. экон. ун-т. — Екатеринбург : Изд-во Урал. гос. экон. ун-та, 2019. — 118 с.

http://aciso.ru/files/news/uchebnik.pdf



Персональные данные

Информация. Персональные данные

- В настоящее время **информация – это «нефть 21 века»**.
- Т.е. информация это ценнейший ресурс, который необходимо защищать.
- **Персональные данные** о человеке, компании и т.д. также являются ценнейшим информационным ресурсом.

Что такое персональные данные

- Единого понятия персональных данных не закреплено — каждое государство раскрывает его значение самостоятельно.

- На международном уровне персональные данные были определены **в Конвенции Совета Европы** о защите частных лиц в отношении автоматизированной обработки данных личного характера, согласно которой **«персональные данные» означают любую информацию об определенном или поддающемся определению физическом лице**. Конвенция стала основой для развития законодательства членов Совета Европы, которые понимают «персональные данные» максимально широко.

Что такое персональные данные

- **Как правило, к персональным данным относят** информацию о человеке (субъекте персональных данных), которая самостоятельно или вместе с использованием иной информации идентифицирует или может позволить идентифицировать такого человека.

- **К персональным данным может относиться практически любая информация**, начиная с ФИО, места жительства, работы граждан, их идентификационного или налогового номера и пр., заканчивая данными о поведении, передвижении, взглядах, предпочтениях, убеждениях конкретного лица, его IP адресе, рекламном профиле и пр.

- **В то же время, законодательство конкретного государства может сужать или по-своему интерпретировать понятие «персональных данных»,** поэтому для определения объёма регулирования и требований к операторам персональных данных нужно изучать законодательство конкретного государства и его правоприменительные подходы.

Какими могут быть персональные данные

- Персональные можно разделить на виды по их характеру и степени «чувствительности», уязвимости.
- **От вида персональных данных зависят условия их обработки, предоставления доступа к персональным данным, требования к их защите.**
- **Как правило, выделяют следующие виды персональных данных:**

  1) персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, половой жизни и пр.;

  2) биометрические данные, касающиеся физических, физиологических или поведенческих характеристик человека, которые предоставляют их уникальную идентификацию (изображение лица человека, дактилоскопические данные и пр.);

  3) генетические данные — данные в отношении унаследованных или приобретенных характеристик человека, которые получены в результате анализа его биологических материалов (например, в результате анализа хромосом, ДНК или РНК).

  4) персональные данные в общедоступных источниках;

  5) иные данные — остальные персональные данные, не относящиеся к вышеперечисленным.
- Наиболее уязвимыми являются первые три вида персональных данных, которые, как правило, подлежат особой защите.

Примеры источников персональных данных.
Сбор персональных данных физических лиц (субъектов)

Предоставленные данные

получены от субъектов или их представителей, например, заполнение веб-форм на сайте, представление интересов в суде

Распространенные данные

взяты из общедоступных или открытых источников, например, исследование учетных записей в социальных сетях

Наблюдаемые данные

зафиксированы путем отслеживания действий, например, онлайн-трекинг, геолокация, видеонаблюдение

Принятые данные

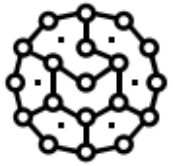
получены не от субъектов, а от других лиц, например, рекомендация от бывшего работодателя соискателя

Назначенные данные

временно или постоянно присвоены субъектам, например, номер социального страхования, наименование должности

Производные данные

созданы путем простого анализа других данных, например, расчет прибыльности клиента по количеству посещений и купленных товаров



Предполагаемые данные

созданы путем анализа корреляции между наборами данных, например, расчет кредитного рейтинга или прогнозирование состояния здоровья

Защита персональных данных РБ

- В каждой из стран действуют законы по защите персональных данных

- **В Республике Беларусь**
  - **Закон** от 07.05.2021 № 99-З «**О защите персональных данных**» https://pravo.by/upload/docs/op/H12100099_1620939600.pdf

  - **Указ** Президента Республики Беларусь от 28 октября 2021 г. № 422 **”О мерах по совершенствованию защиты персональных данных“** https://president.gov.by/ru/documents/ukaz-no-422-ot-28-oktyabrya-2021-g

Защита персональных данных РФ

- В каждой из стран действуют законы по защите персональных данных

- **В Российской Федерации**
  - Федеральный **закон** от 27.07.2006 N 152-ФЗ "**О персональных данных**"
    http://www.consultant.ru/document/cons_doc_LAW_61801/
  - **Постановление** Правительства РФ от 29 июня 2021 г. № 1046 «**О федеральном государственном контроле (надзоре) за обработкой персональных данных**»
    https://www.garant.ru/products/ipo/prime/doc/401316524/
  - **Приказ** Роскомнадзора от 24.02.2021 N 18 «**Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения**»
    http://publication.pravo.gov.ru/Document/View/0001202104210039

Защита персональных данных

- **Республика Казахстан**
  - **Приказ** Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 21 октября 2020 года № 395/НҚ «**Об утверждении правил сбора, обработки персональных данных**».
    https://www.tadviser.ru/index.php/Статья:Обработка_персональных_данных_в_Казахстане
    https://online.zakon.kz/Document/?doc_id=39051375#pos=2;-52

- **Украина**
  - **Закон** України. **Про захист персональних даних** (Відомості Верховної Ради України (ВВР), 2010, № 34, ст. 481)
    https://zakon.rada.gov.ua/laws/show/2297-17#Text
    https://zakon.rada.gov.ua/laws/show/3454-17#Text

Защита персональных данных

- **В Европейском союзе** - GDPR (General Data Protection Regulation) - Общий регламент защиты персональных данных.
- **В США** – Privacy Act of 1974 и Privacy Protection Act of 1980, SP 800-122, а также ряд других документов в зависимости от каждого конкретного штата.
- **В США в Калифорнии** - CCPA (California Consumer Privacy Act)
- **В Китае** - Закон о защите личной информации Personal Information Protection Law (PIPL)

Защита персональных данных

- **LGPD** - Lei Geral de Proteção de Dados – Бразилия
- **NZPA** - New Zealand Privacy Act 2020 – Новая Зеландия
- **PDPA** - Personal Data Protection Act – Сингапур
- South Africa **POPIA** - South Africa, Parliament passed the Protection of Personal Information Act – Африка
- **APPs** - Australia Privacy Act 1988 – Австралия
- **ALRC** 108 - Australian Privacy Law and Practice – Австралия
- **DIFC** - DIFC Data Protection Law, 2020 – Дубай
- **PDPA** - Personal Data Protection Act, B.E. 2562 (2019) – Таиланд
- **PIPEDA** - Personal Information Protection and Electronic Documents Act - Канада
- Data Protection Bill 2017 – Великобритания

Защита персональных данных

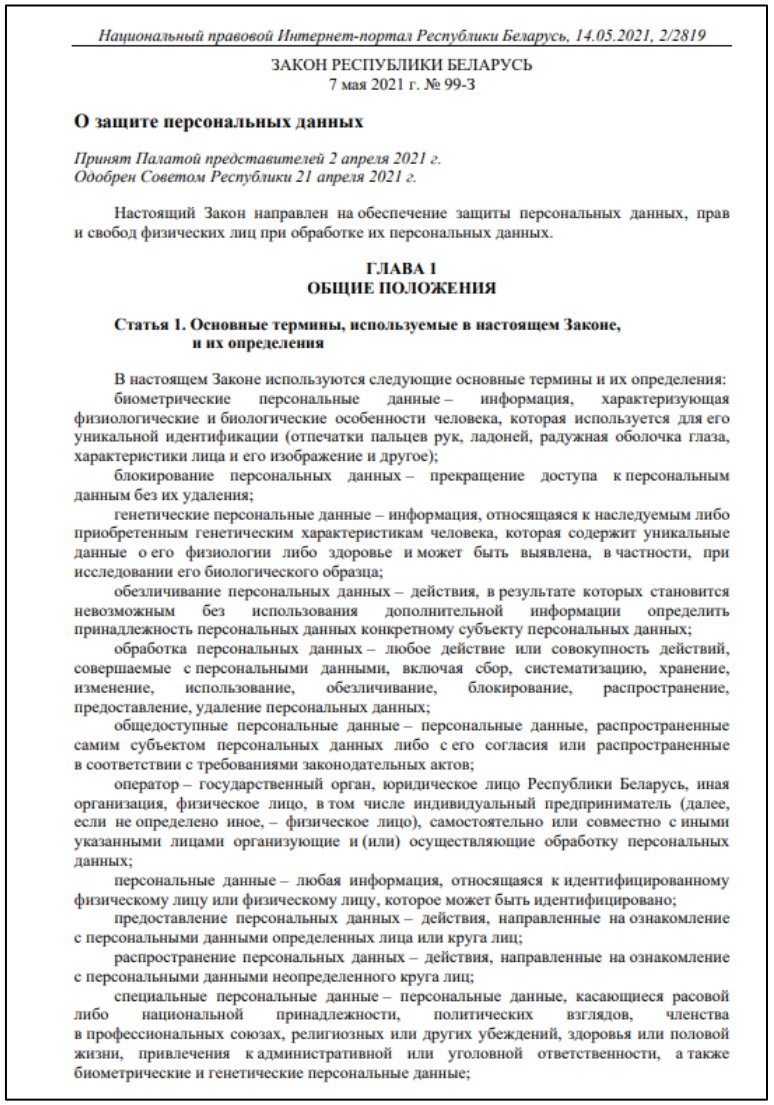
- **ADHICS** - Abu Dhabi Healthcare Information and Cyber Security – Абу-Даби
- **ECL** - E-Commerce Law 2019 – Саудовская Аравия
- **LPPD** - Law on the Protection of Personal Data No. 6698 - Турция
- **PDPB** - Personal Data Protection Bill - Индия
- **Irish DPA** - Irish Data Protection Act, 2018 - Ирландия
- **Hong Kong's PDPO** - Personal Data (Privacy) Ordinance (Cap. 486) as amended in 2012 – Гонг-Конг
- **Philippines DPA** - Data Privacy Act of 2012 Republic Act. No, 10173 - Филиппины
- **Federal Telecommunication Law** (Federal Law) – Объединенные арабские эмираты

Принят Палатой
представителей
2 апреля 2021 г.
Одобрен Советом Республики
21 апреля 2021 г.

Закон Республики Беларусь от 07.05.2021 № 99-З О защите персональных данных

https://pravo.by/upload/docs/op/H12100099_1620939600.pdf

Закон Республики Беларусь от 07.05.2021 № 99-З «О защите персональных данных»



Национальный правовой Интернет-портал Республики Беларусь, 14.05.2021, 2/2819

ЗАКОН РЕСПУБЛИКИ БЕЛАРУСЬ
7 мая 2021 г. № 99-З

О защите персональных данных

Принят Палатой представителей 2 апреля 2021 г.
Одобрен Советом Республики 21 апреля 2021 г.

Настоящий Закон направлен на обеспечение защиты персональных данных, прав и свобод физических лиц при обработке их персональных данных.

ГЛАВА 1
ОБЩИЕ ПОЛОЖЕНИЯ

Статья 1. Основные термины, используемые в настоящем Законе, и их определения

В настоящем Законе используются следующие основные термины и их определения:

биометрические персональные данные – информация, характеризующая физиологические и биологические особенности человека, которая используется для его уникальной идентификации (отпечатки пальцев рук, ладоней, радужная оболочка глаза, характеристики лица и его изображение и другое);

блокирование персональных данных – прекращение доступа к персональным данным без их удаления;

генетические персональные данные – информация, относящаяся к наследуемым либо приобретенным генетическим характеристикам человека, которая содержит уникальные данные о его физиологии либо здоровье и может быть выявлена, в частности, при исследовании его биологического образца;

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

обработка персональных данных – любое действие или совокупность действий, совершаемые с персональными данными, включая сбор, систематизацию, хранение, изменение, использование, обезличивание, блокирование, распространение, предоставление, удаление персональных данных;

общедоступные персональные данные – персональные данные, распространенные самим субъектом персональных данных либо с его согласия или распространенные в соответствии с требованиями законодательных актов;

оператор – государственный орган, юридическое лицо Республики Беларусь, иная организация, физическое лицо, в том числе индивидуальный предприниматель (далее, если не определено иное, – физическое лицо), самостоятельно или совместно с иными указанными лицами организующие и (или) осуществляющие обработку персональных данных;

персональные данные – любая информация, относящаяся к идентифицированному физическому лицу или физическому лицу, которое может быть идентифицировано;

предоставление персональных данных – действия, направленные на ознакомление с персональными данными определенных лица или круга лиц;

распространение персональных данных – действия, направленные на ознакомление с персональными данными неопределенного круга лиц;

специальные персональные данные – персональные данные, касающиеся расовой либо национальной принадлежности, политических взглядов, членства в профессиональных союзах, религиозных или других убеждений, здоровья или половой жизни, привлечения к административной или уголовной ответственности, а также биометрические и генетические персональные данные;

- Закон Республики Беларусь от 07.05.2021 № 99-З **О защите персональных данных**

- https://pravo.by/upload/docs/op/H12100099_1620939600.pdf

Закон Республики Беларусь от 07.05.2021 № 99-З «О защите персональных данных»

Термины

- **субъект персональных данных** – физическое лицо, в отношении которого осуществляется обработка персональных данных;
- **оператор** – государственный орган, юридическое лицо Республики Беларусь, иная организация, физическое лицо, в том числе индивидуальный предприниматель (далее, если не определено иное, – физическое лицо), самостоятельно или совместно с иными указанными лицами организующие и (или) осуществляющие обработку персональных данных;
- **уполномоченное лицо** – государственный орган, юридическое лицо Республики Беларусь, иная организация, физическое лицо, которые в соответствии с актом законодательства, решением государственного органа, являющегося оператором, либо на основании договора с оператором осуществляют обработку персональных данных от имени оператора или в его интересах;
- **физическое лицо,** которое может быть идентифицировано, – физическое лицо, которое может быть прямо или косвенно определено, в частности через фамилию, собственное имя, отчество, дату рождения, идентификационный номер либо через один или несколько признаков, характерных для его физической, психологической, умственной, экономической, культурной или социальной идентичности.

Персональные данные

- **Персональные данные – любая информация, относящаяся к идентифицированному физическому лицу или физическому лицу, которое может быть идентифицировано;** (то есть прямо или косвенно определено через фамилию, собственное имя, отчество, дату рождения, идентификационный номер либо через один или несколько признаков, характерных для его физической, психологической, умственной, экономической, культурной или социальной идентичности) (абз.9, 17 ст.1 Закона № 99-З).

- В целом сохраняется действующий подход, в соответствии с которым персональными данными является любая информация, с помощью которой возможно идентифицировать лицо.

Виды персональных данных

Виды персональных данных

- **Биометрические** (информация, характеризующая физиологические и биологические особенности человека, которая используется для его уникальной идентификации (отпечатки пальцев рук, ладоней, радужная оболочка глаза, характеристики лица и его изображение и другое);
- **Генетические** (информация, относящаяся к наследуемым либо приобретенным генетическим характеристикам человека, которая содержит уникальные данные о его физиологии либо здоровье и может быть выявлена, в частности, при исследовании его биологического образца)
- **Общедоступные** (персональные данные, распространенные самим субъектом персональных данных либо с его согласия или распространенные в соответствии с требованиями законодательных актов)
- **Любая информация** (любая информация, относящаяся к идентифицированному физическому лицу или физическому лицу, которое может быть идентифицировано)
- **Специальные** (персональные данные, касающиеся расовой либо национальной принадлежности, политических взглядов, членства в профессиональных союзах, религиозных или других убеждений, здоровья или половой жизни, привлечения к административной или уголовной ответственности, а также биометрические и генетические персональные данные)

Категории персональных данных

Основные

- идентификационный номер;
- фамилия, собственное имя, отчество (если таковое имеется);
- пол;
- число, месяц, год (далее - дата) рождения;
- место рождения;
- цифровой фотопортрет;
- данные о гражданстве (подданстве);
- данные о регистрации по месту жительства и (или) месту' пребывания;
- данные о смерти или объявлении физического лица умершим, признании безвестно отсутствующим, недееспособным, ограниченно дееспособным

(п. 1 ст. 8 Закона № 418-З).

Дополнительные

- о родителях, опекунах, попечителях; семейном положении; супруге, ребенке (детях) физического лица;
- о высшем образовании; ученой степени., ученом звании;
- о роде занятий;
- о пенсии., ежемесячном денежном содержании по законодательству о государственной службе, ежемесячной страховой выплате по обязательному страхованию от несчастных случаев на производстве и профессиональных заболеваний;
- о налоговых обязательствах;
- об исполнении воинской обязанности;
- об инвалидности

(п. 1 ст. 10 Закона № 418-З).

Специальные персональные данные

- Законом № 99-З выделяется особая категория персональных данных - **специальные персональные данные** (абз.12 ст.1 Закона № 99-З), которая включает в себя данные о:
  - расовой или национальной принадлежности,
  - политических взглядах,
  - членстве в профессиональных союзах,
  - религиозных или других убеждениях,
  - здоровье или половой жизни,
  - привлечении к административной или уголовной ответственности,
  - физиологических и биологических особенностях человека (отпечатки пальцев рук, ладоней, радужная оболочка глаза, характеристики лица и его изображение и другое), которые используются для его уникальной идентификации (биометрические персональные данные) (абз.2 ст.1 Закона № 99-З);
- и **генетические персональные данные** - наследуемые либо приобретенные генетические характеристики человека, которые содержат уникальные данные о его физиологии либо здоровье (абз.4 ст.1 Закона № 99-З)

Специальные и общедоступные персональные данные

- **В отношении специальных персональных данных предусматриваются дополнительные гарантии**: осуществление их обработки допускается лишь при условии принятия комплекса мер, направленных на предупреждение рисков, которые могут возникнуть при этом для прав и свобод субъектов персональных данных (п.3 ст.8 Закона № 99-З).

- Кроме того, выделяется такая категория персональных данных, как **общедоступные** - **это персональные данные, распространенные самим субъектом персональных данных либо с его согласия или распространенные в соответствии с требованиями законодательных актов** (абз.7 ст.1 Закона № 99-З).

- Если, например, специальные персональные данные сделаны общедоступными самим субъектом персональных данных, то согласие на их обработку не требуется (абз.2 п.2 ст.8 Закона № 99-З).

Информация не для распространения

- **К информации, распространение и (или) предоставление которой ограничено, относятся** (ч. 1 ст. 17 Закона № 455-З):
  - информация о частной жизни физического лица и персональные данные;
  - сведения, составляющие государственные секреты;
  - служебная информация ограниченного распространения;
  - информация, составляющая коммерческую, профессиональную, банковскую и иную охраняемую законом тайну;
  - информация, содержащаяся в делах об административных правонарушениях, материалах и уголовных делах органов уголовного преследования и суда до завершения производства по делу;
  - иная информация, доступ к которой ограничен законодательными актами Республики Беларусь.

***Закон РБ № 455-З**. Об информации, информатизации и защите информации.*

Информация не для распространения

- При этом **никто не вправе требовать от физического лица предоставления информации** о его частной жизни и персональных данных, включая сведения, составляющие личную и семейную тайну, тайну телефонных переговоров, почтовых и иных сообщений, касающиеся состояния его здоровья, либо получать такую информацию иным образом помимо воли данного физического лица, кроме случаев, установленных законодательными актами Республики Беларусь (ч. 1 ст. 18 Закона № 455-З).

***Закон РБ № 455-З**. Об информации, информатизации и защите информации.*

Обработку каких данных не регулирует Закон № 99-З

- **Из сферы действия Закона № 99-З исключены отношения, касающиеся случаев обработки персональных данных, отнесенных в установленном порядке к государственным секретам** (п.2 ст.2 Закона № 99-З).

- Кроме того, требования Закона № 99-З могут не соблюдаться при обработке персональных данных физическими лицами в процессе исключительно личного, семейного, домашнего и иного подобного их использования, не связанного с профессиональной или предпринимательской деятельностью (п.2 ст.2 Закона № 99-З).

- Во всех остальных случаях обработка персональных данных требует учитывать положения Закона № 99-З. Кроме того, если законодательным актом, устанавливающим правовой режим охраняемой законом тайны, предусматриваются особенности обработки персональных данных, входящих в состав охраняемой законом тайны, применяются положения этого законодательного акта (п.3 ст.3 Закона № 99-З).

Права субъектов

1. на отзыв согласия на обработку ПД (ст. 10)
2. на получение информации, касающейся обработки ПД (ст. 11)
3. на получение информации о предоставлении ПД третьим лицам (ст. 12)
4. требовать внесения изменений в ПД (ст. 11)
5. требовать прекращения обработки ПД и (или) их удаления (ст. 13)
6. на обжалование действий (бездействия) и решений оператора, связанных с обработкой ПД (ст. 15)
7. на возмещение морального вреда, причинённого незаконной обработкой ПД (ст. 19)

Реализация прав субъекта персональных данных

- **Права субъекта персональных данных реализуются путем подачи заявления оператору.**
- В случае направления заявления субъекта персональных данных для реализации своих прав уполномоченному лицу, последний не обязан отвечать на данный запрос.
- Вместе с тем, ответ уполномоченным лицом на заявление субъекта персональных данных не будет противоречить законодательству о персональных данных.

Срок ответа субъекту персональных данных

- **Порядок подачи** заявления субъектом персональных данных оператору установлен в статье 14 Закона.
- **Для реализации прав**, предусмотренных статьями 10 – 13 Закона, субъекту персональных данных необходимо подать оператору заявление в письменной форме либо в виде электронного документа в котором указано большое количество персональных данных.
- **Срок ответа** на заявление зависит от реализуемого субъектом персональных данных права (часть первая пункта 2 статьи 10, пункт 2, часть вторая пункта 4 статьи 11, пункт 2 статьи 12, часть первая пункта 2 статьи 13 Закона):

Реализуемое право субъекта персональных данных	**Срок ответа субъекту персональных данных**
Отзыв согласия	15 дней после получения заявления
Получение информации об обработке персональных данных	5 дней после получения заявления
Внесение изменений в персональные данные	15 дней после получения заявления
Получение информации о предоставлении персональных данных третьим лицам	15 дней после получения заявления
Прекращение обработки персональных данных (их удаление)	15 дней после получения заявления

Организация подпадает под действие закона если

- **Если в организации происходит сбор персональных данных:**
  - заполнение анкет и проведение опросов;
  - составление договоров (гражданско-правовые, трудовые), получение заявлений;
  - сбор информации на сайте компании о пользователях с помощью куки-файлов;
  - данные приложения или иного продукта (геолокация, изображения и иные данные пользователей);
  - операции с любыми данными о любом человеке в ходе любой деятельности.
- **то она подпадает под действие закона № 99-З**

Категории субъектов: оператор и уполномоченное лицо

- Закон № 99-З вводит две новые **категории субъектов** в сфере обработки и защиты персональных данных: **оператор и уполномоченное лицо**.
- Любой субъект, который самостоятельно или совместно с кем-либо организует и (или) осуществляет обработку персональных данных, является оператором (абз.8 ст.1 Закона № 99-З).

Справочно

Закон № 99-З приводит следующий перечень операторов:

государственный орган,

юридическое лицо Республики Беларусь,

иная организация,

физическое лицо, в том числе индивидуальный предприниматель.

Категории субъектов: оператор и уполномоченное лицо

- **По сути, оператором может стать любое лицо, которое осуществляет обработку персональных данных** в связи с профессиональной или предпринимательской деятельностью. **При этом не важно, как именно обрабатываются данные: с помощью автоматизированных средств или без них** (например, картотеки, списки и т. п.) (п.1 ст.2 Закона № 99-З).

- При этом законодатель признает, что не всегда непосредственную обработку данных (или часть действий с ними) осуществляет оператор. В этой связи введена такая категория как **уполномоченное лицо - субъект, который осуществляет обработку персональных данных от имени оператора или в его интересах** в соответствии с актом законодательства или на основании договора (абз.16 ст.1 Закона № 99-З).

