Сравнение подходов к защите персональных медицинских данных в ЕС и Российской Федерации

Алексей Сабанов, д.т.н., доцент,
эксперт ISO/JTC1/SC27/WG5
эксперт ТК-362, ТК-122, ТК-26
профессор кафедры МГТУ им. Баумана
зам. ген. директора ЗАО "Аладдин Р.Д."

Актуальность

25 апреля 2021г. Президент В.В. Путин поручил Премьеру М.Д. Мишустину усилить работу по защите ПДн

27 апреля 2021г. М.Д. Мишустин анонсировал штрафы за незаконный сбор данных покупателей. Зачастую под разными предлогами покупателей просят предоставлять «избыточные» персональные данные, считает премьер. Правительство рассмотрит поправки в Кодекс об административных правонарушениях (КоАП), которые вводят штрафы для компаний за незаконный сбор данных клиентов.
Источник: https://www.rbc.ru/politics/27/05/2021/60af7ed59a79474a39d0f231

ВОПРОС: что лучше - платить штрафы после проверок ФСБ России на соответствие защиты ПДн приказу №378 или защитить базы в ИСПДн?

Аладдин

За рубежом

В области защиты персональных данных

Тенденции

- Число нормативных документов по защите ПДн растет
- Требования по защите ПДн становятся все строже
- Штрафы за нарушения возрастают

Стандарты

- За последние 5 лет только в ИСО разработано 7 стандартов по защите ПДн
- 8 стандартов находятся на разных стадиях разработки – цифровизация требует
- На основе международных стандартов страны разрабатывают свои стандарты

Основные отличия от наших требований

- В случае утечки оператор обязан известить надзирающий орган в течение 72 часов и довести информацию об утечке до граждан, чьи данные утекли
- Выбор средств защиты основывается на анализе рисков, выполняемых контроллером (сборщиком) ПДн, определяющим цели и методы их обработки. При передаче ПДн процессору (обработчику) за безопасность отвечает контроллер.
- Требования к сертификации продуктов отсутствуют

Судебная практика

- Штрафы реально велики, до 4% годового оборота

Аладдин

Цитаты из GDPR

Глава 2, статья 9, п.1. Запрещена обработка таких персональных данных, которые раскрывают расовую или этническую принадлежность, политические взгляды, религиозные убеждения или философские воззрения, членство в профсоюзе, также запрещена обработка генетических данных, биометрических данных для проведения уникальной идентификации физического лица, данных о здоровье, половой жизни или сексуальной ориентации физического лица.

Государства-члены ЕС могут сохранять или вводить дополнительные условия, в том числе ограничения, в отношении обработки генетических данных, биометрических данных или данных о здоровье.

Глава 4, статья 32, п.1. Принимая во внимание уровень техники, расходы и характер, объём, контекст и цели обработки, а также различные степени вероятности и тяжести рисков в отношении прав и свобод физических лиц, оператор и обработчик осуществляют соответствующие технические и организационные меры для обеспечения уровня безопасности, соответствующего рискам, включая псевдонимизацию и шифрование персональных данных.

Глава 4, статья 34, п.1. В случае, если нарушение защиты персональных данных может создать высокую степень риска для прав и свобод физических лиц, то *оператор* без необоснованной задержки уведомляет субъекта данных об утечке персональных данных. В уведомлении субъекта данных, используя ясный и простой язык, описывают характер нарушения защиты персональных данных и, как минимум, информацию и меры, предусмотренные в подпунктах b), c) и d) пункта 3 статьи 33: сообщают имя и фамилию, и контактную информацию специалиста по защите данных или указывают другой контактный пункт, где можно получить дополнительную информацию; описывают возможные последствия нарушения защиты персональных данных; описывают меры, которые контроллер принял или планирует осуществить для предотвращения нарушения защиты персональных данных...