Согласие на обработку персональных данных

- Закон № 99-З **сохраняет возможность фиксации дачи согласия в письменной форме, в виде электронного документа или в иной электронной форме** (например, введение подтверждающего кода из смс-сообщения, проставление отметки «я согласен» в соответствующей форме на сайте и т. п.) (п.3 ст.5 Закона № 99-З)

Согласие на обработку персональных данных

- **Важно!** **Согласие субъекта персональных данных** - это свободное, однозначное, информированное выражение его воли (п.1 ст.5 Закона № 99-З).

- Исходя из практики реализации схожих норм за рубежом, **согласие не будет считаться полученным**:
  - если лицу не была дана полная и понятная информация об обработке данных;
  - если лицо было вынуждено дать согласие, чтобы воспользоваться определенной услугой (хотя сама по себе эта услуга не требует использования персональных данных);
  - если невозможно достоверно установить наличие согласия (например, когда согласием на обработку считается использование лицом сервиса).

Согласие на обработку персональных данных

- **Субъект персональных данных имеет право в любое время без объяснения причин отозвать свое согласие на обработку данных**, а если такое согласие не давалось (либо отсутствуют иные законные основания для обработки) - потребовать прекращения их обработки и (или) удаления (п.1 ст.10 Закона № 99-З).

- При этом **отзыв согласия действует только на будущее время**: персональные данные, которые обрабатывались пока действовало согласие, считаются обрабатывавшимися на законной основе (а соответствующие материалы, в которых могли бы быть зафиксированы данные лица, не подлежат изъятию из гражданского оборота) (п.4 ст.10 Закона № 99-З).

Согласие на обработку персональных данных

- Субъект персональных данных имеет право получить информацию о том, какие данные о нем имеются у оператора, а также потребовать корректировки сведений о себе (пп.1-4 ст.11 Закона № 99-З).

- Один раз в году можно также на безвозмездной основе получить информацию о том, кому (каким третьим лицам) предоставлялись персональные данные субъекта (абз.1 п.1 ст.12 Закона № 99-З).

- Субъект персональных данных вправе обжаловать действия (бездействие) и решения оператора, нарушающие его права при обработке персональных данных, в уполномоченный орган по защите прав субъектов персональных данных, а далее - в суд (ст.15 Закона № 99-З).

Справочно

Пример письменного согласия на обработку персональных данных содержится в приложении 8 к Инструкции о порядке выписывания рецепта врача и создания электронных рецептов врача, утвержденной постановлением Минздрава от 31.10.2007 № 99.

Приложение 8
к Инструкции о порядке выписки
рецепта врача и создания
электронных рецептов врача
(в редакции постановления
Министерства здравоохранения
Республики Беларусь
17.06.2019 № 60)

Форма

Письменное согласие пациента (уполномоченного лица)
на обработку персональных данных

Я, _____
(фамилия, собственное имя, отчество (если таковое имеется)
документ, удостоверяющий личность: _____
серия _____ номер _____ кем выдан _____,
дата выдачи «___» _____ ____ г., проживающий по адресу: _____
_____,
номер медицинской карты амбулаторного пациента: _____,
даю согласие на обработку персональных данных и информации, составляющей врачебную тайну, в информационных системах, информационных ресурсах, базах (банках) данных в здравоохранении.

Мне разъяснено, что персональные данные будут переданы на хранение в автоматизированную информационную систему «Электронный рецепт».

_____ _____ _____
(дата) (подпись) (инициалы, фамилия)

Обязанности операторов

Обязанность	Норма Закона № 99-З
1. Обеспечивать на всех этапах обработки персональных данных справедливое соотношение интересов всех заинтересованных лиц	Пункт 2 ст.4
2. Обеспечивать соразмерность обработки персональных данных заявленным целям их обработки	Пункт 2 ст.4
3. При изменении целей обработки персональных данных получать на это отдельное согласие	Пункт 4 ст.4
4. Принимать меры по обеспечению достоверности обрабатываемых им персональных данных, при необходимости обновлять их (а также корректировать по запросам субъектов данных)	Пункт 7 ст.4, п.1 ст.16
5. Хранить персональные данные не дольше, чем это требуют заявленные цели обработки	Пункт 8 ст.4
6. Предоставлять субъекту данных информацию обо всех условиях обработки персональных данных. **Важно!** Рекомендуется разработать стандартные формы для различных категорий персональных данных	Абзацы 2, 5 п.1 ст.16

Обязанности операторов

Обязанность	Норма Закона № 99-З
7. Предоставлять пользователю отдельный документ (в письменном или электронном виде), в котором простым и ясным языком разъяснить субъекту данных его права, связанные с обработкой персональных данных, механизм реализации таких прав, а также последствия дачи согласия субъекта персональных данных или отказа в даче такого согласия	Часть 2 п.5 ст.5
8. Получать согласие на обработку персональных данных от субъектов данных. **Важно!** Рекомендуется обеспечить фиксацию и хранение соответствующих данных, так как согласно п.7 ст.5 Закона № 99-З обязанность доказывания получения согласия субъекта персональных данных возлагается на оператора	Абзац 3 п.1 ст.16
9. Обеспечивать защиту персональных данных	Абзац 4 п.1 ст.16
10. При обработке специальных персональных данных принимать комплекс мер, направленных на предупреждение рисков, которые могут возникнуть при этом для прав и свобод субъектов персональных данных	Пункт 3 ст.8

Обязанности операторов

Обязанность	Норма Закона № 99-З
11. Соблюдать процедуры и условия трансграничной передачи данных	Статья 9
12. При получении заявления от субъекта персональных данных при наличии установленных оснований прекратить обработку данных, осуществить их удаление (или, в зависимости от технических возможностей, блокирование) и уведомить субъекта об этом	Абзац 7 п.1 ст.16
13. По запросу субъекта персональных данных предоставлять ему в доступной форме информацию о том, какие его данные обрабатываются и как (категории, сроки, источники и т. п.), кому они передавались	Абзац 5 п.1 ст.16
14. В установленном порядке уведомлять уполномоченный орган по защите прав субъектов персональных данных о нарушениях систем защиты персональных данных	Абзац 8 п.1 ст.16
15. Выполнять указания уполномоченного органа по защите прав субъектов персональных данных по изменению, блокированию или удалению недостоверных или полученных незаконным путем персональных данных	Абзац 9 п.1 ст.16

Меры по защите персональных данных

- Особое внимание законодатель уделяет мерам по защите персональных данных (ст.17 Закона № 99-З).
- **Оператор (уполномоченное лицо) обязан принимать правовые, организационные и технические меры по обеспечению защиты персональных данных от несанкционированного или случайного доступа к ним, изменения, блокирования, копирования, распространения, предоставления, удаления персональных данных, а также от иных неправомерных действий в отношении персональных данных** (п.1 ст.17 Закона № 99-З).

Алгоритм приведения деятельности операторов, уполномоченных лиц в соответствие с требованиями

1. Назначение структурного подразделения или лица, ответственного за осуществление внутреннего контроля за обработкой персональных данных, определение его должностных обязанностей, утверждение положения об организации внутреннего контроля за обработкой персональных данных.

2. Выявление и фиксация бизнес-процессов, в которых используются персональные данные.

3. Анализ бизнес-процессов, в которых используются персональные данные, на предмет соответствия требованиям законодательства о персональных данных.

4. Издание документов, определяющих политику в отношении обработки персональных данных и обеспечение неограниченного доступа, в том числе с использованием глобальной компьютерной сети Интернет к данной политике.

5. Разработка иных (кроме определяющих политику в отношении персональных данных) документов:

6. Внесение изменений в должностные обязанности лиц, обрабатывающих персональные данные.

7. Ознакомление работников и иных лиц, непосредственно осуществляющих обработку персональных данных, с положениями законодательства о персональных данных.

8. Обучение лиц, непосредственно осуществляющих обработку персональных данных, и лиц, ответственных за осуществление внутреннего контроля за обработкой персональных данных.

9. Реализация организационных и технических мер.

10. Осуществление технической и криптографической защиты персональных данных в соответствии с классификацией информационных ресурсов (систем), содержащих персональные данные.

У компании появляется ряд обязательств по защите персональных данных

1. **Назначить** лицо или отдел, ответственные за защиту персональных данных в компании.

2. **Разработать** политику компании в отношении обработки персональных данных и сделать ее доступной для неограниченного круга лиц (в том числе посредством сети Интернет).

3. **Провести** обучение работников работе с персональными данными.

4. **Установить** порядок доступа к персональным данным.

5. **Осуществлять** техническую и криптографическую защиту персональных данных.

Алгоритм действий оператора по защите персональных данных физических лиц

Этап 1

- **Предоставление** субъектам персональных данных необходимой информации до получения их согласий на обработку персональных данных

Этап 2

- **Разъяснение** субъектам персональных данных их прав, связанных с обработкой персональных данных

Этап 3

- **Получение** письменных согласий субъектов персональных данных на обработку их персональных данных, за исключением случаев, предусмотренных законодательством Республики Беларусь

Алгоритм действий оператора по защите персональных данных физических лиц

Этап 4

- **Назначение** структурного подразделения или лица, ответственного за осуществление внутреннего контроля за обработкой персональных данных

Этап 5

- **Издание** документов, определяющих политику оператора в отношении обработки персональных данных

Этап 6

- **Ознакомление** работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства о персональных данных

Алгоритм действий оператора по защите персональных данных физических лиц

Этап 7

- **Установление** порядка доступа к персональным данным, в том числе обрабатываемым в информационном ресурсе (системе)

Этап 8

- **Осуществление** технической и криптографической защиты персональных данных в порядке, установленном Оперативно-аналитическим центром при Президенте Республики Беларусь, в соответствии с классификацией информационных ресурсов (систем), содержащих персональные данные

Этап 9

- **Обеспечение** неограниченного доступа, в том числе с использованием глобальной компьютерной сети Интернет, к документам, определяющим политику оператора в отношении обработки персональных данных, до начала такой обработки

Алгоритм действий оператора по защите персональных данных физических лиц

Этап 10

- **Прекращение** обработки персональных данных при отсутствии оснований для их обработки

Этап 11

- **Незамедлительное уведомление** уполномоченного органа по защите прав субъектов персональных данных о нарушениях систем защиты персональных данных

Этап 12

- **Осуществление** изменения, блокирования, удаления недостоверных или полученных незаконным путем персональных данных

Алгоритм действий оператора по защите персональных данных физических лиц

Этап 13

- **Ограничение** обработки персональных данных достижением конкретных, заранее заявленных законных целей

Этап 14

- **Осуществление** хранения персональных данных в форме, позволяющей идентифицировать субъектов персональных данных, не дольше, чем этого требуют заявленные цели обработки персональных данных

Этап 15

- **Прекращение** обработки персональных данных и их удаление

Ответственность в сфере защиты персональных данных

- **За ненадлежащую защиту персональных данных законом предусмотрена:**
  - Дисциплинарная ответственность
  - Административная ответственность
  - Уголовная ответственность

В соответствии со статьей 19 Закона Республики Беларусь ”О защите персональных данных“ лица, виновные в нарушении настоящего Закона, несут ответственность, предусмотренную законодательными актами.
Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, установленных настоящим Законом, подлежит возмещению. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

Дисциплинарная ответственность

- **Статья 47 ТК (с 29.06.2021)**
- Трудовой договор с работником может быть прекращен в случаях нарушения им порядка сбора, систематизации, хранения, изменения, использования, обезличивания, блокирования, распространения, предоставления, удаления персональных данных.

- Кроме того, за нарушение должностных обязанностей в сфере обработки персональных данных может наступать также дисциплинарная ответственность и другие меры ответственности, предусмотренные Трудовым кодексом.

Административная ответственность

- **Статья 23.7 КоАП (с 01.03.2021)**

- Умышленные незаконные **сбор, обработка, хранение или предоставление** персональных данных физического лица либо **нарушение его прав**, связанных с обработкой персональных данных, влекут штраф до 50 БВ (ч.1 ст.23.7 КоАП).

- Деяния, предусмотренные ч.1 ст.23.7 КоАП, совершенные лицом, которому персональные данные известны в связи с его профессиональной или служебной деятельностью, влекут штраф от 4 до 100 БВ (ч.2 ст.23.7 КоАП).

- Умышленное незаконное **распространение** персональных данных физических лиц влечет штраф до 200 БВ (ч.3 ст.23.7 КоАП).

- Несоблюдение мер **обеспечения защиты** персональных данных физических лиц влечет штраф от 2 до 10 БВ, на ИП - от 10 до 25 БВ, а на юрлицо - от 20 до 50 БВ (ч.4 ст.23.7 КоАП)

Кодекс Республики Беларусь «Об административных правонарушениях» https://pravo.by/document/?guid=3871&p0=HK2100091

Размер БАЗОВОЙ ВЕЛИЧИНЫ в РБ

Дата, с которой установлен размер базовой величины	Размер базовой величины (руб.)	Нормативный акт, установивший размер базовой величины
01.01.2024	**40,00**	**Постановление Совмина от 27.12.2023 №944**
01.01.2023	37,00	Постановление Совмина от 30.12.2022 №967
01.01.2022	32,00	Постановление Совмина от 31.12.2021 №792
01.01.2021	29,00	Постановление Совмина от 30.12.2020 №783
01.01.2020	27,00	Постановление Совмина от 13.12.2019 №861
01.01.2019	25,50	Постановление Совмина от 27.12.2018 №956
01.01.2018	24,50	Постановление Совмина от 22.12.2017 №997
01.01.2017	23,00	Постановление Совмина от 28.11.2016 №974

https://belarusbank.by/ru/33139/press/spravochno/bazovaya_velichina

Уголовная ответственность

- **Сейчас в ст. 179 УК предусмотрена ответственность только за незаконное предоставление сведений о частной жизни (личная или семейная тайна)**, и не упоминаются персональные данные.

- Кроме того, **уголовная ответственность предусмотрена за :**
  - разглашение тайны усыновления (удочерения) (ст.177 УК);
  - разглашение врачебной тайны (ст.178 УК).

Уголовная ответственность

- **Статья 203. Нарушение тайны переписки, телефонных переговоров, телеграфных или иных сообщений**
- **1. Умышленное незаконное нарушение тайны переписки, телефонных или иных переговоров**, почтовых, телеграфных или иных сообщений граждан – наказывается общественными работами, или штрафом, или исправительными работами на срок **до одного года**, или арестом.
- 2. **То же деяние, совершенное с использованием специальных технических средств**, предназначенных для негласного получения информации, либо должностным лицом с использованием своих служебных полномочий, – наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом, или лишением свободы на срок **до двух лет**.

Уголовная ответственность

- **Статья 203. Незаконные действия в отношении информации о частной жизни и персональных данных**
- **1. Умышленные незаконные сбор, предоставление информации о частной жизни и (или) персональных данных другого лица без его согласия**, повлекшие причинение существенного вреда правам, свободам и законным интересам гражданина, – наказываются общественными работами, или штрафом, или арестом, или ограничением свободы на срок **до двух лет**, или лишением свободы на тот же срок.
- **2. Умышленное незаконное распространение информации о частной жизни и (или) персональных данных другого лица без его согласия**, повлекшее причинение существенного вреда правам, свободам и законным интересам гражданина, – наказывается ограничением свободы на срок **до трех лет** или лишением свободы на тот же срок со штрафом.
- **3. Действия, предусмотренные частями 1 или 2 настоящей статьи, совершенные в отношении лица или его близких в связи с осуществлением им служебной деятельности или выполнением общественного долга**, – наказываются ограничением свободы на срок **до пяти лет** или лишением свободы на тот же срок со штрафом.

Уголовная ответственность

- **Статья 203. Несоблюдение мер обеспечения защиты персональных данных**

- **Несоблюдение мер обеспечения защиты персональных данных** лицом, осуществляющим обработку персональных данных, повлекшее по неосторожности их распространение и причинение тяжких последствий, – наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или исправительными работами на срок **до одного года**, или арестом, или ограничением свободы на срок **до двух лет**, или лишением свободы на срок **до одного года**.

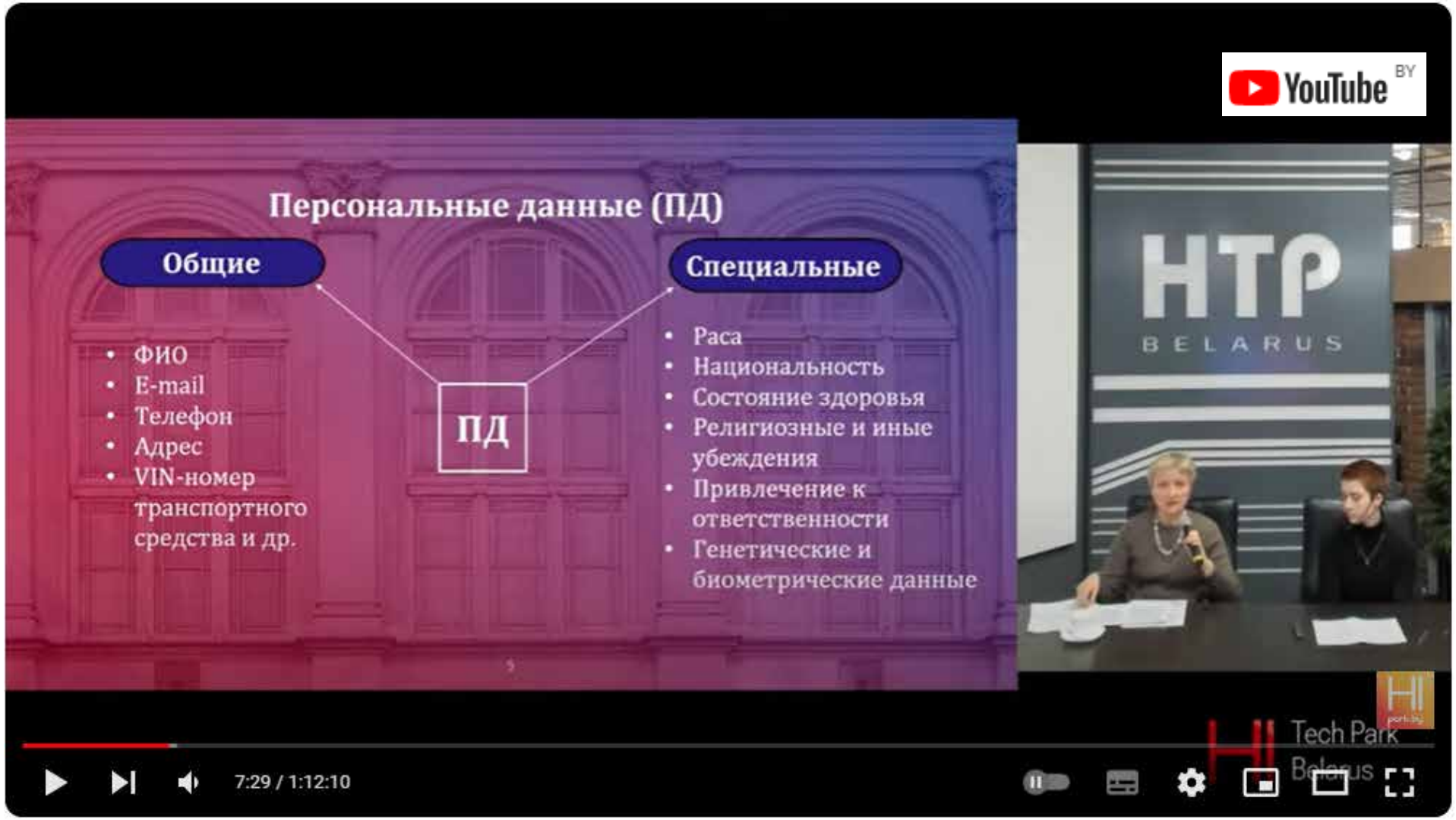
Дополнительные материалы

Белорусские и мировые тренды развития законодательств о приватности (май 2021)
https://www.youtube.com/watch?v=kYh6Mfd2k6w

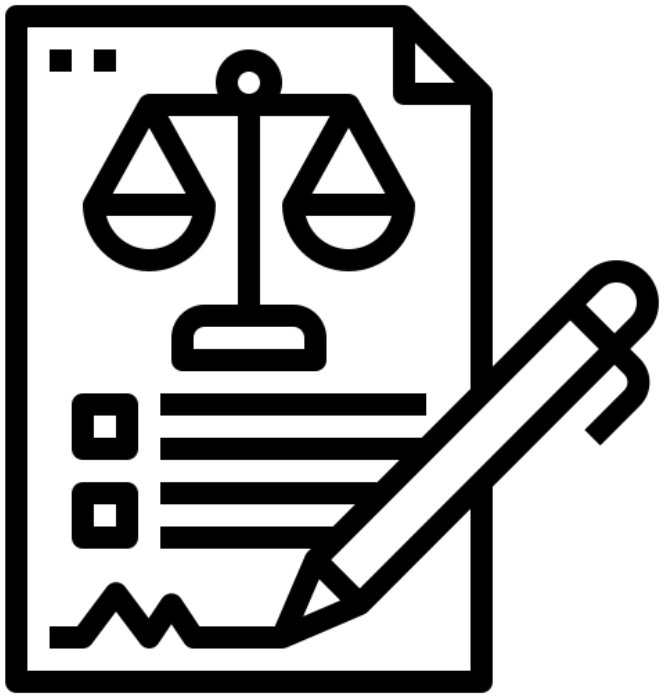
Дополнительные материалы

Персональные данные и репутация компаний: показательные кейсы. (август 2021)
https://www.youtube.com/watch?v=Yq1d1yJKoPg

Дополнительные материалы



Защита персональных данных - Анастасия Малахова и Екатерина Орочко (14 марта 2024)
https://www.youtube.com/watch?v=bXE3YcCG9sU



Защита персональных данных в Российской Федерации

Защита персональных данных

- **Категория защиты персональных данных тесно связана с таким фундаментальным правом человека, как право на защиту неприкосновенности частной жизни**, что прямо указывается в ст. 2 Федерального закона от 27 июля 2006 г. **№ 152-ФЗ «О защите персональных данных».**
- **Хотя не всегда право на защиту персональных данных по своему объему совпадает с правом на защиту неприкосновенности частной жизни**, положения его закрепляющие, а также некоторые положения гарантирующие иные основные права и свободы в Конституции РФ по существу включают и право на защиту персональных данных.

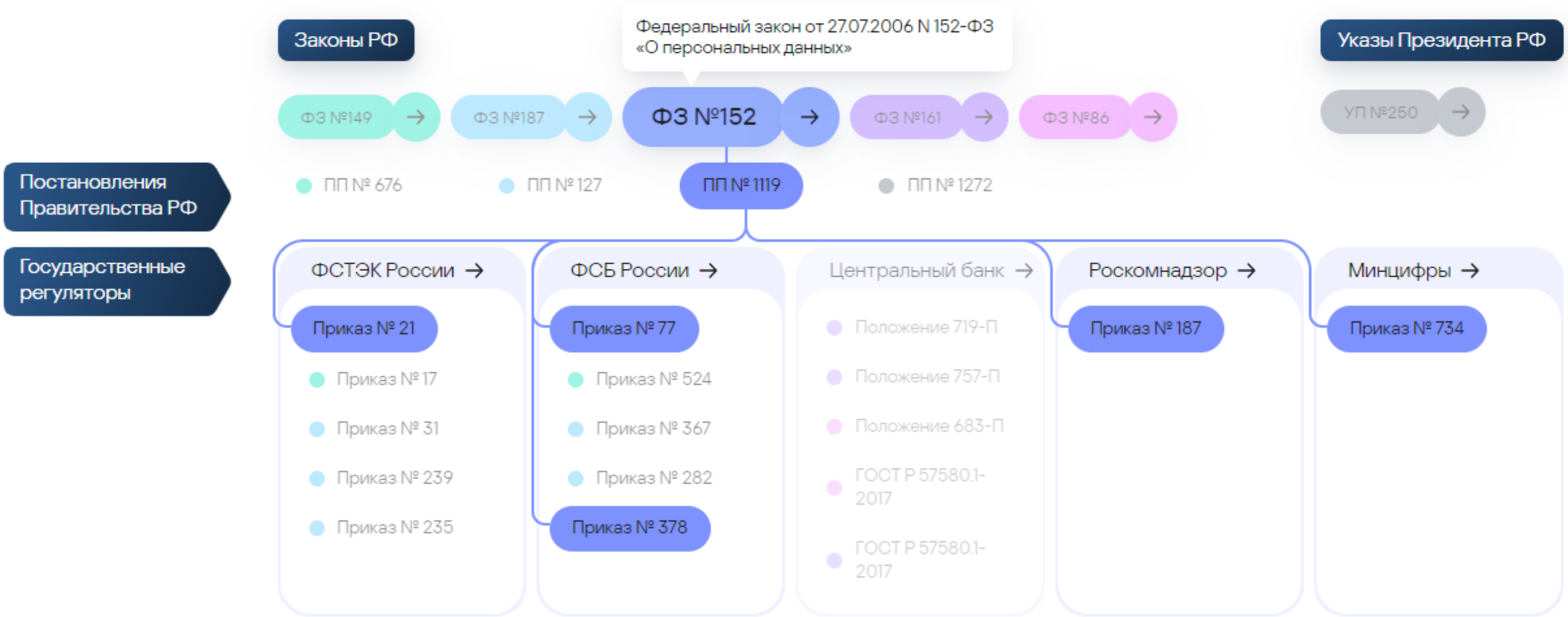
Конституция РФ

- В тексте Конституции РФ, помимо **отсутствия явно выраженного права на защиту персональных данных, обнаруживается непоследовательность в соответствующих положениях**.
- Так, в случае **ч. 2 ст. 23** Конституция предоставляет широкую защиту коммуникаций человека – «**право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений**».
- А **в ч. 1 ст. 24 закреплено требование получения согласия лица при обработке информации о его частной жизни** (Сбор, хранение, использование и распространение информации **о частной жизни** лица без его согласия не допускаются), пределы которой не являются объективными: как неоднократно указывал Конституционный Суд РФ в своих решениях: «лишь само лицо вправе определить, какие именно сведения, имеющие отношение к его частной жизни, должны оставаться в тайне».
- Похожая на положение ч. 1 ст. 24 Конституции РФ формулировка возведена также и в принцип регулирования отношений в сфере информации, информационных технологий и защиты информации (п. 7 ст. 3 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»).

Документы по Защите персональных данных в РФ

- Документы по персональным данным в Российской Федерации
  - **Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»**
    http://www.consultant.ru/document/cons_doc_LAW_61801/
  - Постановление Правительства РФ от 29 июня 2021 г. № 1046 «**О федеральном государственном контроле (надзоре) за обработкой персональных данных**»
    https://www.garant.ru/products/ipo/prime/doc/401316524/
  - Приказ Роскомнадзора от 24.02.2021 № 18 «**Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения**»
    http://publication.pravo.gov.ru/Document/View/0001202104210039
  - Федеральный закон от 8 июня 2020 г. № 168-ФЗ «**О едином федеральном информационном регистре, содержащем сведения о населении Российской Федерации**»
    https://www.garant.ru/products/ipo/prime/doc/74132857/
  - Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «**Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных**»
    https://zags.mosreg.ru/upload/iblock/095/postanovlenie-ot-01.11.2011.doc
  - Федеральный закон от 27 июля 2006 г. № 149-ФЗ «**Об информации, информационных технологиях и о защите информации**»
    http://www.kremlin.ru/acts/bank/24157
  - **Сервис Роскомнадзора** для операторов персональных данных (ПД), **позволяющий сформировать шаблон формы согласия на обработку ПД**, разрешенных субъектом для распространения.
    https://rkn.gov.ru/news/rsoc/news73724.htm
  - Приказом ФСТЭК России от 18.02.2013 N 21 "**Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных**"
  - Приказ ФСБ России от 10.07.2014 N 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**"

Документы по Защите персональных данных в РФ



ФЗ №152

Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных»

https://regulhub.kaspersky.ru/laws/fz-152

Документы по Защите персональных данных в РФ

https://www.sps-ib.ru/materialy:pdn

СПРАВОЧНО-ПРАВОВАЯ СИСТЕМА
ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Новости

Рубрикатор PDF

Вы находитесь здесь: start » Информационно-аналитические материалы » **Персональные данные**

Персональные данные

Общие положения

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). С перечнем категорий персональных данных можно ознакомиться здесь.

Содержание

- Персональные данные
  - Общие положения
  - Нормативные правовые акты, стандарты и рекомендации
  - Надзорные органы
  - Аналитические материалы и комментарии

В Российской Федерации этот вид тайн регулируется с 1997 года после принятия Указа Президента РФ от 06.03.1997 № 188 "Об утверждении Перечня сведений конфиденциального характера". В связи с вступлением в силу Федерального закона от 27.07.2006 №152-ФЗ "О персональных данных", а особенно после внесения в него неоднократных изменений, внимание к сфере персональных данных только усиливается. Продолжают подвергаться изменениям нормативные правовые акты различных уровней, а защите персональных данных государственных служащих теперь посвящены отдельные ведомственные акты. В разработанных стандартах по ИБ для персональных данных выделены отдельные разделы.

Подтверждением актуальности данной темы являются также многочисленные информационные (разъяснительные) письма регуляторов по вопросам, возникающим у операторов персональных данных в процессе реализации требований действующего законодательства (в частности, о необходимости получения лицензий ФСТЭК России и ФСБ России, использовании сертифицированных средств защиты конфиденциальной информации). Кроме того, на сегодняшний день уже существует судебная практика, которая формируется не только на основании материалов проверок Роскомнадзора, но и по результатам рассмотрения исковых заявлений субъектов персональных данных.

Каталог категорий персональных данных

https://www.sps-ib.ru/analitika:katalog_pdn

СПРАВОЧНО-ПРАВОВАЯ СИСТЕМА
ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Новости

Рубрикатор PDF

Вы находитесь здесь: start » analitika » Каталог категорий персональных данных

Каталог категорий персональных данных

Кто ясно мыслит, тот ясно излагает.

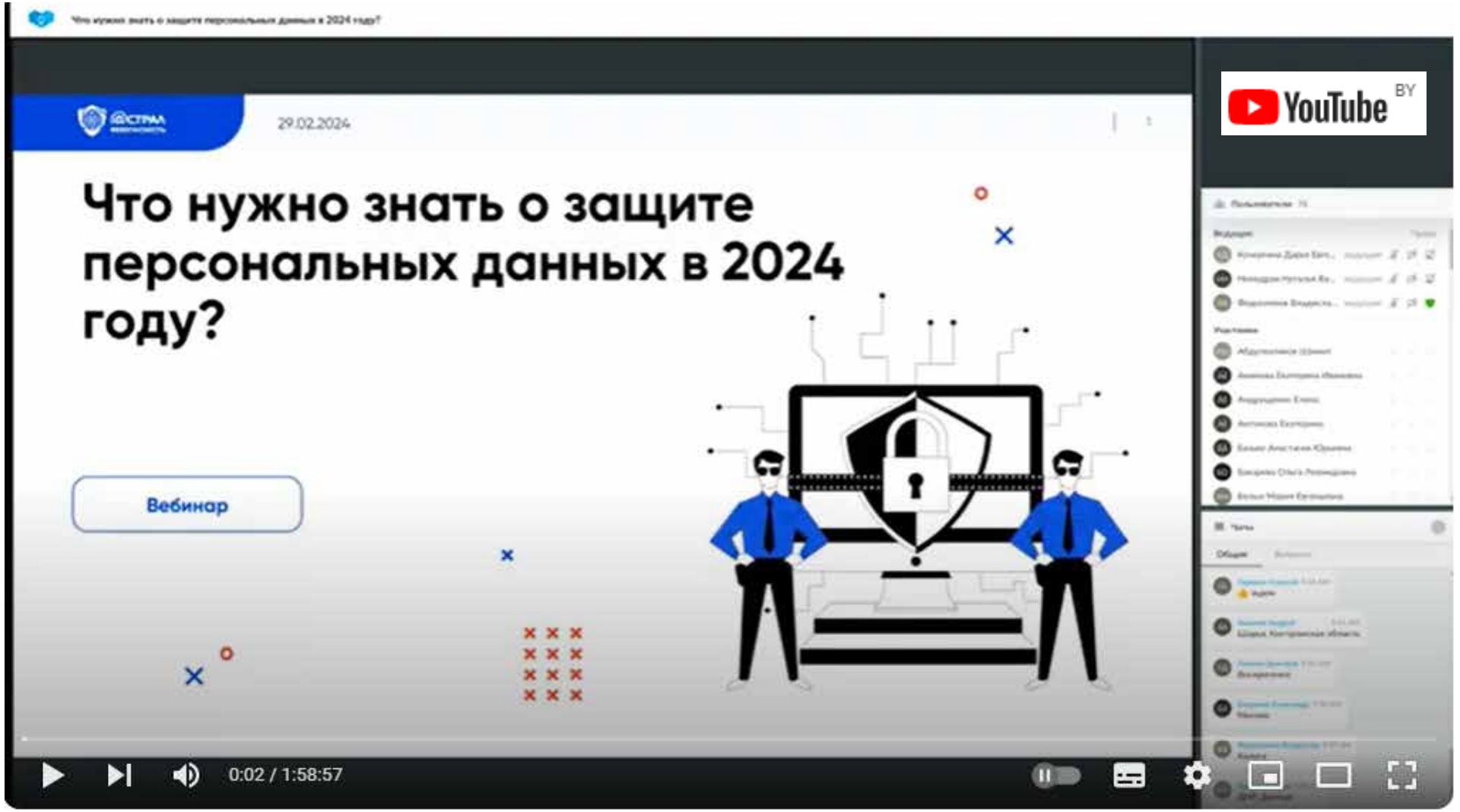
В данном материале представлен итог аналитической работы по идентификации и описанию категорий персональных данных субъектов, обрабатываемых операторами для достижения соответствующих целей. В настоящий момент каталог содержит указание на 304 категории персональных данных, сгруппированных в 21 тематическом разделе. Содержание каталога регулярно актуализируется и дополняется[1)].

Необходимость такой работы продиктована следующими причинами:

1. Понятие персональных данных, закрепленное в п.1 ст.3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», может трактоваться максимально широко, а в действующем законодательстве Российской Федерации отсутствует как систематизированное указание категорий персональных данных, так и нормативно зафиксированные правила определения перечня персональных данных. Таким образом, ставится под сомнение фактическая реализация принципа формальной определенности[2)] по отношению нормативно закрепленному понятию «персональные данные».
2. Результаты деятельности рабочей группы по определению «матрицы персональных данных», созданной в рамках

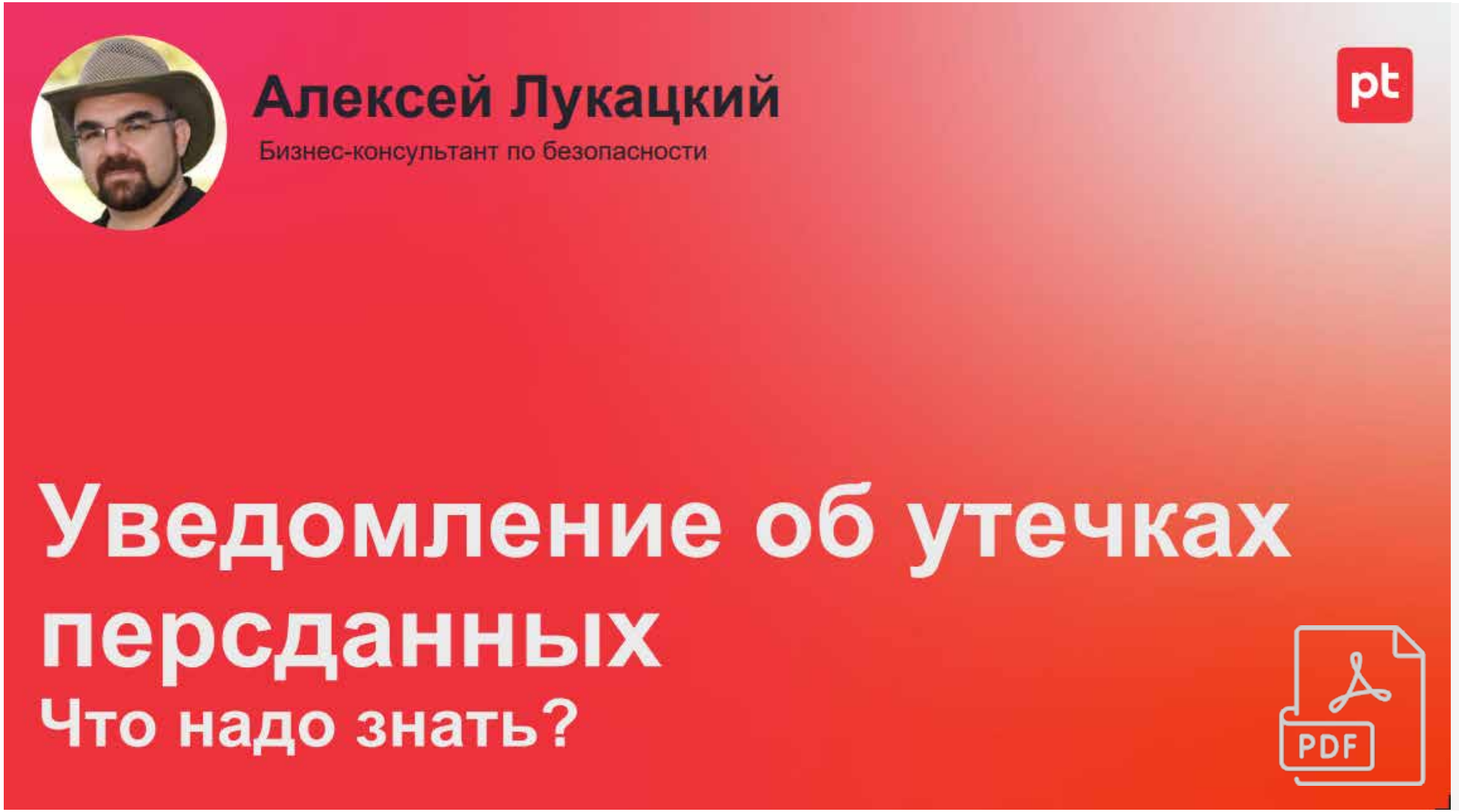
Содержание

Дополнительные материалы

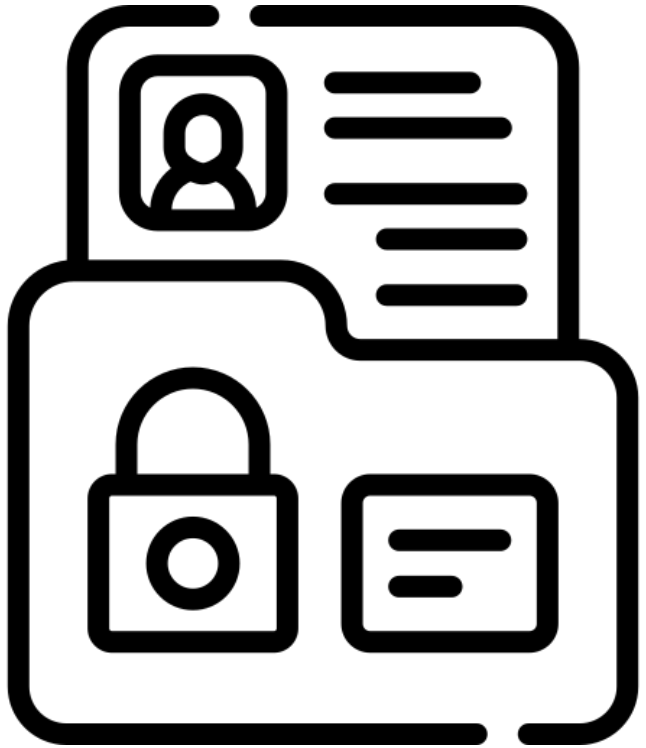


Что нужно знать о защите персональных данных в 2024 году (март 2024)
https://www.youtube.com/watch?v=KfJSg4cXeGk

Дополнительные материалы

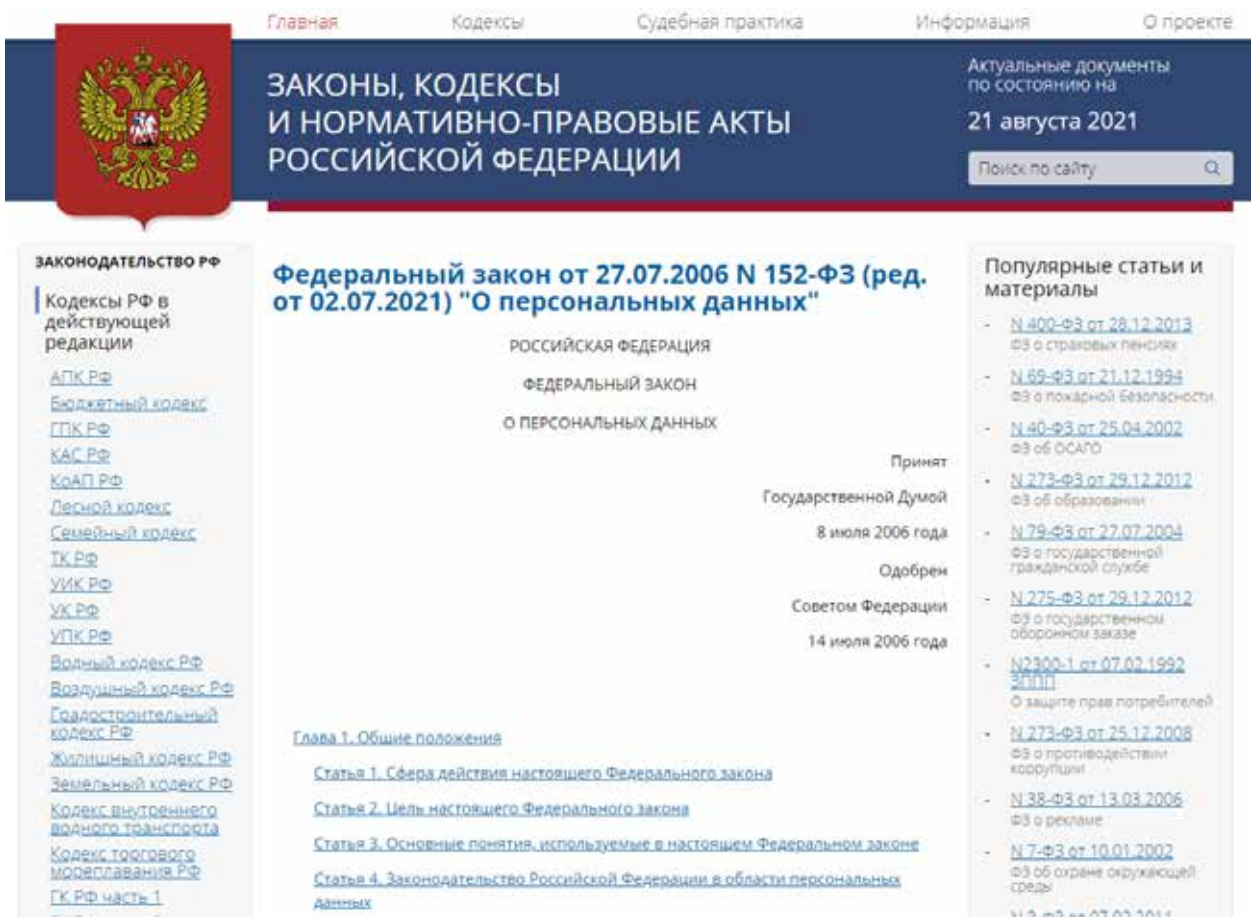


https://www.ptsecurity.com/upload/corporate/ru-ru/webinars/ics/uvedomlenie-ob-utechkah.pdf



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

Федеральный закон РФ от 27.07.2006 N 152-ФЗ «О персональных данных»



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

http://www.consultant.ru/document/cons_doc_LAW_61801/

https://legalacts.ru/doc/152_FZ-o-personalnyh-dannyh/

http://www.kremlin.ru/acts/bank/24154

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

- **Федеральный закон № 152-ФЗ «О персональных данных»** — это отдельный закон о персональных данных в Российской Федерации.
  http://www.kremlin.ru/acts/bank/24154
  http://www.consultant.ru/document/cons_doc_LAW_61801/

- **Он касается их обработки, хранения и доступа к ним.**

- **Цель этого закона** — 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 Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных»

- **Статья 1. Сфера действия настоящего Федерального закона**
- 1. **Настоящим Федеральным законом регулируются отношения, связанные с обработкой персональных данных**, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами (далее - государственные органы), органами местного самоуправления, иными муниципальными органами (далее - муниципальные органы), юридическими лицами и 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.

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

- **Статья 1. Сфера действия настоящего Федерального закона**
- 2. Действие настоящего Федерального закона **не распространяется** на отношения, возникающие при:
  - 1) **обработке персональных данных физическими лицами исключительно для личных и семейных нужд**, если при этом не нарушаются права субъектов персональных данных;
  - 2) организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других **архивных документов** в соответствии с законодательством об архивном деле в Российской Федерации;
  - 3) обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим **государственную тайну**;

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

- **Любые данные о человеке можно публиковать только с его прямого согласия!**

- Согласие не всегда должно быть в письменной форме. Допускается любая форма, позволяющая подтвердить факт его получения.

- **Получение согласия на распространение персональных данных** выполняется в соответствии с Приказом Роскомнадзора «**Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения**» № 18 от 24.02.2021 г., зарегистрированном в Министерстве Юстиции РФ 21 апреля 2021 г.

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

- **Важно!**
- **Статья 15.5** Закона «Об информации..» **позволяет Роскомнадзору по решению суда блокировать сайты**, которые допускают нарушения законодательства в области персональных данных.
- А пункт 14 статьи 10.1 Закона “О персональных данных” **позволяет оспаривать отказ в удалении персональных данных в суде.**

Обезличивание персональных данных

- **Ответственность за не обезличивание персональных данных** теперь несут не только государственные и муниципальные органы власти, но и **все операторы**.
- Невыполнение подобных требований влечет предупреждение или наложение административного штрафа для всех операторов ПДн.

- **обезличивание персональных данных** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

Способы обезличивания персональных данных сотрудников

- Из множества методик, с помощью которых осуществляется обезличивание персональных данных, Роскомнадзор рекомендует применять четыре: метод идентификаторов; метод замены состава информации; метод декомпозиции; метод перемешивания.

Методы обезличивания персональных данных

Суть	Описание
Применение идентификаторов	Часть сведений заменяется идентификаторами - условными обозначениями. Составляется специальная таблица идентификаторов, используемая при расшифровке
Замена семантики или состава информации	Часть сведений, которая не несёт практической пользы для организации, удаляется или обобщается (например, заменяется статистическими данными)
Декомпозиция данных	Массив сведений разбивается на небольшие блоки, которые невозможно использовать по отдельности, поскольку такое применение информации не имеет практического смысла
Перемешивание данных	Сведения перемешивают до тех пор, пока по результату перемешивания невозможно будет установить принадлежность персональных данных конкретному лицу

Штрафы в РФ с 12 декабря 2023 года

- **По общему правилу обработка персональных данных возможна при наличии согласия работника.**
- Федеральный закон от 12 декабря 2023 № 589-ФЗ значительно ужесточил штрафы за обработку персональных данных без письменного согласия.

- За нарушения законодательства РФ в области персональных данных штрафуют по статье 13.11 КоАП РФ.
- В часть 2 и 2.1. данной статьи внесены поправки, которые вступают в силу 23 декабря 2023 года.

- Документ - Федеральный закон от 12 декабря 2023 г. № 589-ФЗ. https://na.buhgalteria.ru/document/n213909

Штрафы в РФ с 12 декабря 2023 года

- С 23 декабря 2023 года **штрафовать за обработку персональных данных без письменного согласия будут так** (ч. 2 ст. 13.11 КоАП РФ)::
  - штраф для граждан – 10 000 до 15 000 рублей;
  - для должностных лиц – от 100 000 до 300 000 рублей;
  - для юрлиц – от 300 000 до 700 000 рублей.