Аладдин

Официальный отчет ISO WG5 SD2 Privacy References List

апрель 2021

Аладдин

Пример: стандарты ИСО по защите ПДн

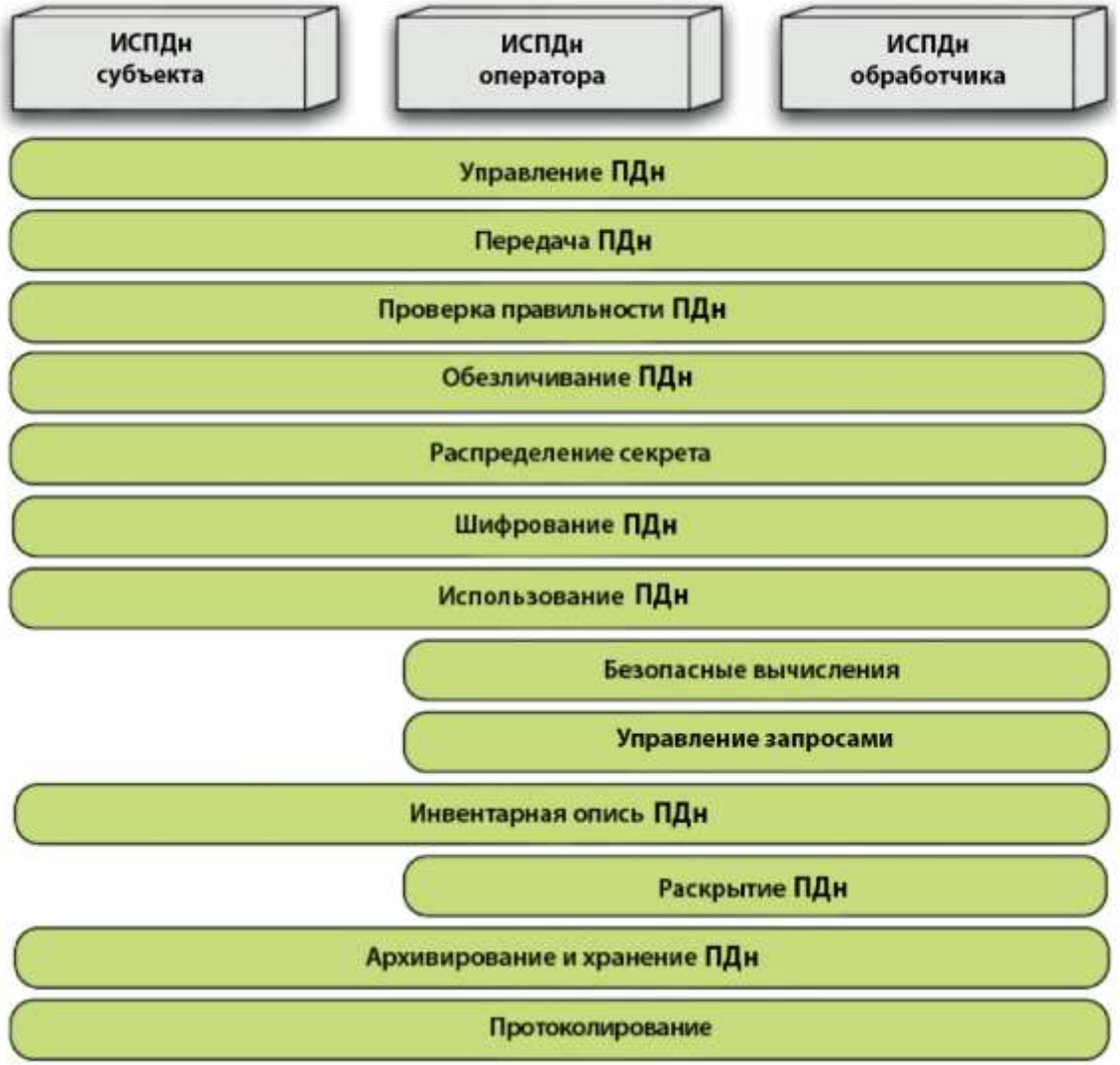
1. ISO/IEC 29100:2011 Privacy framework – Руководство по защите ПДн - **ГОСТ Р ИСО/МЭК 29100-2013 Основы обеспечения приватности**
2. ISO/IEC 29101:2018 Privacy architecture framework – Руководство по архитектуре защиты ПДн –**ГОСТ Р 59407—2021 Базовая архитектура защиты ПДн**
3. ISO/IEC 29134:2017 PIA Guiderlines – руководство по защите персональной идентифицирующей информации
4. ISO/IEC 29151 PII protection – защита идентифицирующей информации
5. ISO/IEC 29184 Online privacy notices and consent – Он-лайн уведомление о согласии [на обработку] и конфиденциальности ПДн.
6. ISO/IEC 29190:2015 Privacy capability assessment model - Модель утверждений, способная обеспечить защиту ПДн
7. ISO/IEC 29191:2012 Anonymous protection - Requirements for partially anonymous, partially unlinkable authentication
8. ISO/IEC 27017: 2015 Code of practice for information security controls based on ISO/IEC 27002 for cloud services - Правила защиты ПДн в публ.облаках
9. ISO/IEC 27550:2019 Privacy Engineering – Разработка защиты ПДн
10. ISO/IEC 27551:-в разработке Requirements for attribute-based unlinkable entity authentication
11. ISO/IEC 27552:-в разработке Extension 27001 for privacy information management -Расширение стандарта 27001 на управление персональной информацией
12. ISO/IEC 27570:-в разработке Privacy for smart cities
13. ISO/IEC 27559: в разработке Privacy enhancing update de-identification framework
14. ISO/IEC 29556:-в разработке User-centric framework for PII handling based on privacy preferences
15. ISO/IEC 27018 Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
16. ISO/IEC 20889 Privacy enhancing data deidentification terminology and classification of techniques
17. ISO/IEC 20547-4 Big data sensitivity and privacy – Чувствительность и приватность больших данных (Big data)
18. ISO/IEC 20889:2018 Privacy enhancing data deidentification terminology and classification of techniques
19. ISO/IEC 20649: -в разработке Privacy enhancing data de-identification framework
20. ISO/IEC 22307:2008 Privacy impact assessment – Оценка атак на приватность