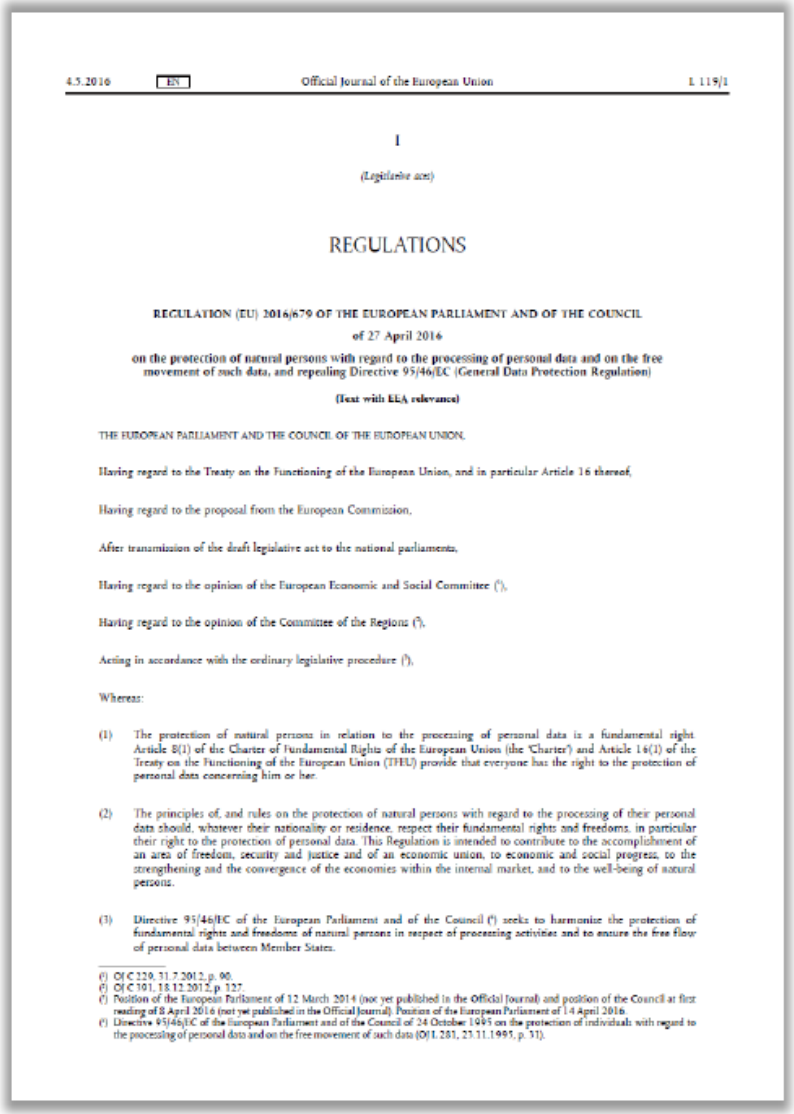
- **За повторное нарушение еще строже** (ч. 2.1 ст. 13.11 КоАП РФ):
  - штраф для граждан – от 15 000 до 30 000 рублей;
  - для должностных лиц – от 300 000 до 500 000 рублей;
  - для ИП – от 500 000 до 1 млн. рублей;
  - для юрлиц – от 1 млн. до 1,5 млн. рублей.

- Как видим в сравнении, **штрафы ужесточили более чем в 10 раз**. Будьте внимательны.

Европейский союз GDPR (General Data Protection Regulation)

GDPR (General Data Protection Regulation) – Общий регламент по защите данных, принятый Европейским союзом для обеспечения согласованного и высокого уровня защиты физических лиц и устранения препятствий для движения потоков персональных данных в рамках Евросоюза

General Data Protection Regulation (GDPR)



4.5.2016 EN Official Journal of the European Union L 119/1

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.

(1) OJ C 229, 31.7.2012, p. 90.
(2) OJ C 391, 18.12.2012, p. 127.
(3) Position of the European Parliament of 12 March 2014 (not yet published in the Official Journal) and position of the Council at first reading of 8 April 2016 (not yet published in the Official Journal). Position of the European Parliament of 14 April 2016.
(4) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

- **General Data Protection Regulation (GDPR)** - это регламент ЕС о защите персональных данных, формирующий обязательные к соблюдению единые принципы и подходы как для государств-членов ЕС, так и для иных государств. 19.04.2018 проведена гармонизация прочтения некоторых положений GDPR на разных языках ЕС.
- **Некоторые факты:**
  - вступил в силу 25.05.2018
  - заменяет собой Директиву 95/46/EC от 24.10.1995
  - гармонизирует правотворчество и правоприменение
  - локальный надзор осуществляется национальными органами стран-участниц Евросоюза по защите данных (Data Protection Authorities)
  - общий надзор осуществляется Европейским советом по защите данных (European Data Protection Board)
  - непосредственно применяется национальными судами государств-членов ЕС и Судом справедливости Евросоюза (European Court of Justice)

General Data Protection Regulation (GDPR)

- **Общий регламент защиты персональных данных (GDPR) Европейского союза**

  - Оригинал на английском - Регламент (EU) 2016/679 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

  - Текст на русском языке - Регламент (EU) 2016/679 https://gdpr-text.com/ru/
  - Текст на русском языке - Директива (EU) 2016/680 https://ogdpr.eu/ru/gdpr-2016-680

  - Разъяснения. Официальные руководства и разъяснения, заключения и рекомендации общеевропейского надзорного органа в области защиты персональных данных (EDPB — Европейского совета по защите персональных данных или Art29WP — Рабочей группы 29-ой статьи). Переводы на русский язык. https://gdpr-text.com/ru/guidelines/

  - Регламент Европейского Парламента и Совета Европейского Союза 2016/679 от 27 апреля 2016 г. «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС» (Общий Регламент о защите персональных данных). (General Data Protection Regulation) (GDPR) http://www.eurasiancommission.org/ru/act/texnreg/depsanmer/consumer_rights/Documents/Регламент%20Европейского%20Парламента%20и%20Совета%20Европейского%20Союза%202016%20679%20от%2027%20апр.pdf

- *В тексте регламента основная часть ссылок идет на стандарт ISO 27701 – Менеджмент персональной информации*

General Data Protection Regulation (GDPR)

Рассмотрение механизмов и специфики применения Генерального регламента ЕС о защите данных (GDPR)

Алексей Мунтян

Редакция от 01.10.2023 – 1057 с. https://rppa.ru/_media/analitika/gdpr_01.10.2023.pdf
Редакция от 29.12.2022 – 822 с. https://rppa.ru/_media/analitika/gdpr_29.12.2022.pdf
Редакция от 05.07.2021 – 532 с. https://rppa.ru/_media/analitika/gdpr_05.07.2021.pdf
Редакция от 28.12.2020 – 444 с. https://rppa.ru/_media/world/gdpr_28.12.2020.pdf
Редакция от 23.12.2019 – 250 с. https://www.sps-ib.ru/gdpr.pdf

General Data Protection Regulation (GDPR)

- **GDPR не определяет каких-либо конкретных средств управления защитой данных**, которые должна использовать организация.
- Компания может сама определять необходимые средства обеспечения безопасности собранных данных, конфиденциальности и управления рисками.

Однако кроме основных требований указанных в регламенте **необходимо выполнять требования ISO 27701**.

ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines
(ISO/IEC 27701:2019 - Расширение до ISO / IEC 27001 и ISO / IEC 27002 для управления информацией о конфиденциальности. Требования и руководящие принципы)

General Data Protection Regulation (GDPR)

- GDPR оказывает влияние на информационно-коммуникационный потенциал предприятий во всём мире, где бы ни находились их серверы.
- **Если компании предоставляют гражданам ЕС любую информацию, контент или услугу в Интернете, GDPR будет оказывать на них влияние.**
- **Регламент будет затрагивать все организации, которые занимаются обработкой данных граждан ЕС независимо от того, является ли компания резидентом ЕС или нет.**
- Регламент GDPR охватывает широкий спектр персональных данных, включая онлайн-идентификаторы, такие как IP-адреса и файлы cookie, а с другой стороны – информацию о кредитной карте и здоровье.

General Data Protection Regulation (GDPR)

- Регламент гарантирует, что **личные данные будут храниться только с прямого разрешения клиента** и использоваться только для той цели, для которой они были получены, а также будут храниться не более, чем это необходимо.
- Кроме того, что **разрешение на использование данных должно быть чётким и понятным**, пользователи имеют право требовать удалять свои данные по запросу.
- Организации должны будут следовать строгим указаниям для обеспечения того, что данные всегда точны и обрабатываются без нарушения закона.
- Если безопасность информации под угрозой, организации должны будут проинформировать об этом соответствующие надзорные органы в течение 72 часов.

General Data Protection Regulation (GDPR)

- **Персональные данные** — любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу («субъект данных»).
- Например, прямо или косвенно человек может быть идентифицирован с использованием идентификатора, фамилии, идентификационного номера, данных о местоположении, любые онлайн-идентификаторы, а также при помощи характерных для данного лица физических, физиологических, генетических, духовных, экономических, культурных факторов или ссылаясь на факторы социальной идентичности и т.п.
- То **все данные, которые с ним связаны — это персональные данные.** То есть просто **данные становятся персональными данными, если, используя некую их совокупность, можно однозначно идентифицировать человека**.

General Data Protection Regulation (GDPR)

- **Примеры персональных данных:**
  - имя, фамилия
  - номер паспорта или ИД удостоверения
  - дата и место рождения
  - место проживания, регистрация, прописка
  - е-мейл, телефон, или другая контактная информация
  - IP-адрес и параметры соединения
  - дата и время посещения ресурса, история и параметры посещений, включая название браузера.

General Data Protection Regulation (GDPR)

- **А также особо охраняемые данные:**
  - раса и национальность
  - политические взгляды
  - вероисповедание
  - сексуальная ориентация
  - биометрические данные — физические, физиологические или поведенческие признаки физического лица, при помощи которых возможно однозначно идентифицировать человека. Например, изображение человеческого лица, отпечатки пальцев, сетчатки глаза, запись голоса и т.п.
  - данные о здоровье – данные о физическом или психическом здоровье человека. Например, медицинские анализы и заключения.
  - генетические данные – унаследованные или приобретенные генетические признаки физического лица, предоставляющие уникальную информацию о физиологии или здоровье, а также соответствующие биологические образцы

General Data Protection Regulation (GDPR)
Требования к обработке персональных данных

- **GDPR закрепляет ряд принципов, на которых должна основываться обработка персональных данных:**
- **1) Законность, справедливость, прозрачность** — персональные данные можно обрабатывать только при наличии одного из шести законных оснований.
- **2) Целевое ограничение** — персональные данные могут обрабатываться только для конкретной цели, о которой должно быть известно субъекту персональных данных.
- **3) Минимизация данных** — персональные данные могут обрабатываться только в объеме, необходимом для достижения заявленной цели.
- **4) Точность** — данные должны быть точными и при необходимости обновляться; неактуальные данные должны быть удалены.
- **5) Ограничение хранения данных** — персональные данные должны храниться не дольше срока, необходимого для достижения целей их использования.
- **6) Целостность и безопасность** — при обработке персональных данных должна обеспечиваться защита от случайной потери, уничтожения или повреждения с использованием соответствующих технических или организационных мер.

Справочно

- **Общий регламент о защите персональных данных** (англ. General Data Protection Regulation, GDPR; Постановление (Европейский Союз) 2016/679) **распространяет свои требования на субъектов правоотношений (в том числе и белорусских) по защите персональных данных, обрабатывающих персональные данные граждан Республики Беларусь, находящихся на территории Европейского союза** (например, при оплате банковской пластиковой карточкой).
- Кроме того, **Общий регламент о защите персональных данных будет применяться к организациям Республики Беларусь, обрабатывающим персональные данные граждан Европейского союза** (гостиницы, туристические компании, организации, оказывающие информационные услуги, доступ к онлайн-играм и др.), при оказании услуг таким лицам.
- При этом несоблюдение норм Общего регламента о защите персональных данных в таком случае может влечь предусмотренную им ответственность (например, административные штрафы в размере не более 10 000 000 евро или в случае предприятия, в размере не более 2% от общего годового оборота за предыдущий финансовый год в соответствии с пунктом 4 статьи 83 Общего регламента о защите персональных данных).

General Data Protection Regulation (GDPR)

Штраф в размере до 4% от суммарного оборота

Ранее размеры штрафов и их влияние были ограничены. Согласно GDPR штрафы будут одинаково применимы и к контроллерам данных, и к операторам.

Увеличение зоны действия

GDPR будет применяться ко всем компаниям, обрабатывающим персональные данные субъектов ЕС вне зависимости от географического расположения компании.

Конкретное и однозначное согласие

Должно составляться на доступном языке, в информативной и понятной форме. Согласие на обработку персональных данных при необходимости должно быть так же легко отозвать, как и предоставить.

Аналогично 152-ФЗ

Права субъекта персональных данных

Субъект персональных данных может запросить подтверждение обработки его персональных данных, а также место и цель обработки. Кроме того, субъект обладает «правом на забвения», что подразумевает удаление всех данных, относящихся к данному субъекту.

Частично совпадает со 152-ФЗ

Уведомление о нарушениях в течение 72 часов

Существенные нарушения информационной безопасности должны доводиться до сведения регулирующих органов и, при необходимости, до сведения физических лиц, затронутых такими нарушениями.

Конфиденциальность по умолчанию

Теперь существует законодательное требование по включению механизмов защиты данных на этапе проектирования новой технологии/системы вместо ретроспективного анализа и включения дополнительных механизмов.

Инвентаризация данных

Организации должны вести реестр всех персональных данных, которые они обрабатывают. Реестр должен содержать всю необходимую информацию, в том числе цель обработки данных.

Позиция директора по защите данных

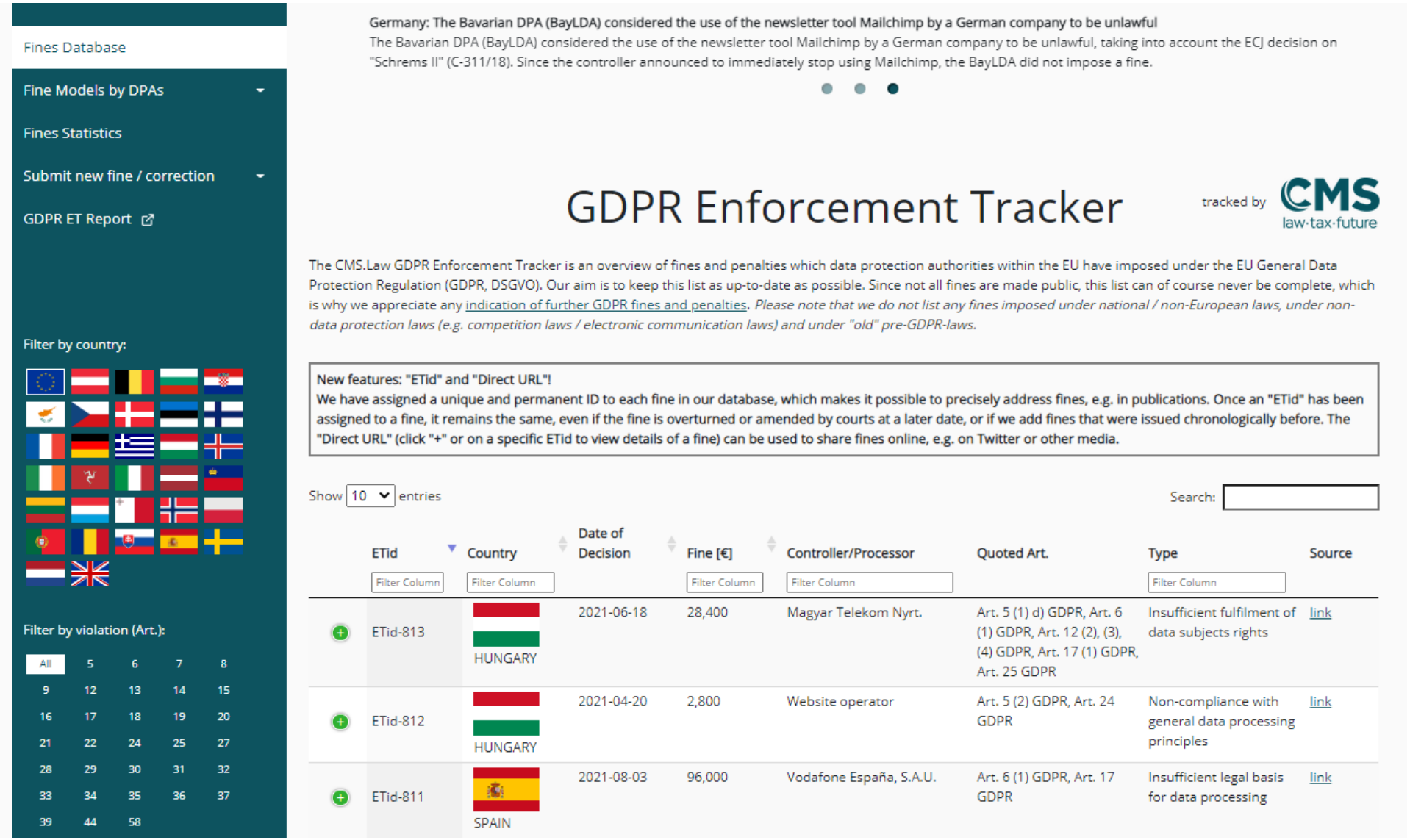
В ряде случаев необходимо учредить должность директора по защите данных для соответствия требованиям GDPR и компенсации отсутствия дальнейшей необходимости предоставления информации об операциях по обработке или передаче данных на основании соответствующих положений типовых договоров.

GDPR - **Штрафы**

- **GDPR предусматривает два вида штрафов в следующем размере:**
- 1) **до 10 миллионов евро или 2% от годового оборота** компании за прошлый финансовый год (в зависимости от того, что больше);
- 2) **до 20 миллионов евро или 4% от годового оборота** компании за прошлый финансовый год (в зависимости от того, что больше). Повышенный размер штрафа предусмотрен, например, за нарушение принципов обработки данных, прав субъектов персональных данных и иные нарушения.

База сведений о штрафов за нарушение GDPR

https://www.enforcementtracker.com

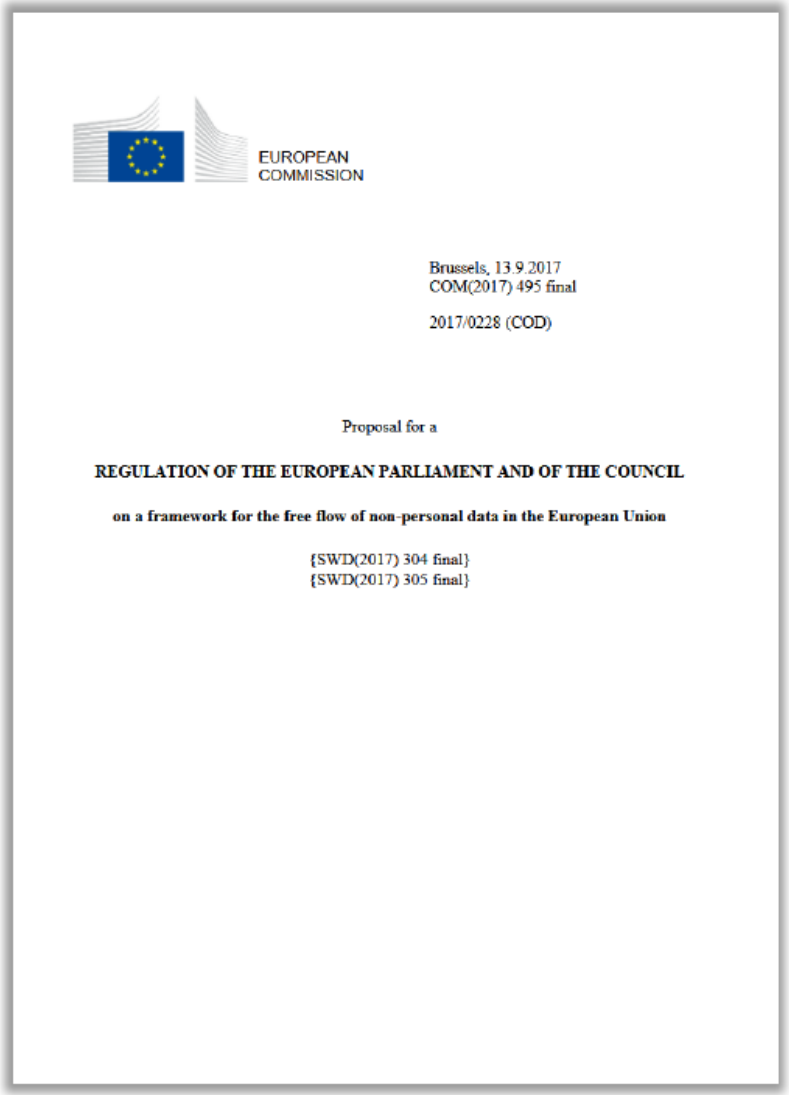


Дополнительные материалы

Штрафуют даже GOOGLE. Ошибки в GDPR за 2 года. (май 2020)
https://www.youtube.com/watch?v=GHQ5pgdJT3c

Европейский союз

Digital Single Market (Цифровой единый рынок): свободное перемещение в ЕС данных, не являющихся персональными



EUROPEAN
COMMISSION

Brussels, 13.9.2017
COM(2017) 495 final

2017/0228 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on a framework for the free flow of non-personal data in the European Union

{SWD(2017) 304 final}
{SWD(2017) 305 final}

- **Proposal 2017/0228 (COD) for a Regulation on a framework for the free flow of non-personal data in the European Union**
- Проект Регламента о свободном перемещении неличных данных в ЕС. По расчетам Европейской Комиссии потенциальный эффект от снятия внутренних барьеров ЕС для свободного перемещения информации составит до €739 млрд, к 2020 году, удвоив дою отрасли до 4% ВВП ЕС.
- **Примеры требований о локализации данных в ЕС:**
  - данные о транзакциях при оказании финансовых услуг;
  - сведения, составляющие профессиональные тайны (например, врачебная тайна);
  - информация, образующаяся в процессе работы государственных органов, вне зависимости от ее критичности.