ГОСТ Р 59407—2021 Базовая архитектура защиты ПДн
Архитектура ИСПДн оператора

Аладдин

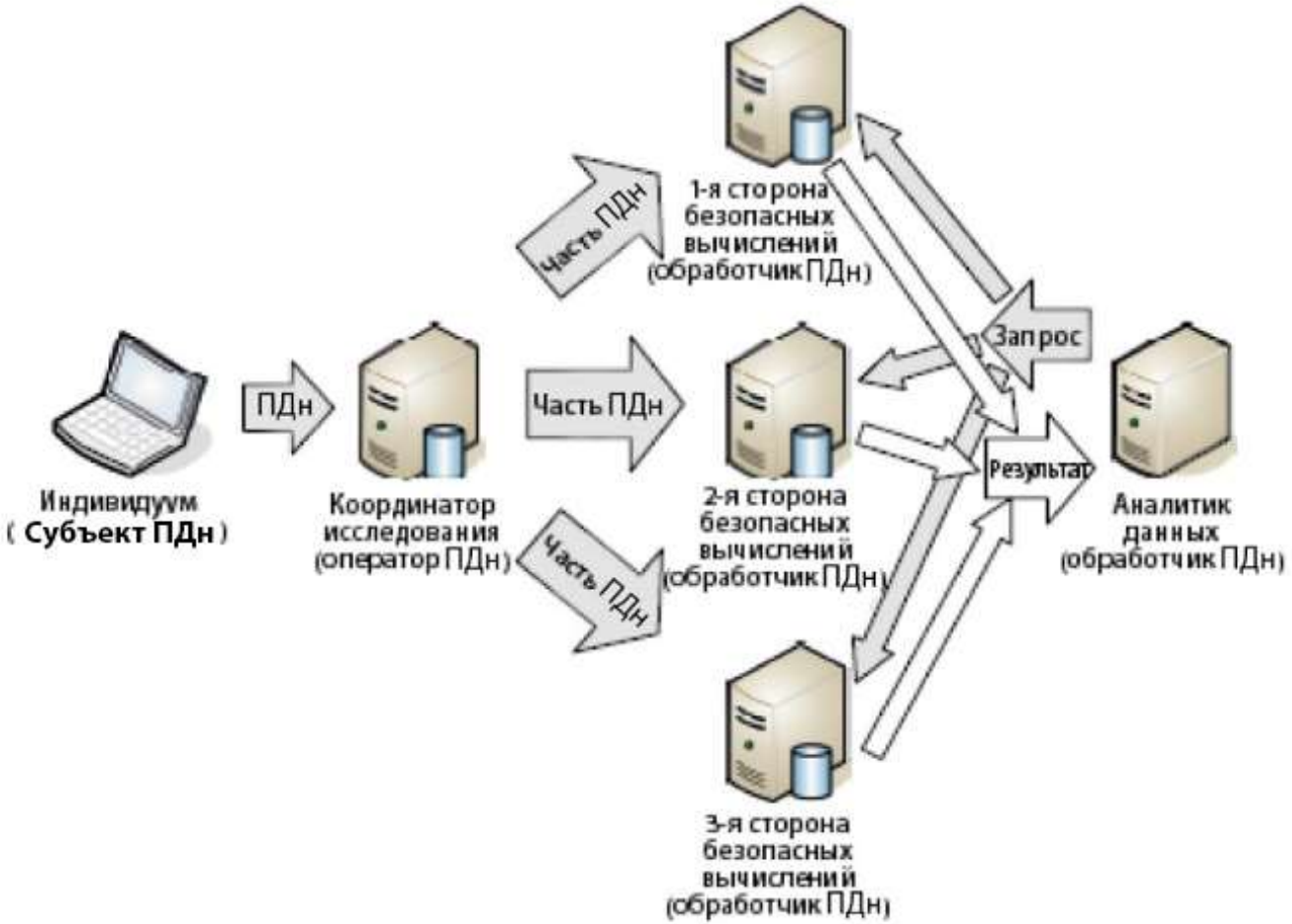
ГОСТ Р 59407—2021 Базовая архитектура защиты ПДн