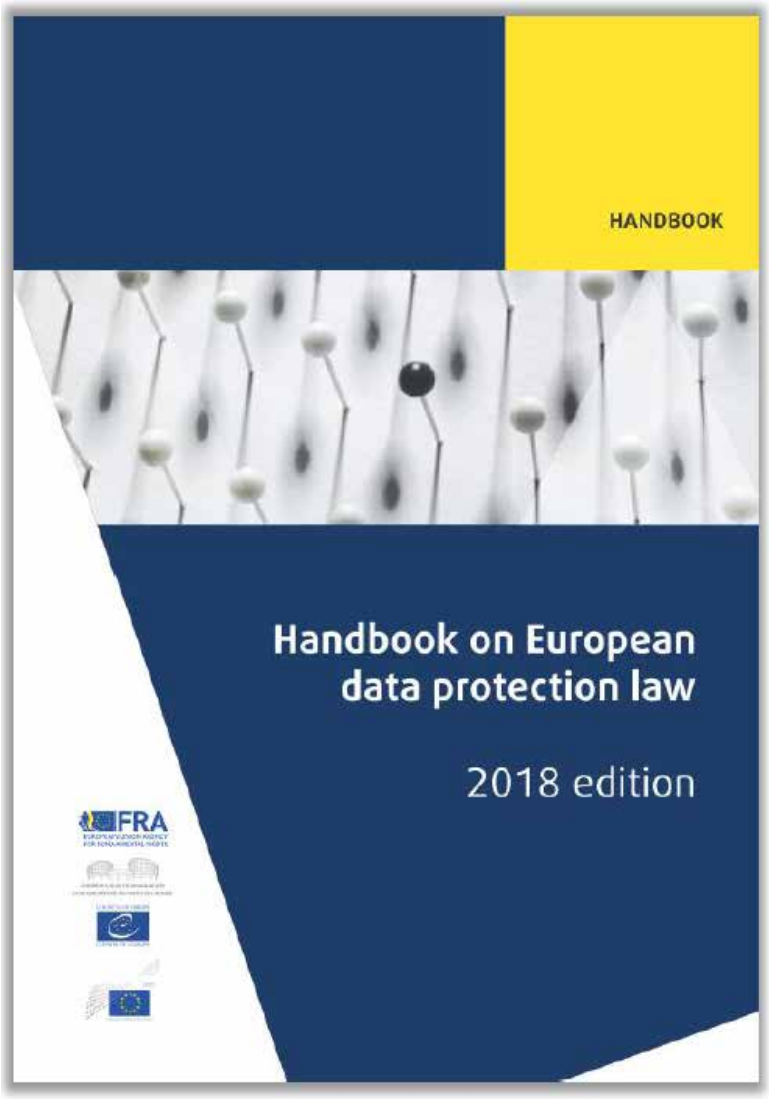
Digital Single Market **(Цифровой единый рынок): свободное перемещение в ЕС данных, не являющихся персональными**

- Proposal 2017/0228 (COD) for a Regulation on a framework for the free flow of non-personal data in the European Union
  https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2017)495&lang=ru

- Framework for the free flow of non-personal data in the EU
  https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_4249

- EU negotiators reach a political agreement on free flow of non-personal data
  https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4227

Руководство по европейскому законодательству о защите данных от FRA



В мае 2018 года Агентство Европейского союза по фундаментальным правам человека (European Union Agency for Fundamental Rights) и Совет Европы (Council of Europe) опубликовали обновленное **Руководство по европейскому законодательству о защите данных**. Положения Руководства охватывают не только основные определения, принципы и требования GDPR, но и рассматривают применимую судебную практику Европейского суда по правам человека (European Court of Human Rights) и Европейского суда (European Court of Justice).

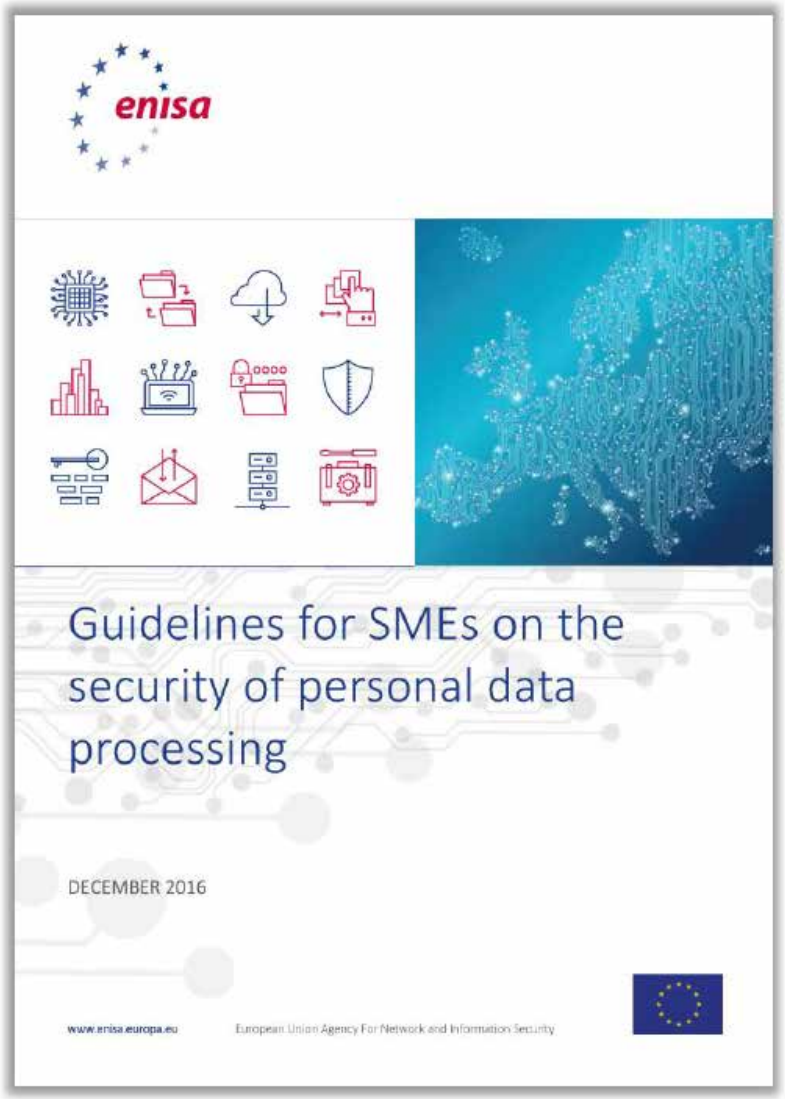
Руководство по европейскому законодательству о защите данных от FRA

- Data protection, privacy and new technologies
  https://fra.europa.eu/en/themes/data-protection-privacy-and-new-technologies

- Handbook on European data protection law - 2014 edition
  https://fra.europa.eu/en/publication/2014/handbook-european-data-protection-law-2014-edition
  https://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf

- Handbook on European data protection law - 2018 edition
  https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition
  https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf

Руководство для малых и средних компаний (SME) по защите персональных данных



Guidelines for SMEs on the security of personal data processing

Security risk management for personal data

Руководство для малых и средних компаний (SME) по защите персональных данных в ЕС

- Во вступлении **Guidelines for SMEs on the security of personal data processing** написано, что крупные компании при обеспечении безопасности персональных данных в рамках GDPR могут использовать риск ориентированный подход, придумывать собственные методики анализа, рассматривать сотни угроз и самостоятельно подбирать контрмеры для каждой угрозы.
- Но малые и средние компании как правило не имеют достаточной экспертизы и ресурсов, чтобы провести такой подробный анализ, а ведь SME составляет 99% от общего количества операторов персональных данных.
- Для того чтобы помочь малым и средним компаниям выполнить требования GDPR по безопасности по упрощенной схеме и при этом сохранить риск-ориентированный подход и адаптацию мер защиты под особенности обработки данных, ENISA и выпустила данное руководство (guidelines).

Руководство для малых и средних компаний (SME) по защите персональных данных в ЕС

- **The European Union Agency for Cybersecurity (ENISA) https://www.enisa.europa.eu**

- **Guidelines for SMEs on the security of personal data processing**
  https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing
  https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing/at_download/fullReport

- **ПДн. Лучшие практики ENISA по защите персональных данных**
- https://www.securitylab.ru/blog/personal/sborisov/343462.php

- ENISA Publications
  https://www.enisa.europa.eu/publications#c5=2011&c5=2021&c5=false&c2=publicationDate&reversed=on&b_start=0

База отчетов, исследований и мнений от Совета Европы по защите персональных данных

WWW.COE.INT HUMAN RIGHTS DEMOCRACY RULE OF LAW EXPLORE English Connect

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

COUNCIL OF EUROPE Data Protection

Home | Convention 108 and Protocols | Activities | Documentation | Data Protection Commissioner | Stefano Rodotà Award | Data Protection Day | COVID-19 and Data Protection

You are here: Data-protection > Documentation

Reports, studies and opinions

2021

- Guidelines on facial recognition (T-PD(2020)03rev4)
- Opinion on recommendation 2185 (2020) of the Parliamentary Assembly of the Council of Europe "Artificial intelligence in health care: medical, legal and ethical challenges ahead"
- Opinion of the Committee of Convention 108 on the draft second additional Protocol to the Budapest Convention
- Interpretation of provisions: Convention 108+
- T-PD-BUR(2021)7 - Opinion of the Bureau on the draft Recommendation of the Committee of Ministers to Member States on Electoral communication and Media Coverage of Election Campaigns

2020

2019

2018

www.coe.int/dataprotection

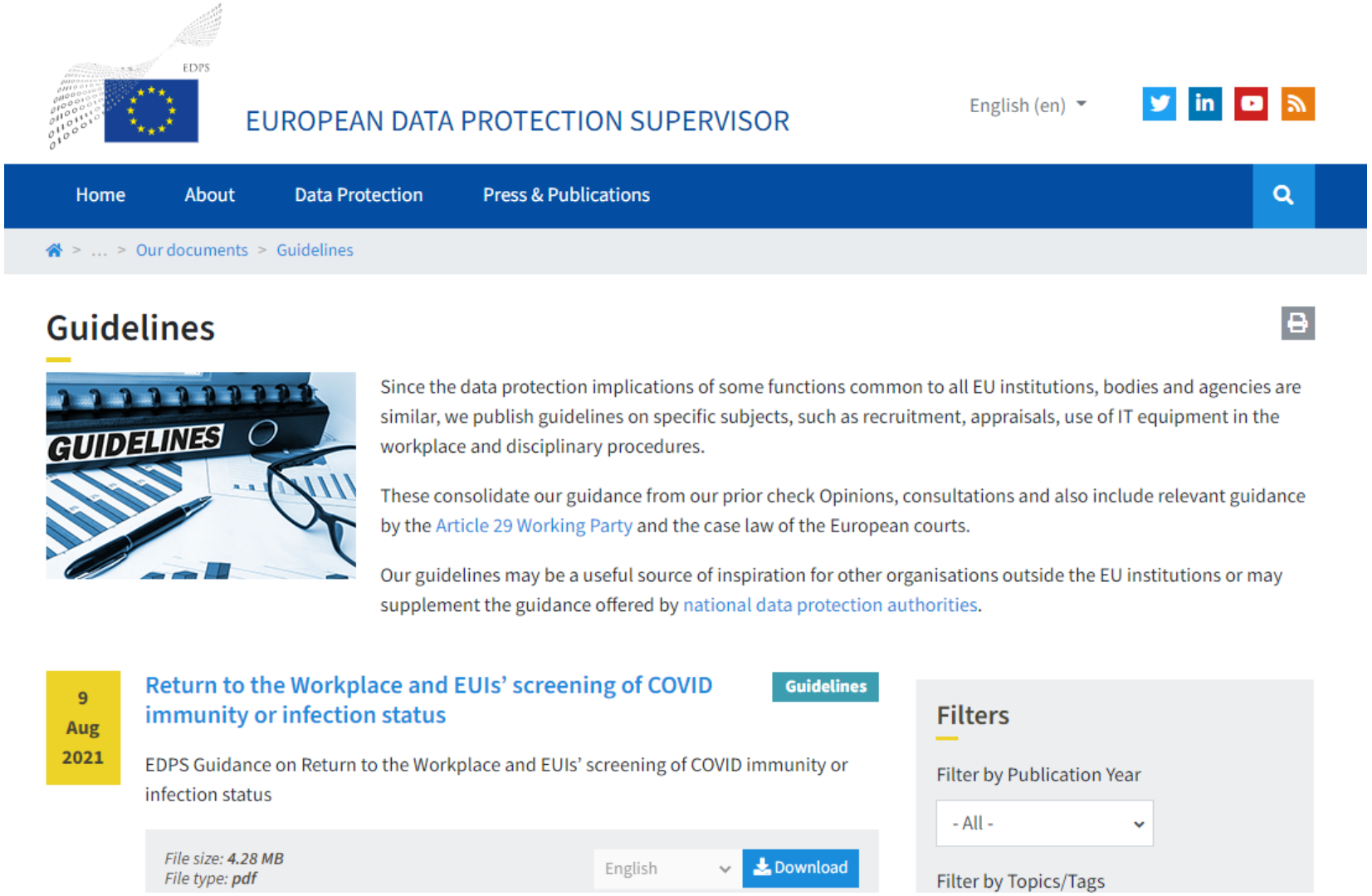
Search tool

ECHR Factsheets

Personal data protection

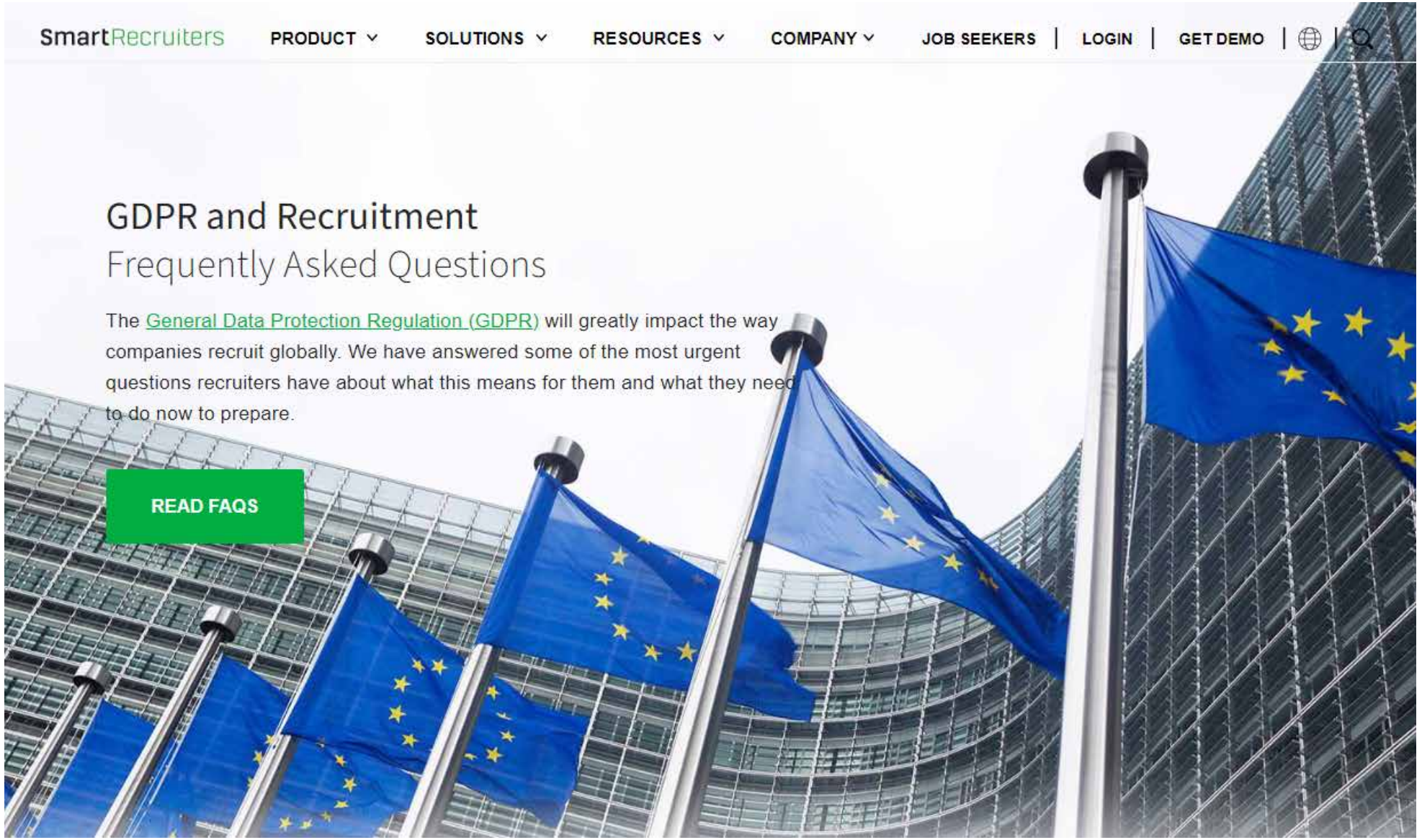
https://www.coe.int/en/web/data-protection/reports-studies-and-opinions

Рекомендации от Европейского инспектора по защите данных



https://edps.europa.eu/data-protection/our-work/our-work-by-type/guidelines_en

Соблюдение GDPR при подборе персонала



https://www.smartrecruiters.com/resources/gdpr-recruiting/recruitment-gdpr-faq/

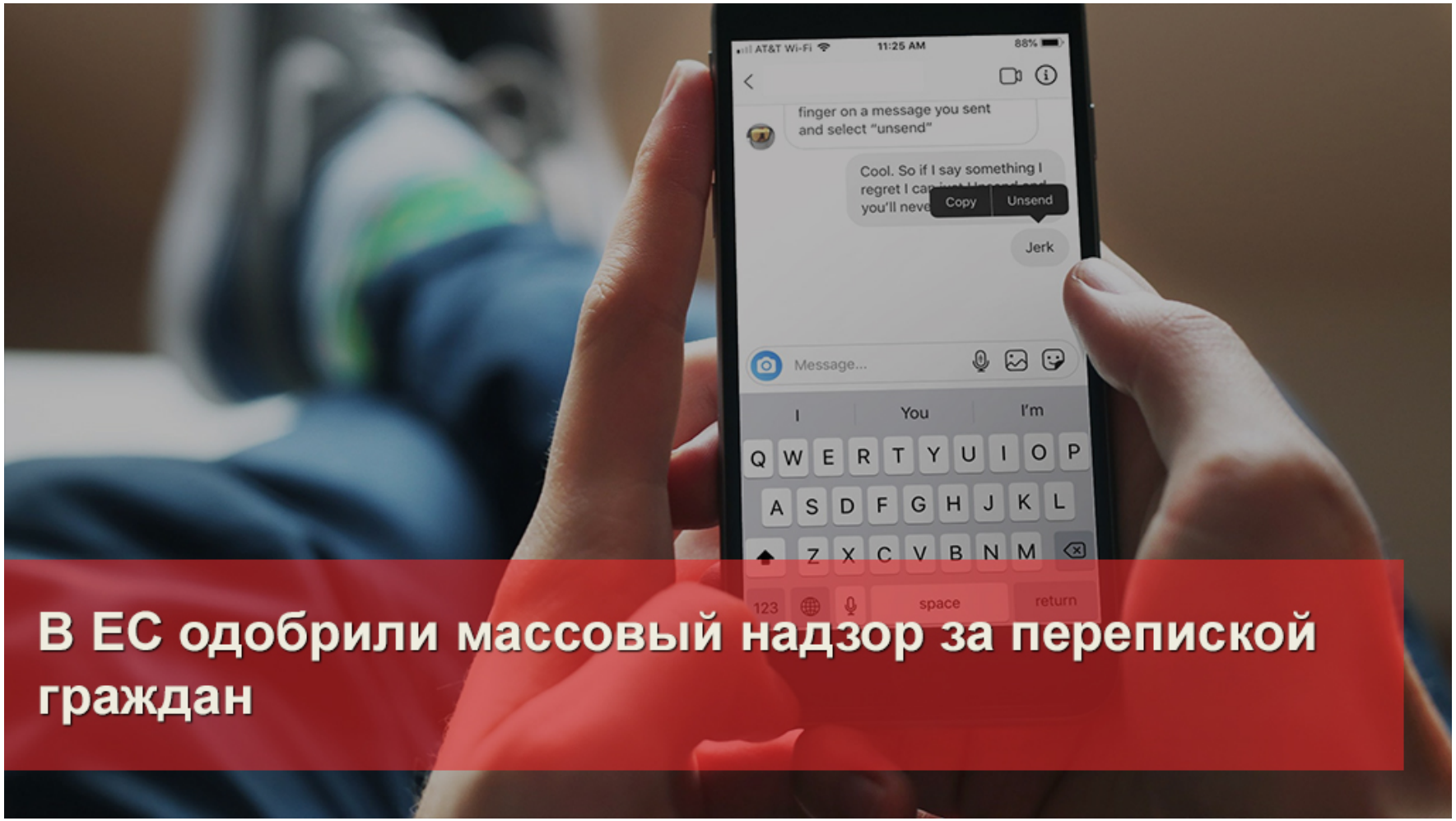
отмена GDPR **когда нужно**

- **В июле 2021 года** Европарламент одобрил постановление, получившее названия **ePrivacy derogation** («отступление от интернет-приватности») или **Chatcontrol**, которое разрешает временный отход от европейских правил конфиденциальности в Сети, включая общий регламент по защите данных (GDPR).
- **ePrivacy derogation** это конец сквозному шифрованию и тайне переписки в мессенджерах, а также в электронной почте в европейском союзе. Все сообщения будут автоматически проверяться на наличие информации о сексуальном насилии над детьми и детской порнографией.
- **Аналогичную систему (CSAM) применяет компания Apple в своих продуктах уже несколько лет, с 2019 года.**

CSAM в устройствах и сервисах Apple

- Apple подтвердила информацию что с 2019 года используется технология в iOS, macOS, watchOS, iCloud и iMessage, которая выявляет на пользовательских устройствах изображения, потенциально содержащие элементы жестокого обращения с детьми (CSAM).
- Важный момент в реализации данной функции заключается в том, что алгоритмы локально сканируют фотографии перед резервным копированием в iCloud. Для этого нейросети сопоставляют изображения из облачных хранилищ с хешами изображений, предоставленных NCMEC и другими организациями по детской безопасности.
- В США технология позволит компании отчитываться об опасных случаях в Национальный центр пропавших и эксплуатируемых детей (NCMEC). Все имеющиеся функции будут работать пока только в США.

Chatcontrol



Европарламент утвердил постановление **Chatcontrol** — частичное нарушение конфиденциальности, позволяющее поставщикам услуг электронной почты и обмена сообщениями автоматически искать в личных сообщениях пользователей подозрительный контент и сообщать правоохранителям.

https://chatcontrol.se
https://www.patrick-breyer.de/en/posts/chat-control/
https://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=CELEX:52022PC0209&from=SV
https://eur-lex.europa.eu/resource.html?uri=cellar:13e33abf-d209-11ec-a95f-01aa75ed71a1.0018.02/DOC_1&format=PDF

Chatcontrol. **Как это повлияет на пользователей?**

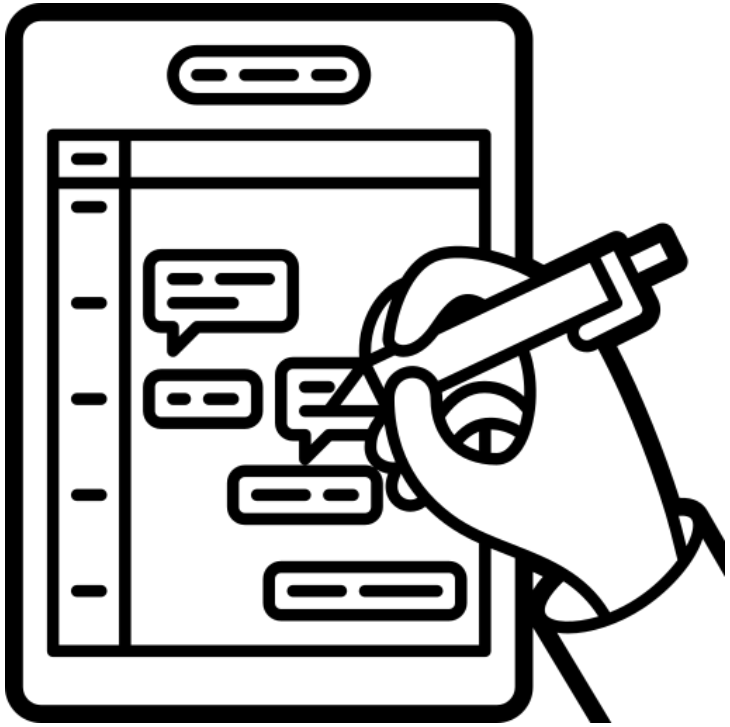
- **Абсолютно все переписки в мессенджерах и электронные письма будут проверяться на предмет подозрительного контента.** Ничто не останется конфиденциальным или тайным. Для сканирования сообщений пользователей не понадобится судебных решений и даже подозрений. Это будет происходить всегда и автоматически.
- **Если алгоритм классифицирует контент в переписке как подозрительный, то личные и интимные фотографии пользователей могут быть просмотрены сотрудниками и подрядчиками международных корпораций и правоохранительных органов.** То есть абсолютно незнакомыми людьми, в чьих руках они могут представлять вполне осязаемую опасность.
- **Алгоритмы также могут ошибочно срабатывать на флирт и секстинг**, что автоматически сделает подобные личные переписки доступными сотрудникам и подрядчикам международных корпораций и правоохранительных органов.