Распределение компонентов защиты ПДн



Аладдин

ГОСТ Р 59407—2021 Базовая архитектура защиты ПДн
Реализация системы безопасных вычислений



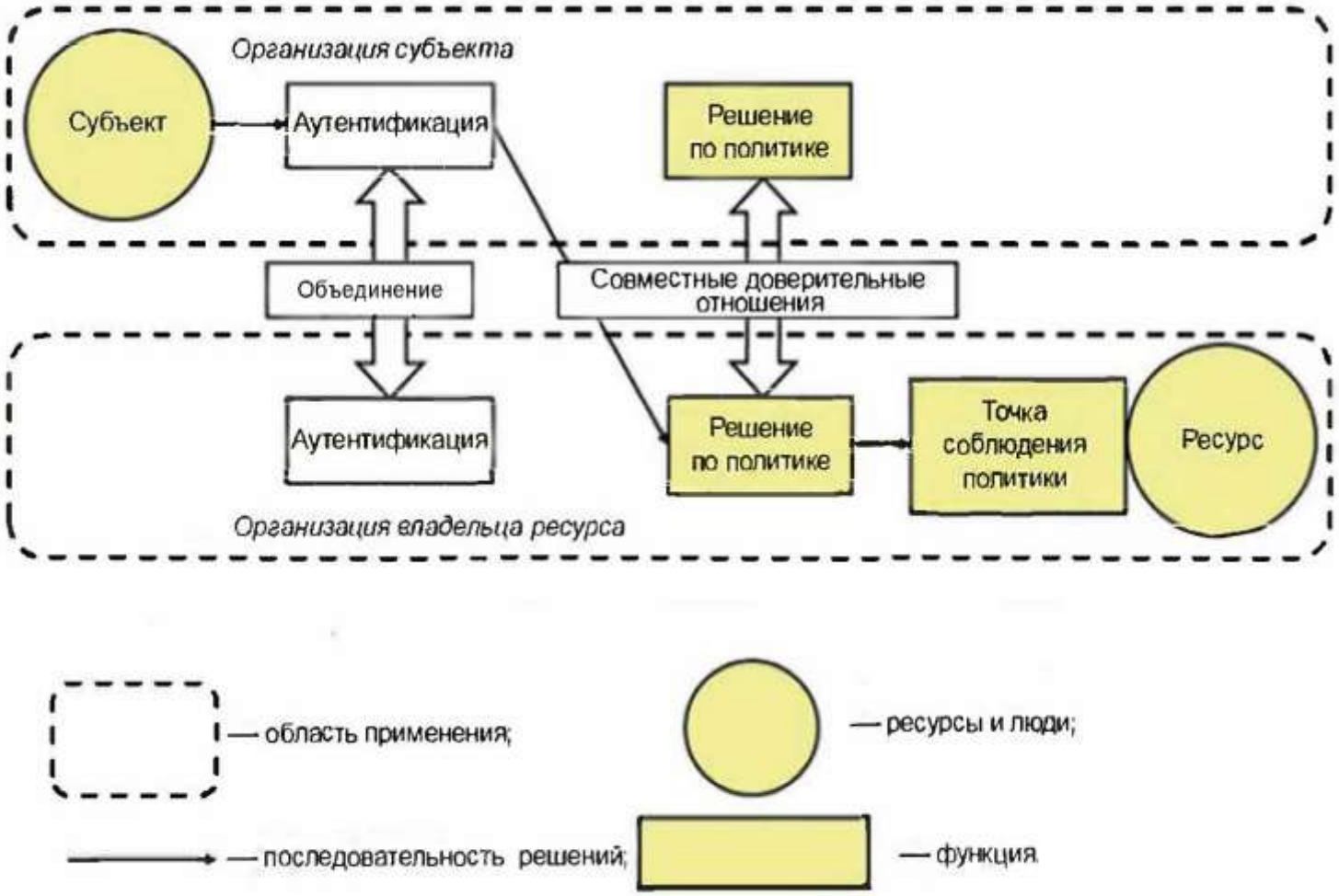
Аладдин

ГОСТ Р 59383-2021 Информационные технологии. Методы и средства обеспечения безопасности. Основы управления доступом

Последовательность действий

Взаимосвязь системы управления идентификационными данными и авторизацией

ГОСТ Р 59383-2021 Информационные технологии. Методы и средства обеспечения безопасности. Основы управления доступом



Управление федеративным доступом

Аладдин

Проект ГОСТ Р ХХХ Информационные технологии. Методы и средства обеспечения безопасности. Уровни доверия аутентификации

№	Что используется при аутентификации	Аутентификационная информация	Защита аутентификационной информации	Обмен	Факторы аутентификации	Вид аутентификации	Уровень доверия к результату аутентификации
1	запоминаемый секрет (примеры: пароль, PIN-код)	пароль	защита пароля от известных атак	односторонний	знание	простая	низкий
2	сгенерированный заранее одноразовый пароль, записанный на носителе (пример: скрэтч-карта)	одноразовый пароль	доверенный ДСЧ, защита канала распределения OTP, защита от MitM-атак	односторонний	владение		
3	"второй канал" (пример: телефон+SMS)	одноразовый пароль	защита операций аутентификации в обоих каналах	односторонний	владение		средний
4	устройство одноразовых паролей, динамически генерирующая OTP	одноразовый пароль	защита устройства	односторонний	владение		
5	многоразовый пароль + устройство OTP	одноразовый пароль + многоразовый пароль	защита многоразового пароля	односторонний	владение + знание	усиленная	высокий