Chatcontrol. **Как это повлияет на пользователей?**

- **Алгоритмы могут ложно сработать на законопослушных пользователей**, так как зачастую срабатывают на абсолютно легальные фотографии, например, детей на пляже.
- **Во время поездки за границу пользователей могут ожидать большие проблемы**, так как автоматически сгенерированные отчеты могут быть доступны правоохранительным органам других стран, например, таких как США, где нет регулирования в области персональных данных.
- **Спецслужбы и хакеры смогут шпионить за личными чатами и электронной почтой пользователей**. Потенциальный бэкдор будет доступен для всех, у кого есть технические средства для перехвата переписки, так как будет отключено сквозное шифрование.

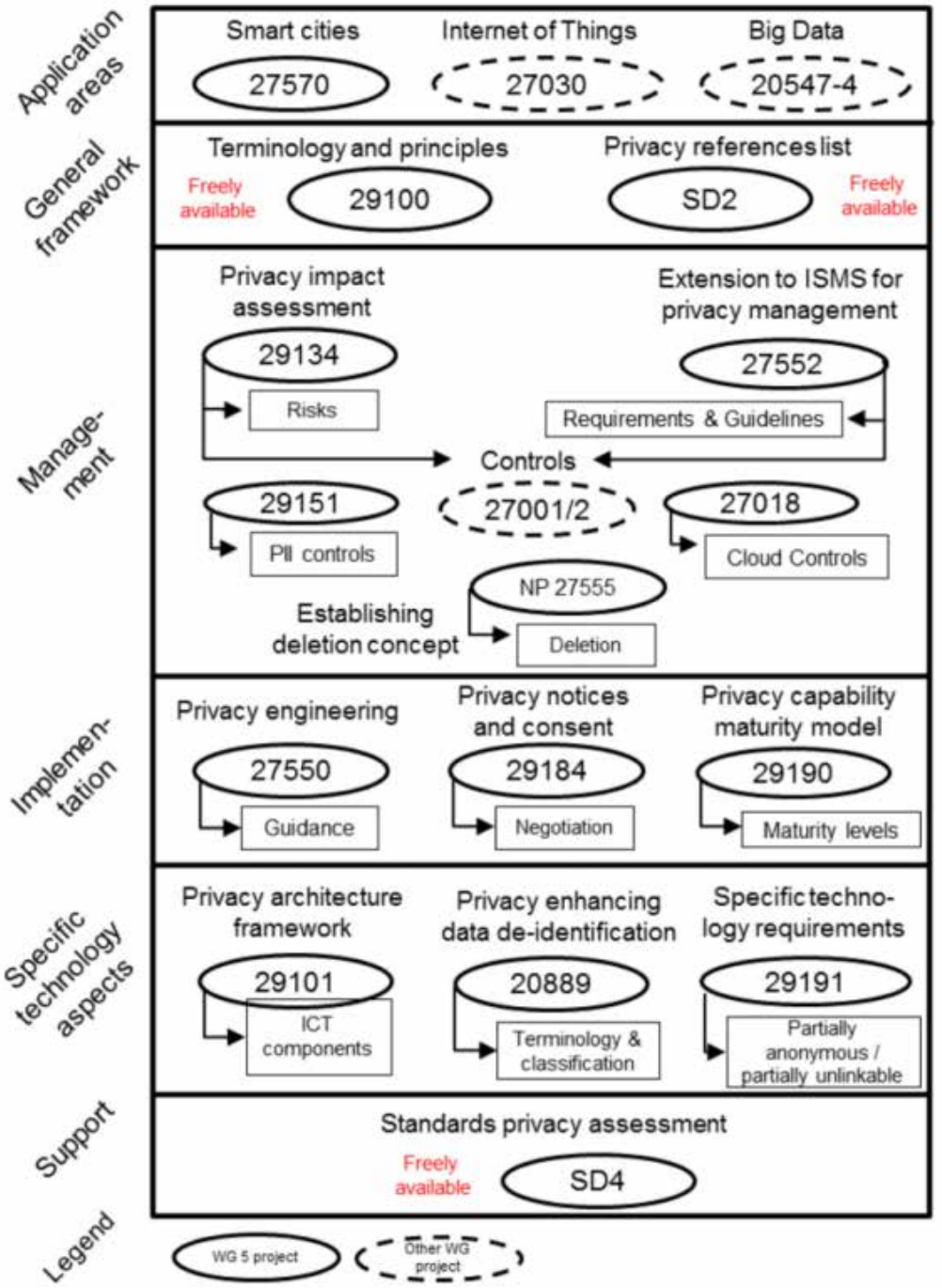
Chatcontrol. **Как это повлияет на пользователей?**

- **Соблюдение Chatcontrol вынудит разработчиков онлайн-сервисов добавлять в свои продукты бэкдоры,** которыми также смогут воспользоваться далеко не те, для кого они предусматривались изначально, например, иностранные спецслужбы или преступники.
- Таким образом могут быть раскрыты деловые секреты, правительственная информация и потенциально любые данные.



Международные стандарты ISO/IEC по персональным данным

Стандарты ISO **в сфере** Privacy



Стандарт ISO/IEC 27701:2019. Расширение до ISO/IEC 27001 и ISO/IEC 27002 по управлению персональными данными


INTERNATIONAL STANDARD

ISO/IEC 27701

First edition 2019-08

Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

Techniques de sécurité — Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection de la vie privée — Exigences et lignes directrices

Reference number ISO/IEC 27701:2019(E)

© ISO/IEC 2019

- Международной организацией по стандартизации (International Organization for Standardization) был опубликован стандарт **27701:2019 «Методы обеспечения безопасности - Расширение до ISO/IEC 27001 и ISO/IEC 27002 по управлению персональными данными - Требования и руководящие указания»** (Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines).
- В стандарте описано руководство по созданию, внедрению, поддержанию и постоянному совершенствованию Системы управления персональными данными (Privacy Information Management System - PIMS) в контексте организации. Стандарт определяет требования, связанные с PIMS, и формулирует правила для операторов (controllers) и обработчиков (processors) в отношении обработки персональных данных.

Стандарт ISO/IEC 27017:2015. Защита персональных данных при предоставлении облачных услуг


INTERNATIONAL STANDARD

ISO/IEC 27017

First edition
2015-12-15

Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

Technologies de l'information — Techniques de sécurité — Code de pratique pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage

Reference number
ISO/IEC 27017:2015(E)

© ISO/IEC 2015

- Международной организацией по стандартизации (International Organization for Standardization) был опубликован стандарт ISO/IEC 27017:2015 «**Информационные технологии - Методы обеспечения безопасности - Система менеджмента облачной безопасности и защиты персональных данных - Меры безопасности**» (Information technology - Security techniques - Cloud computing security and privacy management system - Security controls).
- Стандарт содержит указания по мерам обеспечения информационной безопасности, применимым при предоставлении и использовании облачных услуг, в том числе за счет дополнительных рекомендаций по внедрению соответствующих мер, перечисленных в стандарте ISO/IEC 27002, а также дополнительных, специфических для облачных сервисов мер контроля и управления, а также рекомендаций по их внедрению. Стандарт предлагает меры контроля и управления, а также рекомендации по их внедрению как поставщикам облачных услуг, так и их клиентам.

Стандарт ISO/IEC 27018:2019. Практика защиты персональных данных в публичных облаках


INTERNATIONAL STANDARD

ISO/IEC 27018

Second edition
2019-01

Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

Technologies de l'information — Techniques de sécurité — Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII

ISO IEC

Reference number
ISO/IEC 27018:2019(E)

© ISO/IEC 2019

- Международной организацией по стандартизации (International Organization for Standardization) был опубликован стандарт ISO/IEC **27018:2019** «**Информационные технологии - Методы обеспечения безопасности - Практика защиты персональных данных в публичных облаках, выступающих в роли обработчиков персональных данных**» (Information technology - Security techniques - Code of practice for protection of personally identifiable information (PH) in public clouds acting as PH processors).
- Стандарт устанавливает общепринятые цели управления, меры и средства управления и даёт рекомендации по реализации мер по защите персональных данных (Personally Identifiable Information, PH) в соответствии с принципами защиты неприкосновенности частной жизни, сформулированными в стандарте ISO/IEC 29100, для среды облачных вычислений в публичных облаках.

Стандарт ISO/IEC 27750:2019. Инженерия обеспечения неприкосновенности частной жизни

- Международной организацией по стандартизации (International Organization for Standardization) был опубликован стандарт **27750:2019** «**Информационная безопасность - Меры безопасности - Инженерия обеспечения неприкосновенности частной жизни**» (Information technology - Security techniques - Privacy engineering).
- В стандарте описаны рекомендации по запроектированной защите неприкосновенности частной жизни (privacy engineering), которые призваны помочь организациям интегрировать последние достижения в сфере такого рода «встроенной» защиты в их практику проектирования систем:
- Документ описывает взаимосвязь между инженерией защиты неприкосновенности частной жизни и другими инженерными точками зрения (системное проектирование, инженерия безопасности, управление рисками), а также описывает инженерию защиты неприкосновенности частной жизни в числе ключевых по важности процессов проектирования, таких, как управление знаниями, управление рисками, анализ требований, проектирование архитектуры.

Стандарт ISO/IEC 29100:2018. Концепция защиты персональных данных


INTERNATIONAL STANDARD

ISO/IEC 29100

First edition
2011-12-15
AMENDMENT 1
2018-06

Information technology — Security techniques — Privacy framework

AMENDMENT 1: Clarifications

Technologies de l'information — Techniques de sécurité — Cadre privé
AMENDEMENT 1: Clarifications

ISO IEC

Reference number
ISO/IEC 29100:2011/Amd.1:2018(E)

© ISO/IEC 2018

- Международной организацией по стандартизации (International Organization for Standardization) был опубликован стандарт **29100:2011 «Информационная технология. Методы и средства обеспечения безопасности. Концепция защиты персональных данных»** (Information technology - Security techniques -Privacy framework).
- В стандарте сформулированы принципы и меры по защите неприкосновенности частной жизни, сформулированными. В России адаптирован как **ГОСТ Р ИСО/МЭК 29100-2013** «Информационная технология. Методы и средства обеспечения безопасности. Основы обеспечения приватности».

Стандарт ISO/IEC 29101:2018. Концепция архитектуры, обеспечивающей защиту персональных данных

- Международной организацией по стандартизации (International Organization for Standardization) был опубликован стандарт ISO/IEC **29101:2018** «**Информационная безопасность - Меры безопасности -Концепция архитектуры, обеспечивающей защиту персональных данных**» (Information technology - Security techniques - Privacy architecture framework).
- В стандарте описаны высокоуровневая концепция архитектуры и взаимосвязанные с ней меры контроля и управления, используемые для защиты неприкосновенности частной жизни (персональных данных) в ИКТ-системах, которые хранят и обрабатывают персональные данные.

Стандарт ISO/IEC 29134:2017. Оценка воздействия на неприкосновенность частной жизни


INTERNATIONAL STANDARD

ISO/IEC 29134

First edition
2017-06

Information technology — Security techniques — Guidelines for privacy impact assessment

Technologies de l'information — Techniques de sécurité — Lignes directrices pour l'évaluation d'impacts sur la vie privée

ISO IEC

Reference number
ISO/IEC 29134:2017(E)

© ISO/IEC 2017

- Международной организацией по стандартизации (International Organization for Standardization) был опубликован стандарт ISO/IEC **29134:2017 «Информационные технологии - Методы и средства обеспечения безопасности - Оценка воздействия на неприкосновенность частной жизни - Руководство»** (Information technology - Security techniques - Privacy impact assessment - Guidelines).
- Стандарт определяет методику проведений «**оценки воздействия на неприкосновенность частной жизни**» (Data protection impact assessment - см. ст.35 GDPR) и устанавливает определенные рамки для такой оценки, с тем. чтобы уменьшить разнобой в подходах и повысить качество. Стандарт позволит провести анализ воздействия предполагаемых в ходе обработки операций на защиту персональных данных, если такая обработка способна создать повышенные риски для прав и свобод физических лиц.

Стандарт ISO/IEC 29151:2017. Свод практики по защите персональных данных

- Международной организацией по стандартизации (International Organization for Standardization) был опубликован стандарт **ISO/IEC 29151:2017** «**Информационные технологии - Методы обеспечения безопасности - Свод практики по защите персональных данных**» (Information technology - Security techniques -Code of practice for personally identifiable information protection).
- Стандарт является непосредственным дополнением действующего стандарта **ISO/IEC 27018:2014** «Информационные технологии - Методы обеспечения безопасности - Практика защиты персональных данных в публичных облаках, выступающих в роли обработчиков персональных данных» (Information technology - Security techniques - Code of practice for protection of personally identifiable information (PH) in public clouds acting as PH processors).

Стандарт ISO/IEC 29190:2015. Оценка способности обеспечить неприкосновенность частной жизни


INTERNATIONAL STANDARD

ISO/IEC 29190

First edition
2015-08-15

Information technology — Security techniques — Privacy capability assessment model

Technologies de l'information — Techniques de sécurité — Modèle d'évaluation de l'aptitude à la confidentialité

Reference number
ISO/IEC 29190:2015(E)

© ISO/IEC 2015

- Международной организацией по стандартизации (International Organization for Standardization) был опубликован стандарт **29190:2015 «Информационные технологии - Методы и средства обеспечения безопасности - Модель оценки способности обеспечить неприкосновенность частной жизни»** (Information technology - Security techniques - Privacy capability assessment model).
- Стандарт является высокоуровневым руководством для организаций по вопросам проведения ими оценки своих возможностей по управлению процессами, потенциально затрагивающими неприкосновенность частной жизни. В нём, в частности определены шаги, выполняемые в ходе оценки процессов на предмет их способности обеспечить защиту персональных данных, а также определен набор уровней способности обеспечить защиту персональных данных.

Стандарт ISO/IEC 29191:2012. Требования к частично анонимной и частично несвязываемой аутентификации


INTERNATIONAL STANDARD

ISO/IEC 29191

First edition 2012-12-15

Information technology — Security techniques — Requirements for partially anonymous, partially unlinkable authentication

Technologies de l'information — Techniques de sécurité — Exigences pour l'authentification partiellement anonyme, partiellement non reliable

Reference number ISO/IEC 29191:2012(E)

© ISO/IEC 2012

- Международной организацией по стандартизации (International Organization for Standardization) был опубликован стандарт **29191:2012** «**Информационные технологии - Методы обеспечения защиты - Требования к частично анонимной и частично несцепляемой аутентификации**» (Information technology - Security techniques - Requirements for partially anonymous, partially unlinkable authentication).
- Текущий уровень техники для аутентификации пользователя требует раскрытия идентифицируемой информации аутентифицируемого пользователя. Во многих типах транзакций пользователь предпочел бы оставаться анонимным и не связываемым, что означает, что при выполнении двух транзакций трудно различить, выполняются ли транзакции одним и тем же пользователем или двумя разными пользователями. Тем не менее, в некоторых обстоятельствах существуют законные причины для возможности повторной идентификации (например, необходимость учета). Современные криптографические технологии предоставляют возможности реализации частично анонимной, частично несвязываемой аутентификации.

Стандарт ISO/IEC 20889:2018. Обезличивание персональных данных


INTERNATIONAL STANDARD

ISO

ISO/IEC FDIS 20889

Privacy enhancing data de-identification terminology and classification of techniques

ISO

© ISO

- Международной организацией по стандартизации (International Organization for Standardization) был опубликован стандарт **ISO/IEC 20889:2018** «**Терминология и классификация методов деидентификации (обезличивания) данных с целью усиления защиты неприкосновенности частной жизни (персональных данных)**» (Privacy enhancing data deidentification terminology and classification of techniques).
- В стандарте описаны усиливающие защиту неприкосновенности частной жизни методы деидентификации данных.
- Стандарт предназначен для использования при описании и проектировании мер по де-идентификации в соответствии с принципами защиты неприкосновенности частной жизни, сформулированными в стандарте **ISO/IEC 29100:2011** «Информационная технология. Методы и средства обеспечения безопасности. Концепция защиты персональных данных» (Information technology - Security techniques - Privacy framework).

Технические спецификации ISO/IEC TS 20748-4:2019. Защита персональных данных в сфере образования


TECHNICAL SPECIFICATION

ISO/IEC TS 20748-4

First edition 2019-09

Information technology for learning, education and training — Learning analytics interoperability —

Part 4:
Privacy and data protection policies

ISO IEC

Reference number ISO/IEC TS 20748-4:2019(E)

© ISO/IEC 2019

- Международной организацией по стандартизации (International Organization for Standardization) был опубликован технические спецификации **ISO/IEC TS 20748-4:2019 «Информационные технологии для обучения, образования и подготовки Интероперабельность средств сбора и обработки данных об учащихся - Часть 4: Политики защиты неприкосновенности частной жизни и защиты персональных данных»** (Information technology for learning, education and training - Learning analytics interoperability - Part 4: Privacy and data protection policies).
- В документе устанавливаются требования к защите неприкосновенности частной жизни и персональных данных, которые должны использоваться при проектировании систем сбора и обработки данных об учащихся (learning analytics) и в практике сбора и обработки такого рода данных в школах, университетах, при обучении на рабочем месте и при использовании смешанных подходов к обучению.

Другие стандарты по защите персональных данных

- **ISO/IEC 15944-8:2012** «Информационные технологии - Взгляд с точки зрения деловых операций. Часть 8. Выявление требований к защите персональных данных в качестве внешних ограничений на деловые операции» (Information technology - Business operational view - Part 8: Identification of privacy protection requirements as external constraints on business transactions)
- **ISO/IEC 29187-1:2013** «Информационные технологии - Выявление требований к защите персональных данных, относящихся к обучению, образованию и тренировке (LET). Часть 1: Концепция и эталонная модель» (Information technology - Identification of privacy protection requirements pertaining to learning, education and training (LET) - Part 1: Framework and reference model)
- **ISO 22307:2008** «Финансовые услуги - Оценка воздействия на неприкосновенность частной жизни» (Financial services - Privacy impact assessment)
- **ISO/TS 17975:2015** «Информатика в здравоохранении - Принципы и требования к данным для согласия на сбор, использование или раскрытие персональной информации о здоровье» (Health informatics - Principles and data requirements for consent in the Collection, Use or Disclosure of personal health information)
- **ISO 22857:2013** «Информатика в здравоохранении - Руководство по защите персональных данных с целью содействия трансграничной передаче персональной информации о здоровье» (Health informatics - Guidelines on data protection to facilitate trans-border flows of personal health data)

Другие стандарты по защите персональных данных

- **ISO/TS 14441:2013** «Информатика в здравоохранении - Требования по безопасности и защите персональных данных к системам управления электронными медицинскими документами, для использования при оценке соответствия» (Health informatics -Security and privacy requirements of EHR systems for use in conformity assessment)
- **ISO 25237:2017** «Информатизация здоровья. Псевдонимизация» (Health informatics - Pseudonymization)
- **ISO/TR 12859:2009** «Интеллектуальные транспортные системы (ИТС) - Архитектура систем - Вопросы защиты неприкосновенности частной жизни в стандартах и системах ИТС» (Intelligent transport systems - System architecture - Privacy aspects in ITS standards and systems)
- **ISO 16461:2018** «Интеллектуальные транспортные системы (ИТС) - Критерии защиты целостности и защиты персональных данных в системах бортовых транспортных датчиков» (Intelligent transport systems - Criteria for privacy and integrity protection in probe vehicle information systems)
- **ISO/TR 17427-7:2015** «Интеллектуальные транспортные системы (ITS) - Кооперативные ITS. Часть 7. Вопросы защиты неприкосновенности частной жизни» (Intelligent transport systems - Cooperative ITS - Part 7: Privacy aspects)
- **ISO/IEC TS 19608:2018** «Руководство по разработке функциональных требований к безопасности и защите персональных данных на основе ISO/IEC 15408» (Guidance for developing security and privacy functional requirements based on ISO/IEC 15408)
- **ISO/IEC 19086-4:2019** « Облачные вычисления - Концепция соглашений о качестве услуг (SLA) - Часть 4: Компоненты безопасности и защиты персональных данных» (Cloud computing - Service level agreement (SLA) framework - Part 4: Components of security and of protection of PII)

США

**Privacy Act of 1974,
Privacy Protection
Act of 1980,
SP 800-122 и др.**

Основные документы

- **Privacy Act of 1974**
  Закон «О защите конфиденциальности»
  - https://en.wikipedia.org/wiki/Privacy_Act_of_1974
  - https://www.justice.gov/opcl/privstat.htm
- **Privacy Protection Act of 1980**
  Закон «О защите информации»
  - https://en.wikipedia.org/wiki/Privacy_Protection_Act_of_1980
  - https://epic.org/privacy/ppa/
- **SP 800-122** «Руководство по защите конфиденциальности персонально идентифицируемой информации» (Guide to Protecting the Confidentiality of Personally Identifiable Information (PII))
  - http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf
- **SP 800 Series**
  - https://csrc.nist.gov/publications/sp
  - https://csrc.nist.gov/publications/sp800
  - https://www.pvsm.ru/informatsionnaya-bezopasnost/23835

Основные документы

- **California Consumer Privacy Act** 2020 года
- California Consumer Privacy Act, или CCPA – это закон о защите персональных данных пользователей штата Калифорния, который на данный момент является одним из наиболее регламентированных нормативных актов в сфере защиты персональных данных на территории США.
  - https://oag.ca.gov/privacy/ccpa
  - https://en.wikipedia.org/wiki/California_Consumer_Privacy_Act

материалы по теме

- https://uz.ligazakon.ua/magazine_article/EA013372
- https://vc.ru/legal/94782-kaliforniyskiy-zakon-o-konfidencialnosti-potrebiteley-vstupaet-v-silu-s-1-yanvarya-2020-goda

California Consumer Privacy Act (CCPA)

- Основу законодательства штата Калифорния (США) о защите персональных данных составляет **California Consumer Privacy Act (CCPA)**, который вступил в силу с 1 января 2020 года.
- **Основы регулирования. «Персональные данные»** — информация, которая прямо (имя, паспортные данные, водительское удостоверение) или косвенно (куки, номер телефона, IP) идентифицирует потребителя или домохозяйство, биометрические данные (внешность, отпечатки пальцев), геолокация, действия в интернете (история браузера, история поиска) и чувствительные данные (медицинские данные, данные о трудоустройстве, образовании).
- **Сфера действия.** CCPA применяется к компаниям, которые ведут бизнес и обрабатывают данные потребителей из штата Калифорния, если они соответствуют хотя бы одному из следующих условий:
  - Годовой валовый доход компании превышает 25 миллионов долларов США;
  - Компания ежегодно покупает, получает, либо продает персональные данные 50 000 и более потребителей, домохозяйств или устройств;
  - Компания получает не менее 50% своей прибыли от продажи персональных данных потребителей.

California Consumer Privacy Act (CCPA)
Требования к защите персональных данных

- **CCPA обязывает компании при обработке персональных данных соблюдать следующие требования:**
- **1. Предоставлять** потребителям информацию о процессах обработки их персональных данных, их правах в отношении персональных данных, в том числе обновлять политику обработки персональных данных не реже, чем один раз в 12 месяцев;
- **2. Обеспечивать** механизм реализации прав пользователей, в том числе обеспечивать технические средства (например, размещение соответствующей ссылки на веб-сайте или в мобильном приложении), чтобы потребитель мог запретить компании продавать его персональные данные. При этом потребителю не может быть отказано в предоставлении услуг или предложены другие условия их предоставления по причине того, что потребитель реализовал какие-либо права, предоставляемые ему CCPA, в том числе запретил продавать свои персональные данные.
- **3. Верифицировать** личность потребителей, которые направляют запросы.
- **4. Хранить** записи о полученных запросах и ответах на них в течение 24 месяцев.
- На компании, которые обладают персональными данными более чем 4 миллионов потребителей, налагаются дополнительные обязанности.

California Consumer Privacy Act (CCPA)
Ответственность. Штрафы

- **Размер штрафов** составляет 2,500 долларов США за каждое нарушение и 7,500 долларов США за каждое умышленное нарушение. То есть, за непреднамеренное нарушение требований CCPA в отношении 10 000 потребителей штраф достигнет 2,5 миллионов долларов США, а при наличии умысла — 7,5 миллионов долларов США.
- Сам потребитель, чьи права были нарушены, может требовать от компании компенсации в размере от 100 до 750 долларов США.

NIST SP 800-53

- **NIST SP 800-53** «Меры обеспечения безопасности и защиты персональных данных, рекомендуемые для федеральных информационных систем и организаций» (Security and Privacy Controls for Federal Information Systems and Organizations)
- **NIST SP 800-144** «Руководство по обеспечению безопасности и защиты персональных данных при использовании публичных облачных вычислений» (Guidelines on Security and Privacy in Public Cloud Computing)
- **NIST SP 800-122** «Руководство по защите конфиденциальности персональных данных» (Guide to Protecting the Confidentiality of Personally Identifiable Information (PH))
- **NIST SP 800-188** «Деидентификация государственных наборов данных» (De-Identifying Government Datasets)

Китай
Закон о защите личной информации
Personal Information Protection Law (PIPL)

Законы КНР

- **Закон о защите личной информации (Personal Information Protection Law).** Документ впервые устанавливает исчерпывающий набор правил по сбору и защите ПД и может применяться к зарубежным обработчикам.

- **Закон о безопасности данных (Data Security Law).** Сфокусирован на защите национальной безопасности Китая. Идея закона заключается в создании всеобъемлющей системы защиты данных, управляемой государством.

Законы КНР

- **Гражданский кодекс.** Закрепляет право на неприкосновенность частной жизни и принципы защиты личной информации. Он устанавливает правовую основу для обработки ПД, обязанности для операторов ПД, права отдельных лиц на их личную информацию и обязанности административных органов по сохранению, неразглашению и нераспространению данных, полученных ими в ходе выполнения должностных регламентов.

Дополнительные материалы по теме

- Защита личной информации должна стать новой нормой в Китае (05.2021) https://prc.today/zashhita-lichnoj-informaczii-dolzhna-stat-novoj-normoj-v-kitae/
- Personal Information Protection Law of the PRC (2nd Deliberation Draft) (04.2021) https://www.chinalawtranslate.com/en/pipl-draft-2/
- Регулирование персональных данных в Китае (05.2021) https://prc.today/regulirovanie-personalnyh-dannyh-v-kitae/
- Работодатели в Китае должны подготовиться в соответствии с проектом PIPL (02.2021) https://prc.today/rabotodateli-v-kitae-dolzhny-podgotovitsya-v-sootvetstvii-s-proektom-pipl/
- Анализ политики Китая в киберпространстве (06.2021) https://rdc.grfc.ru/2021/06/china_cyberpolicy/
- China's draft Personal Information Protection Law ("PIPL") – why it is, and isn't, like the GDPR (11.2020) https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/china-draft-personal-information-protection-law-pipl

Австралия
Australian Privacy Law and Practice (ALRC 108)

Дополнительные материалы по теме

- For Your Information: Australian Privacy Law and Practice (ALRC Report 108) https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/

- Законы Южного полушария: австралийские чиновники хотят получить доступ ко всем данным пользователей (2018) https://www.forbes.ru/tehnologii/370843-zakony-yuzhnogo-polushariya-avstraliyskie-chinovniki-hotyat-poluchit-dostup-ko

Индия
PDPB (Personal Data Protection Bill)

Дополнительные материалы по теме PDPB

- The Personal Data Protection Bill, 2019
  https://prsindia.org/billtrack/the-personal-data-protection-bill-2019
  https://prsindia.org/files/bills_acts/bills_parliament/Personal%20Data%20Protection%20Bill,%202019.pdf

- Personal Data Protection Bill, 2019
  https://en.wikipedia.org/wiki/Personal_Data_Protection_Bill,_2019

- The Personal Data Protection Bill, 2019 and its repercussions
  https://blog.ipleaders.in/personal-data-protection-bill/

Немного аналитики

Исследование утечек информации ограниченного доступа в 2020 году – Аналитика InfoWatch

- **В 2020 году** специалистами Экспертно-аналитического центра InfoWatch **зафиксировано 2395 утечек данных** из коммерческих, некоммерческих (государственных, муниципальных) организаций в различных странах мира. Это на 4,5% меньше, чем в 2019 году (2509 утечек), но на 5,8% превышает показатели 2018 года (2263).
- **За 2018-2020 гг. сохраняются тенденции роста доли утечек умышленного характера** (внешних и внутренних) и снижения доли утечек внутреннего характера.
- **Общая доля умышленных утечек ПДн выросла с 60,2% до 72,5%**

Исследование утечек информации ограниченного доступа в 2020 году – Аналитика InfoWatch

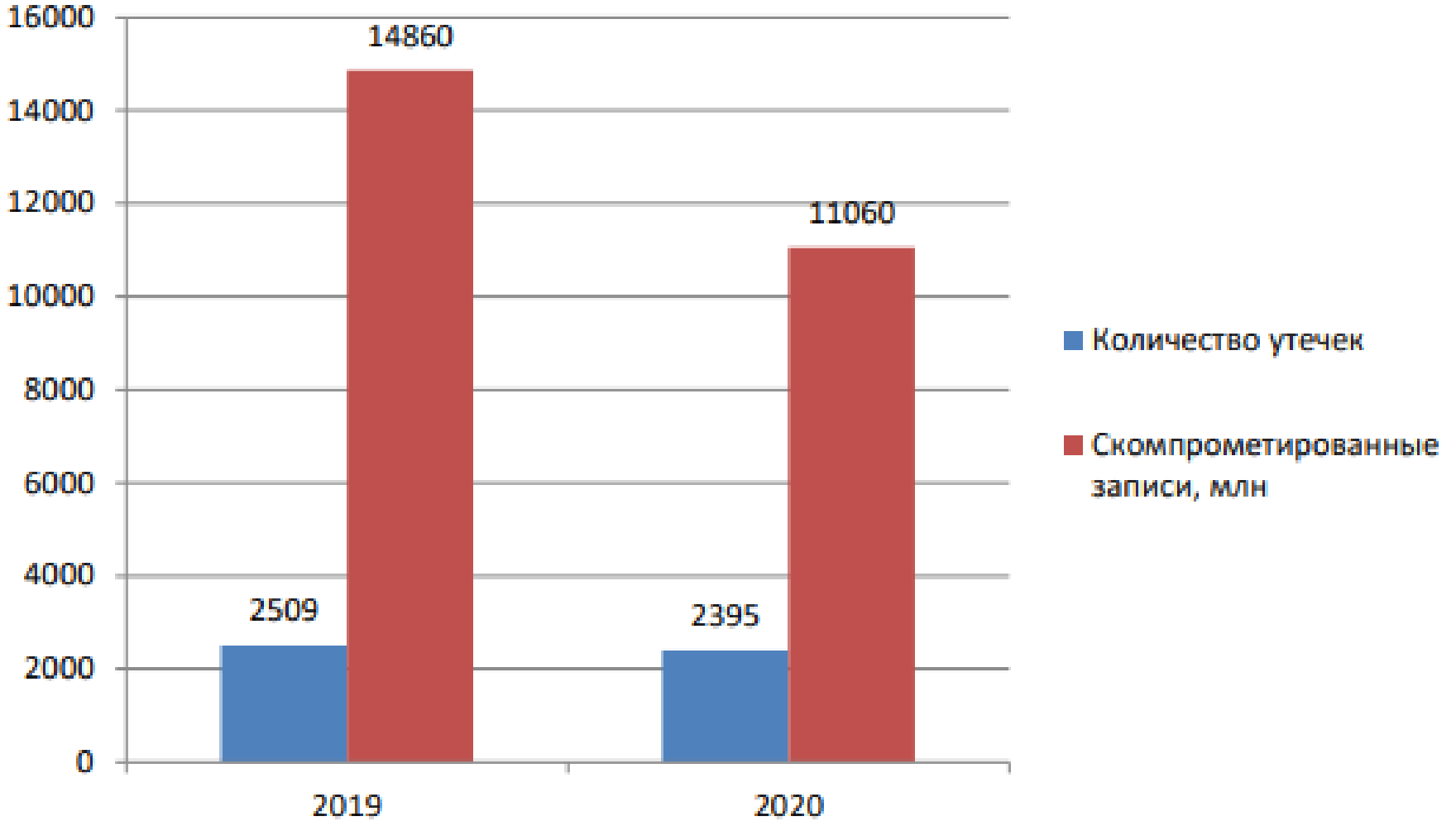
- Доля **утечек платежной информации** (как умышленных, так и неумышленных) продолжает падать, в 2020 г. по сравнению с 2019 г. она сократилась в 2 раза, по сравнению с 2018 – более чем 3 раза.
- **55,9%** утечек были спровоцированы внешними нарушителями, **44,1%** - внутренними.
- **35,4%** утечек стали результатом действий и бездействия непривилегированных сотрудников.
- **Более 11 млрд записей ПДн и платежной информации оказалось скомпрометировано** за прошлый год, что по сравнению с 2019 годом снизилось более чем на 25%.

Исследование утечек информации ограниченного доступа в 2020 году – Аналитика InfoWatch

- **4,62 млн записей** в среднем было скомпрометировано в результате одной утечки. Это на 22% меньше, чем в 2019 году.
- **В 2020 году было зафиксировано 84 утечки, в результате каждой из которых «утекло» более 10 млн записей.** Совокупно на такие разрушительные утечки пришлось 95,7% всех скомпрометированных записей.
- В общей совокупности утечек с числом утекших записей менее 1 млн каждая, **в 2020 году на каждую утечку в среднем пришлось 28,1 тыс. записей**, тогда как в 2019 году на подобную утечку в среднем приходилось 19,9 тыс. записей.
- В 2020 году **2,8 млн** записей в среднем пришлось на утечку внешнего характера, **6,8 млн** записей – на утечку внутреннего характера.
- Более **79% утечек** происходит через Сеть

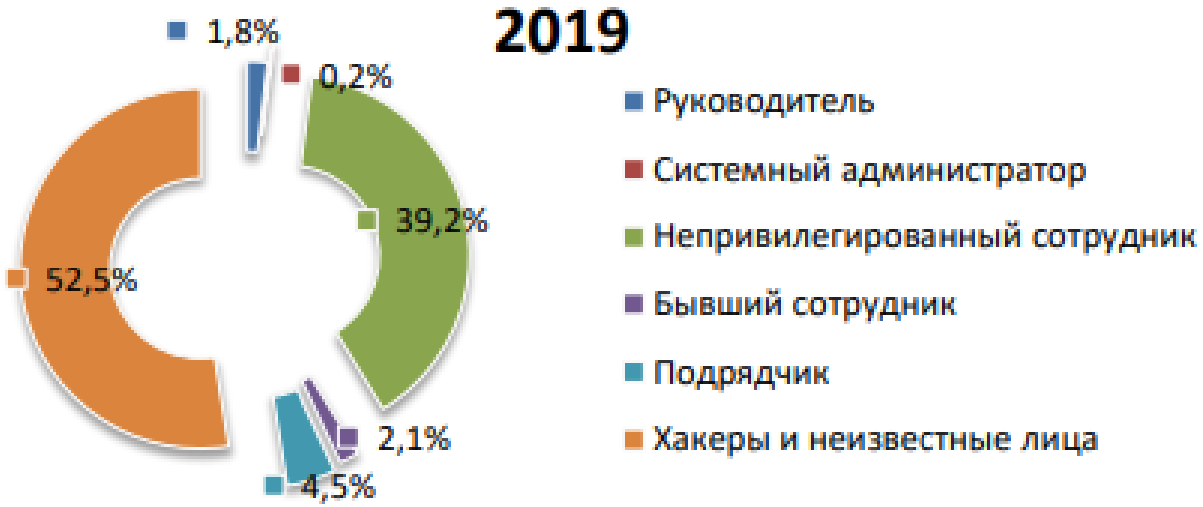
INFOWATCH®

Исследование утечек информации ограниченного доступа в 2020 году – Аналитика InfoWatch

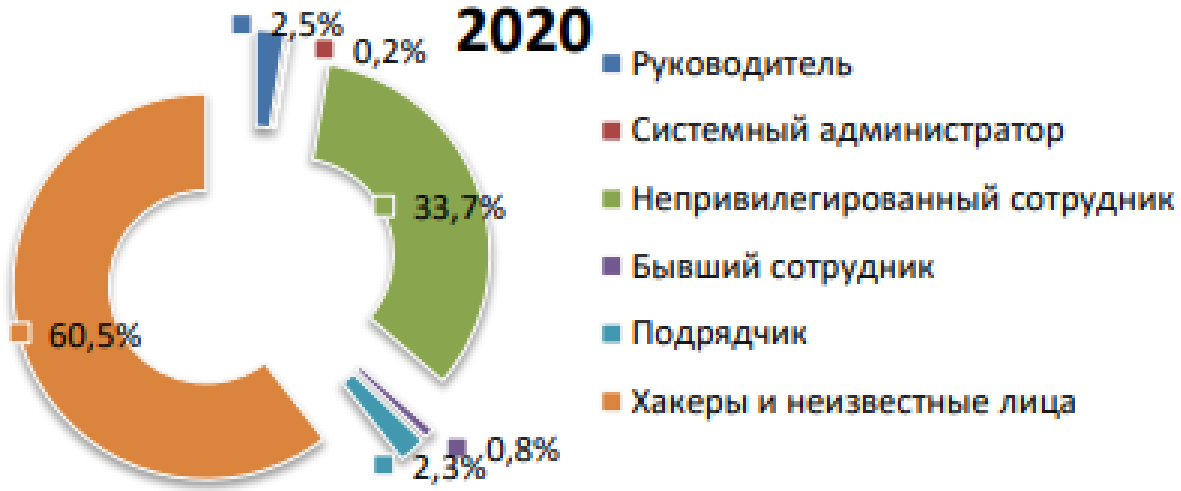


Число утечек информации и объем персональных данных, скомпрометированных в результате утечек. 2019 - 2020 гг.

Исследование утечек информации ограниченного доступа в 2020 году – Аналитика InfoWatch



Распределение утечек по источнику (виновнику), 2019-2020 гг



INFOWATCH®

Исследование утечек информации ограниченного доступа в 2020 году – Аналитика InfoWatch

Распределение утечек по типам данных, 2019-2020 гг

INFOWATCH®

Некоторые Новости о персональных данных и их утечках

Наиболее масштабные утечки в РФ: 2023

- **В 2023 году в России стали чаще утекать крупные базы данных (от 1 млн записей ПДн).**
- Например, в апреле с вероломной и масштабной атакой столкнулся сервис Kassy.ru по продаже билетов на зрелищные мероприятия. Украинские хакеры украли в общей сложности около 14 млн строк данных. Скомпрометированы ФИО, адреса электронной почты, телефоны, идентификаторы и даты приобретения билетов. У некоторых пользователей утекли даты рождения.

- Летом 2023 года неизвестный хакер разместил в открытом доступе данные **7,8 млн клиентов сети гипермаркетов «Ашан»**. В опубликованном файле содержатся имена и фамилии, номера телефонов, адреса электронной почты, адреса доставки и самовывоза.

Наиболее масштабные утечки в РФ: 2023

- **2 миллиона строк**, содержащих пароли, логины и электронные адреса клиентов хакеры похитили в результате взлома баз данных сети косметических магазинов «Подружка».
- **3,5 миллиона строк из баз данных Mail.ru** попали в открытый доступ вследствие преступных действий хакерской группы NLB. «Слитая» часть данных сервиса содержит имена, почтовые адреса и телефонные номера пользователей. По заявлениям представителей NLB, общий объем похищенных данных составляет около 2 миллиардов строк, однако оставшиеся данные группировка не публиковала.
- Злоумышленники не обошли своим вниманием и сферу образования. После атаки на **сервисы «Российской электронной школы» в сети оказалось около 9 миллионов уникальных строк с чувствительными данными сотрудников и учеников**.

Наиболее масштабные утечки в РФ: 2023

- В публичный доступ попала **часть баз данных ОАО «РЖД».** Злоумышленники выложили более миллиона уникальных строк, содержащих паспортные данные пассажиров, сведения о купленных билетах и другую информацию. Ранее сервисы компании подвергались массированной DDoS-атаке, из-за чего была нарушена работа мобильного приложения, сайта и ряда виртуальных сервисов.
- **14 миллионов строк** с ФИО, логинами, паролями и датами рождения были опубликованы киберпреступниками в результате взлома **сервиса kassy.ru**.
- Хакерская группировка NLB взломала базы данных **МТС Банка**. Злоумышленники заявили об успешном хищении **21 миллиона строк**, однако в публичный доступ выложили только 1 миллион.

Наиболее масштабные утечки в РФ: 2023

- Более **30 миллионов строк** было украдено и опубликовано после масштабной июньской атаки на **несколько крупных сетей ритейлеров**.
- **99 миллионов строк** — таков объем утечки ПДн из-за взлома **базы данных клиентов сети магазинов «Спортмастер»**. Помимо телефонных номеров, электронных адресов и имен «слитый» архив также содержит даты рождения клиентов.

Утекли персональные данные более 60 млн американцев - 06 августа 2021

- **Маркетинговая компания OneMoreLead, работающая на B2B-рынке, оставила в облаке незащищенную базу данных, в которой хранились персональные данные граждан США. Всего в скомпрометированной базе оказались персональные данные по меньшей мере 63 млн человек, пишет портал Techaeris со ссылкой на отчет vpnMentor.**
- В пресс-релизе компания vpnMentor сообщила, что ее исследователи безопасности обнаружили открытый сервер Amazon Web Services еще 16 апреля. Выяснилось, что скомпрометированное хранилище объемом 34 ГБ принадлежало компании OneMoreLead. Достоянием общественности могли стать имена, адреса электронной почты и данные о рабочих местах десятках миллионов американцев. **Предположительно в базе было 126 млн записей персональных данных, число пострадавших граждан США оценивается как минимум в 63 млн человек.** Спустя четыре дня исследователи связались с компанией OneMoreLead, а та, в свою очередь, оповестила об утечке компанию Amazon, в облачной среде которой размещалось хранилище данных.
- Судя по всему, маркетинговый стартап был ограничен в ресурсах и не смог обеспечить безопасность информации. Если оставленные без защиты персональные данные окажутся в руках мошенников, это может вызвать волну фишинговых атак на американских граждан, поэтому безопасность информации так важна.
- Исследователи vpnMentor подчеркивают, что идентифицировать OneMoreLead как оператора найденных данных оказалось несложно. Однако, до сих пор остается загадкой происхождение этой информации и то, каким образом она оказалась у OneMoreLead. Дело в том, что эта компания была основана совсем недавно, в 2020 году. Маловероятно, что небольшой стартап мог за короткий срок собрать персональные данные десятков миллионов человек, если только люди, основавшие компанию, не работали в аналогичном бизнесе ранее.
- Кроме того, утекшие из OneMoreLead данные имеют странное сходство с теми записями, которые в 2020 г. предположительно утекли из немецкой маркетинговой компании Leadhunter. Впрочем, представители Leadhunter тогда отрицали факт утечки.
- https://www.infowatch.ru/analytics/utechki-informatsii/utekli-personalnye-dannye-bolee-60-mln-amerikantsev

Персональные данные миллионов индонезийцев проданы хакерами - 03 августа 2021

- В даркнете хакеры реализовали похищенные персональные данные клиентов страховой компании BRI Life. Вероятно, эти персональные данные были получены хакерами в результате взлома компьютеров сотрудников BRI, передает KrAsia.
- Элон Гал (Alon Gal), соучредитель и технический директор компании Hudson Rock, занимающейся разведкой в сфере киберпреступлений, в конце июля сообщил в своем Твиттере, что в подпольном сегменте Сети **продается конфиденциальная информация порядка 2 млн граждан Индонезии. Цена полного пакета этой конфиденциальной информации составила $7000.**
- Выяснилось, что неизвестные киберпреступники украли персональные данные из компании BRI Life, страховом подразделении крупнейшего в стране кредитного учреждения BRI. Произошла утечка по меньшей мере 463 тыс. различных документов, содержащих такие персональные данные, как сведения о национальных удостоверений личности, номера налогоплательщиков, фотографии банковских книжек, свидетельства о рождении и медицинские записи. По словам Гэла, хакеры получили эти данные, взломав компьютеры менеджеров BRI Life.
- Представители пострадавшей компании пока не раскрывают детали инцидента. Генеральный директор BRI Life сообщил журналистам, что продолжается расследование. Для проведения соответствующих мероприятий привлечена команда независимых специалистов в области кибербезопасности.
- Крупные предприятия и государственные организации Индонезии все чаще становятся объектами хакерских атак. **В мае 2021 г. злоумышленникам удалось взломать сервер BPJS Kesehatan, агентства по здравоохранению и социальному обеспечению. В результате были украдены персональные данные более 270 млн индонезийцев.**
- В прошлом году в Индонезии произошли как минимум семь крупных утечек конфиденциальной информации. В частности, жертвами утечек стали технологические компании Tokopedia и Bukalapak, кредитный провайдер KreditPlus, а также государственная избирательная комиссия.
- https://www.infowatch.ru/analytics/utechki-informatsii/personalnye-dannye-millionov-indoneziytsev-prodany-khakerami

Украдена конфиденциальная информация 3,3 млн клиентов Volkswagen - 18 июня 2021

- Немецкий автомобилестроительный концерн Volkswagen и его дочерняя компания Audi потеряли конфиденциальную информацию. Автопроизводители уведомили **более 3 млн заказчиков из Северной Америки о том, что конфиденциальная информация оказалась скомпрометирована** по вине подрядчика, отмечает Bank InfoSecurity.
- Согласно сообщению Volkswagen AG, в наихудших случаях у клиентов утекла такие персональные данные, как имена, почтовые адреса, а также адреса электронной почты и номера телефонов. Инцидент, в результате которого были похищены персональные данные, произошел из-за непреднамеренных действий персонала компании, которая предоставляла концерну Volkswagen маркетинговые услуги. Известно, что эта компания хранила у себя данные автопроизводителя, собранные в период с 2014 по 2019 гг.
- Известно, что около 163 тыс. пострадавших людей живут в Канаде, остальные являются резидентами США. Примерно у 90 тыс. американцев утекли номера водительских удостоверений. Вероятно, у части этих людей также были скомпрометированы даты рождения, номера социального страхования (SSN), номера кредитных договор и номера налогоплательщиков.

- https://www.infowatch.ru/analytics/utechki-informatsii/ukradena-konfidentsialnaya-informatsiya-3-3-mln-klientov-volkswagen

Незащищенные данные 10 млн. пользователей - 20 ноября 2020

- **The Threat Post:** Аналитики компании vpnMentor обнаружили в облаке несколько незащищенных баз данных, относящихся к религиозному приложению Pray.com.
- В кластерах сервиса Amazon исследователи насчитали более **1,9 млн различных файлов общим объемом 262 ГБ.** Большая часть скомпрометированных данных представляли внутренние документы, однако один из кластеров содержал порядка **80 тыс. файлов с персональными данными** подписчиков приложения. **Число людей, которых затронула эта утечка, vpnMentor оценивает в 10 миллионов**. В файлах были списки приходов, с подробной информацией о каждом прихожанине, включая имена, домашний и электронный адреса, номера телефонов и семейное положение. По словам исследователей, самое неприятное в этой утечке то, что были скомпрометированы телефонные справочники пользователей
- https://threatpost.com/10m-impacted-pray-com-data-exposure/161459/

Утечка данных более чем 20 миллионов пользователей – 9 ноября 2020

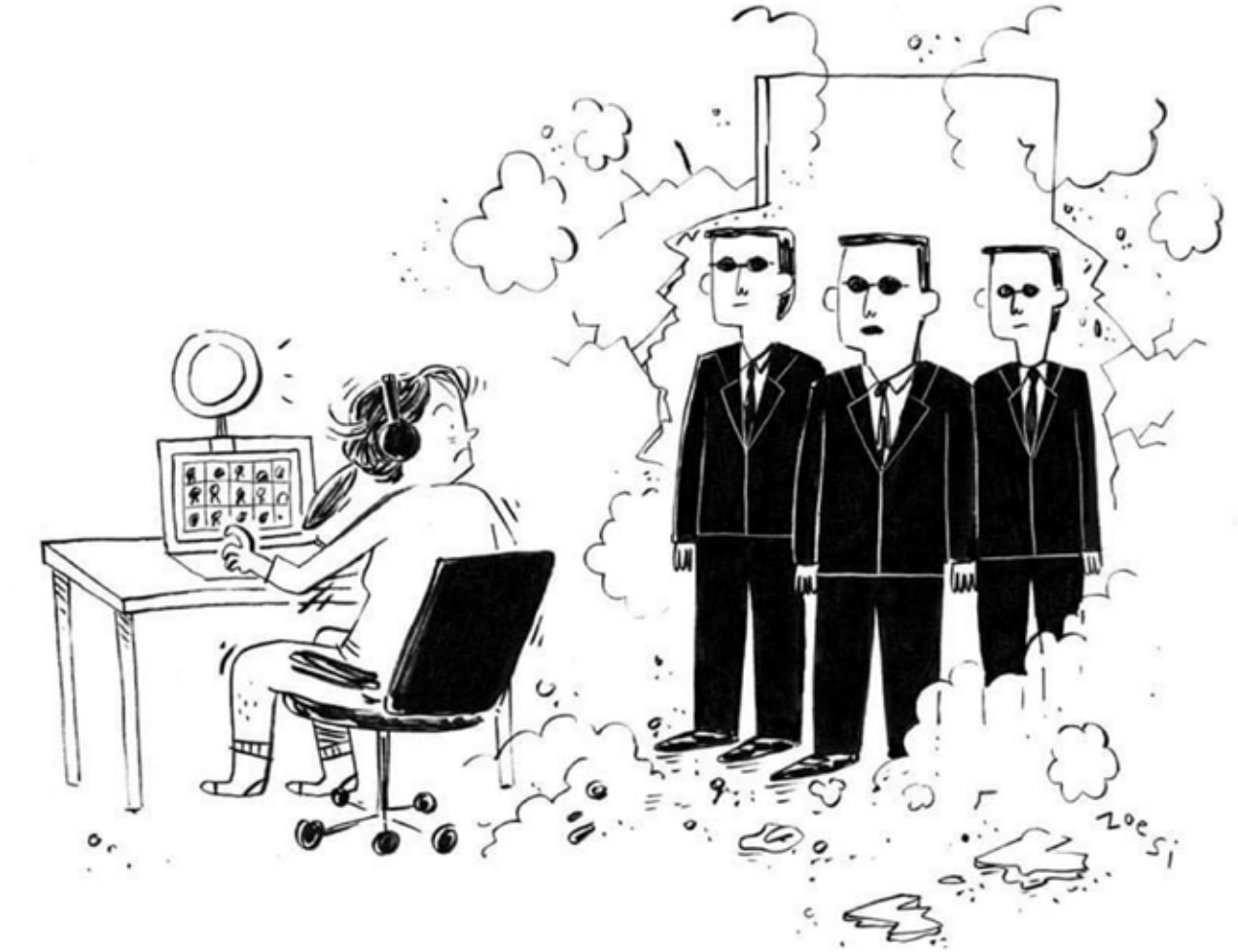
- **Business Insider:** Исследователи безопасности обнаружили на черном рынке объявление о продаже данных порядка **20 млн клиентов индийской службы доставки продуктов BigBasket**. База данных стартапа **продается за $40 тыс**. По данным Cyble, украденные в BigBasket данные могут включать имена пользователей, адреса электронной почты, хэшированные пароли, пин-коды, контактные номера, адреса, даты рождения, сведения о местоположении и IPадреса.
- https://www.businessinsider.in/business/startups/news/bigbasket-the-e-grocery-startup-which-tata-group-is-eyeing-admits-a-data-breach-of-over-20-million-users/articleshow/79122791.cms

Европарламент утвердил массовый надзор за частными сообщениями

- **Европейский парламент одобрил** постановление **Chatcontrol — частичное нарушение конфиденциальности, позволяющее поставщикам услуг электронной почты и обмена сообщениями автоматически искать во всех личных сообщениях каждого пользователя предполагаемый подозрительный контент и сообщать о подобных случаях в полицию**.
- Делегация Европейской пиратской партии, входящей в состав фракции ЕП «Зеленые — Европейский свободный альянс», решительно осуждает автоматическое массовое наблюдение, которое фактически означает конец конфиденциальности в цифровой переписке. Депутаты Европарламента от Европейской пиратской партии планируют подать в суд.
- В ходе голосования **537 членов Европейского парламента одобрили Chatcontrol**, 133 голосовали против и 24 воздержались. По данным полиции, в подавляющем большинстве случаев невиновные граждане попадают под подозрение в совершении правонарушения из-за ненадежных процедур.
- **«Принятие первого в ЕС постановления о массовой слежке — печальный день для всех, кто полагается на бесплатные и конфиденциальные сообщения и советы, включая жертв насилия и информаторов СМИ.** Постановление наносит смертельный удар по конфиденциальности цифровой переписки», — сообщил член Европейского парламента от Немецкой пиратской партии Патрик Брейер (Patrick Breyer).

Европарламент утвердил массовый надзор за частными сообщениями https://www.securitylab.ru/news/523222.php

Европарламент утвердил массовый надзор за частными сообщениями



Вы упомянули название значимого объекта КИИ 3 раза.
Вам придется пройти с нами!

КИИ – Критически важная инфраструктура


-Защитим
от супостата
персональные
данные!
Zasmeshi.Ru

Защита информации

Тема: Защита персональных данных

Благодарю за внимание

КУТУЗОВ Виктор Владимирович

Белорусско-Российский университет, Кафедра «Программное обеспечение информационных технологий»
Республика Беларусь, Могилев, 2024

Список использованных источников

1. Рабочая программа дисциплины «Защита информации» / Кутузов В.В. – Могилев : Белорусско-Российский университет, 2019
2. Фотографии и картинки взяты с сайтов Яндекс.Картинки и Гугл.Картинки, иконки с flaticon.com
3. Закон от 07.05.2021 № 99-З «О защите персональных данных»
   https://pravo.by/upload/docs/op/H12100099_1620939600.pdf
4. Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных«
   http://www.kremlin.ru/acts/bank/24154
   http://www.consultant.ru/document/cons_doc_LAW_61801/
5. Постановление Правительства РФ от 29 июня 2021 г. № 1046
   «О федеральном государственном контроле (надзоре) за обработкой персональных данных»
   https://www.garant.ru/products/ipo/prime/doc/401316524/
6. Приказ Роскомнадзора от 24.02.2021 N 18 «Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения»
   http://publication.pravo.gov.ru/Document/View/0001202104210039
7. Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 21 октября 2020 года № 395/НҚ «Об утверждении правил сбора, обработки персональных данных».
   https://www.tadviser.ru/index.php/Статья:Обработка_персональных_данных_в_Казахстане
   https://online.zakon.kz/Document/?doc_id=39051375#pos=2;-52
8. Закон України. Про захист персональних даних (Відомості Верховної Ради України (ВВР), 2010, № 34, ст. 481)
   https://zakon.rada.gov.ua/laws/show/2297-17#Text
   https://zakon.rada.gov.ua/laws/show/3454-17#Text

Список использованных источников

9. Комментарий к Закону от 07.05.2021 № 99-З «О защите персональных данных» https://bii.by/tx.dll?d=456664
10. ПОСТАНОВЛЕНИЕ МИНИСТЕРСТВА ЗДРАВООХРАНЕНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ 17 июня 2019 г. № 60 Об изменении постановления Министерства здравоохранения Республики Беларусь от 31 октября 2007 г. № 99 https://pravo.by/upload/docs/op/W21934489_1566594000.pdf
11. Кодекс Республики Беларусь «Об административных правонарушениях» https://pravo.by/document/?guid=3871&p0=HK2100091
12. Уголовный Кодекс Республики Беларусь https://pravo.by/document/?guid=3871&p0=Hk9900275
13. Белорусские и мировые тренды развития законодательств о приватности (май 2021) https://www.youtube.com/watch?v=kYh6Mfd2k6w
14. Персональные данные и репутация компаний: показательные кейсы. (август 2021) https://www.youtube.com/watch?v=Yq1d1yJKoPg
15. Какими нормами и законами регулируется защита персональных данных? https://habr.com/ru/company/digitalrightscenter/blog/569900/
16. Федеральный закон от 8 июня 2020 г. № 168-ФЗ «О едином федеральном информационном регистре, содержащем сведения о населении Российской Федерации» https://www.garant.ru/products/ipo/prime/doc/74132857/
17. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» http://www.kremlin.ru/acts/bank/24157

Список использованных источников

18. Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» https://zags.mosreg.ru/upload/iblock/095/postanovlenie-ot-01.11.2011.doc
19. Сервис Роскомнадзора для операторов персональных данных (ПД), позволяющий сформировать шаблон формы согласия на обработку ПД, разрешенных субъектом для распространения. https://rkn.gov.ru/news/rsoc/news73724.htm
20. Новое в Законе «О персональных данных» 2021. Что нас ждет? https://mediapravo.com/privacy/rasprostranenie-pd.html
21. Согласие на распространение персональных данных —требования Роскомнадзора https://mediapravo.com/privacy/soglasie-na-rasprostrnenie-personalnih.html
22. Персональные данные в 2021: как компаниям с ними работать и не получать штрафы https://rb.ru/opinion/personal-data-2021/
23. Обезличивание персональных данных: пошаговый алгоритм для кадровика https://www.kdelo.ru/art/386102-obezlichivanie-personalnyh-dannyh-21-m6
24. Новые штрафы за нарушение персональных данных в 2021 году https://www.kdelo.ru/art/386058-novye-shtrafy-za-narushenie-personalnyh-dannyh-21-m03
25. General Data Protection Regulation (GDPR). Текст на русском языке - Регламент (EU) 2016/679 https://gdpr-text.com/ru/
26. Директива (EU) 2016/680 https://ogdpr.eu/ru/gdpr-2016-680

Список использованных источников

27. Разъяснения. Официальные руководства и разъяснения, заключения и рекомендации общеевропейского надзорного органа в области защиты персональных данных (EDPB — Европейского совета по защите персональных данных или Art29WP — Рабочей группы 29-ой статьи). Переводы на русский язык. https://gdpr-text.com/ru/guidelines/
28. Регламент Европейского Парламента и Совета Европейского Союза 2016/679 от 27 апреля 2016 г. «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС» (Общий Регламент о защите персональных данных). (General Data Protection Regulation) (GDPR) http://www.eurasiancommission.org/ru/act/texnreg/depsanmer/consumer_rights/Documents/Регламент%20Европейского%20Парламента%20и%20Совета%20Европейского%20Союза%202016%20679%20от%2027%20апр.pdf
29. Вебинар по глобальным изменениям в 152 ФЗ (апрель 2021) https://www.youtube.com/watch?v=mWMSPFL-fwQ
30. General Data Protection Regulation (GDPR). Оригинал на английском - Регламент (EU) 2016/679 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679
31. Как защитить персональные данные в соответствии с GDPR https://www.osp.ru/cio/2017/07/13052957
32. Международные стандарты и Регламент ЕС по защите данных https://gosstandart.gov.by/international-standards-and-eu-regulation-on-data-protection
33. Информация о GDPR на русском языке https://ogdpr.eu/ru#__GDPR
34. Штрафуют даже GOOGLE. Ошибки в GDPR за 2 года. (май 2020) https://www.youtube.com/watch?v=GHQ5pgdJT3c

Список использованных источников

35. Privacy Act of 1974. Закон «О защите конфиденциальности»
https://en.wikipedia.org/wiki/Privacy_Act_of_1974
https://www.justice.gov/opcl/privstat.htm

36. Privacy Protection Act of 1980. Закон «О защите информации»
https://en.wikipedia.org/wiki/Privacy_Protection_Act_of_1980
https://epic.org/privacy/ppa/

37. SP 800-122 «Руководство по защите конфиденциальности персонально идентифицируемой информации» (Guide to Protecting the Confidentiality of Personally Identifiable Information (PII))
http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

38. SP 800 Series
https://csrc.nist.gov/publications/sp
https://csrc.nist.gov/publications/sp800
https://www.pvsm.ru/informatsionnaya-bezopasnost/23835

37. California Consumer Privacy Act
https://oag.ca.gov/privacy/ccpa
https://en.wikipedia.org/wiki/California_Consumer_Privacy_Act

38. California Consumer Privacy Act: новый тренд США по защите персональных данных в 2020 году
https://uz.ligazakon.ua/magazine_article/EA013372

39. Калифорнийский закон о конфиденциальности потребителей вступает в силу с 1 января 2020 года
https://vc.ru/legal/94782-kaliforniyskiy-zakon-o-konfidencialnosti-potrebiteley-vstupaet-v-silu-s-1-yanvarya-2020-goda

Список использованных источников

40. Защита личной информации должна стать новой нормой в Китае (05.2021) https://prc.today/zashhita-lichnoj-informaczii-dolzhna-stat-novoj-normoj-v-kitae/
41. Personal Information Protection Law of the PRC (2nd Deliberation Draft) (04.2021) https://www.chinalawtranslate.com/en/pipl-draft-2/
42. Регулирование персональных данных в Китае (05.2021) https://prc.today/regulirovanie-personalnyh-dannyh-v-kitae/
43. Работодатели в Китае должны подготовиться в соответствии с проектом PIPL (02.2021) https://prc.today/rabotodateli-v-kitae-dolzhny-podgotovitsya-v-sootvetstvii-s-proektom-pipl/
44. Анализ политики Китая в киберпространстве (06.2021) https://rdc.grfc.ru/2021/06/china_cyberpolicy/
45. China's draft Personal Information Protection Law ("PIPL") – why it is, and isn't, like the GDPR (11.2020) https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/china-draft-personal-information-protection-law-pipl
46. For Your Information: Australian Privacy Law and Practice (ALRC Report 108) https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/
47. Законы Южного полушария: австралийские чиновники хотят получить доступ ко всем данным пользователей (2018) https://www.forbes.ru/tehnologii/370843-zakony-yuzhnogo-polushariya-avstraliyskie-chinovniki-hotyat-poluchit-dostup-ko
48. The Personal Data Protection Bill, 2019 https://prsindia.org/billtrack/the-personal-data-protection-bill-2019 https://prsindia.org/files/bills_acts/bills_parliament/Personal%20Data%20Protection%20Bill,%202019.pdf

Список использованных источников

49. Personal Data Protection Bill, 2019
https://en.wikipedia.org/wiki/Personal_Data_Protection_Bill,_2019
50. The Personal Data Protection Bill, 2019 and its repercussions
https://blog.ipleaders.in/personal-data-protection-bill/
51. Новое в Законе «О персональных данных» 2021. Что нас ждет?
https://mediapravo.com/privacy/rasprostranenie-pd.html
52. Персональные данные в 2021: как компаниям с ними работать и не получать штрафы
https://rb.ru/opinion/personal-data-2021/
53. Техническая защита ПДн в соответствие с GDPR и ФЗ-152 (презентация)
https://www.securitylab.ru/blog/personal/Business_without_danger/348404.php
54. В Беларуси за разглашение персональных данных будут наказывать штрафом. Новые правила заработают с 1 марта
https://kurjer.info/2021/01/26/fine-5/
55. Экспертная интерпретация "Закона о безопасности данных" вносит свой вклад в китайскую мудрость и китайские решения для глобального управления безопасностью данных (15 Июня 2021)
http://www.cac.gov.cn/2021-06/15/c_1625341228851523.htm
56. Роскомнадзор о персональных данных в 2021
https://mediapravo.com/privacy/rkn-personal-data.html
57. «Пробивка» человека — незаконный сбор персональных данных
https://mediapravo.com/privacy/probivka-cheloveka-nezakonnyj-sbor-personalnyh-dannyh.html

Список использованных источников

58. Что меняется в работе парсеров с 1 марта 2021 г https://mediapravo.com/privacy/parsing-i-personalnie-dannye.html
59. Информационная система Роскомнадзора для согласий на распространение персональных данных https://mediapravo.com/privacy/informatsionnaya-sistema-roskomnadzora.html
60. Персональные данные соискателей в резюме — правила обработки https://mediapravo.com/privacy/personalnie-dannie-soiskatelei.html
61. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). Список опубликованных правовых актов http://publication.pravo.gov.ru/SignatoryAuthority/foiv291
62. Конвенция о защите физических лиц при автоматизированной обработке персональных данных ETS от 28.01.1981 № 108 https://rppa.ru/npa/ets108_28.01.1981
63. ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines https://www.iso.org/standard/71670.html
64. Порядок обработки персональных данных, разрешённых для распространения https://www.anti-malware.ru/analytics/Personal-data-allowed-for-dissemination
65. Общий регламент по защите данных https://ru.wikipedia.org/wiki/Общий_регламент_по_защите_данных
66. GDPR новый регламент Евросоюза по защите данных: Актуально для белорусского бизнеса https://www.bakertilly.by/upload/iblock/34b/34bb7c2a08e29861c0684aad76ebc8bc.pdf

Список использованных источников

67. securiti.ai
https://securiti.ai/

68. securiti.ai – Блог со статьями по защите персональных данных во всех странах мира
https://securiti.ai/blog/

69. Персональные данные и всё, что о них нужно знать (07.2021)
https://habr.com/ru/post/568364/

70. Практика реализации норм GDPR и реакция заинтересованных лиц
https://aebrus.ru/upload/iblock/3ac/presentation_general-data-protection-regulation.pdf

71. Proposal 2017/0228 (COD) for a Regulation on a framework for the free flow of non-personal data in the European Union
https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2017)495&lang=ru

72. Framework for the free flow of non-personal data in the EU
https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_4249

73. ENISA Publications
https://www.enisa.europa.eu/publications#c5=2011&c5=2021&c5=false&c2=publicationDate&reversed=on&b_start=0

74. Revera - Защита персональных данных. Ключевые тезисы для бизнеса
https://revera.by/uploads/files/2020/zashhita-personalnyx-dannyx-klyuchevye-tezisy-dlya-biznesa.pdf

75. База отчетов, исследований и мнений от Совета Европы по защите персональных данных
https://www.coe.int/en/web/data-protection/reports-studies-and-opinions

Список использованных источников

76. EU negotiators reach a political agreement on free flow of non-personal data
https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4227

77. Data protection, privacy and new technologies
https://fra.europa.eu/en/themes/data-protection-privacy-and-new-technologies

78. Handbook on European data protection law - 2014 edition
https://fra.europa.eu/en/publication/2014/handbook-european-data-protection-law-2014-edition
https://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf

79. Handbook on European data protection law - 2018 edition
https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition
https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf

80. Deloitte - General Data Protection Regulation (GDPR) Почему это так важно?
https://www2.deloitte.com/content/dam/Deloitte/ru/Documents/risk/gdpr.pdf

81. ПДн. Лучшие практики ENISA по защите персональных данных
https://www.securitylab.ru/blog/personal/sborisov/343462.php

82. The European Union Agency for Cybersecurity (ENISA)
https://www.enisa.europa.eu

83. Guidelines for SMEs on the security of personal data processing
https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing
https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing/at_download/fullReport

Список использованных источников

84. Trialog - Standards for Privacy-by-design
https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201901/Documents/Antonio_Kung_Presentation.pdf

85. База сведений о штрафов за нарушение GDPR
https://www.enforcementtracker.com

86. Документы по Защите персональных данных в РФ
https://www.sps-ib.ru/materialy:pdn

87. Каталог категорий персональных данных
https://www.sps-ib.ru/analitika:katalog_pdn

88. Европарламент утвердил массовый надзор за частными сообщениями
https://www.securitylab.ru/news/523222.php

89. Защита персональных данных. Полный комплект локальных документов медорганизации, которые защитят от штрафов https://book.zdrav.ru/files/book/28_pdf.pdf

90. Рассмотрение механизмов и специфики применения Генерального регламента ЕС о защите данных (GDPR) - Алексей Мунтян
Редакция от 01.10.2023 – 1057 с. https://rppa.ru/_media/analitika/gdpr_01.10.2023.pdf
Редакция от 29.12.2022 – 822 с. https://rppa.ru/_media/analitika/gdpr_29.12.2022.pdf
Редакция от 05.07.2021 – 532 с. https://rppa.ru/_media/analitika/gdpr_05.07.2021.pdf
Редакция от 28.12.2020 – 444 с. https://rppa.ru/_media/world/gdpr_28.12.2020.pdf
Редакция от 23.12.2019 – 250 с. https://www.sps-ib.ru/gdpr.pdf

Список использованных источников

91. Книги и статьи по теме «Защита персональных данных (ПДн)» https://www.studmed.ru/science/informatics/informacionnaya-bezopasnost/privacy
92. Уголовная ответственность за незаконные действия с персональными данными в Республике Беларусь (30.06.2021) https://pravo.by/novosti/novosti-pravo-by/2021/june/65098/
93. Конец сквозному шифрованию в мессенджерах: что такое Chatcontrol от ЕС и чем он опасен? https://kod.ru/chatcontrol-eu/
94. Apple будет проверять фотографии пользователей для защиты детей https://kod.ru/apple-child-safety/
95. Конец сквозному шифрованию в мессенджерах: что такое ChatControl от ЕС и чем он опасен? https://recode.press/article/4103/
96. MESSAGING AND CHAT CONTROL. The End of the Privacy of Digital Correspondence https://www.patrick-breyer.de/en/posts/message-screening/
97. Apple заявила, что почта iCloud сканируется на наличие CSAM с 2019 года (23.08.2021) https://kod.ru/apple-scans-icloud-mail/
98. Комментарий к Закону Республики Беларусь от 07.05.2021 № 99-З «О защите персональных данных». Н.И. Лимож, юрист, 01.07.2021
99. Исследование утечек информации ограниченного доступа в 2020 году – Аналитика InfoWatch https://www.infowatch.ru/analytics/analitika/issledovanie-utechek-informatsii-ogranichennogo-dostupa-v-2020-godu https://www.infowatch.ru/sites/default/files/analytics/files/InfoWatch_Мир_Утечки_2020_v.1.17.pdf

Список использованных источников

100. Назаров, Д. М. Основы обеспечения безопасности персональных данных в организации [Текст] : учеб. пособие / Д. М. Назаров, К. М. Саматов ; М-во науки и высш. образования Рос. Федерации, Урал. гос. экон. ун-т. — Екатеринбург : Изд-во Урал. гос. экон. ун-та, 2019. — 118 с http://aciso.ru/files/news/uchebnik.pdf

101. Good Heavens! 10M Impacted in Pray.com Data Exposure https://threatpost.com/10m-impacted-pray-com-data-exposure/161459/

102. BigBasket, the e-grocery startup which Tata Group is eyeing, admits a data breach of over 20 million users https://www.businessinsider.in/business/startups/news/bigbasket-the-e-grocery-startup-which-tata-group-is-eyeing-admits-a-data-breach-of-over-20-million-users/articleshow/79122791.cms

103. Украдена конфиденциальная информация 3,3 млн клиентов Volkswagen - 18 июня 2021 https://www.infowatch.ru/analytics/utechki-informatsii/ukradena-konfidentsialnaya-informatsiya-3-3-mln-klientov-volkswagen

104. Утекли персональные данные более 60 млн американцев - 06 августа 2021 https://www.infowatch.ru/analytics/utechki-informatsii/utekli-personalnye-dannye-bolee-60-mln-amerikantsev

105. Персональные данные миллионов индонезийцев проданы хакерами - 03 августа 2021 https://www.infowatch.ru/analytics/utechki-informatsii/personalnye-dannye-millionov-indoneziytsev-prodany-khakerami