6	многоразовый пароль + устройство OTP с доступом к устройству по паролю или биометрии	одноразовый пароль + многоразовый пароль	защита устройства и многоразового пароля	односторонний	владение + знание или биометрия		
7	криптографическй ключ в СВТ или на незащенном паролем носителе	криптографические ключи	защита ключей	односторонний или взаимный	владение		
8	устройство (СВТ или смартфон) с криптографическим ПО + доступ к ключу по паролю	криптографические ключи	защита устройства	односторонний или взаимный	владение + знание		
9	СВТ с криптографическим ПО + доступ к ключу по паролю	криптографические ключи	защита ключей	взаимный	владение + знание	строгая	очень высокий
10	СВТ с криптографическим ПО и отдельное устройство с помещённым и хранящемся в нём криптографическим ключом + доступ к ключу по паролю или биометрии	криптографические ключи	защита устройства, содержащего ключ	взаимный	владение + знание или биометрия		
11	СВТ с криптографическим ПО и отдельное устройство с криптографическим ПО, генерирующее неизвлекаемые ключи (SSCD) + доступ к ключу по паролю и/или биометрии	криптографические ключи	защита устройства, содержащего ключ	взаимный	владение + знание и/или биометрия		высший

Аладдин

Выводы

1. Терминология (роли), концепция и принципы защиты, законодательство и штрафы за нарушение безопасности персональных данных граждан за рубежом существенно отличаются от российских.

2. При построении цифрового государства в условиях роста киберпреступности роль защиты приватности граждан (их цифровых профилей) возрастает.

3. Мировой опыт демонстрирует усиление требований к защите персональных данных, ИТ-администраторам и специалистам по защите информации следует обратить на это особое внимание.

4. На рынке уже имеются решения, удовлетворяющие как международным, так и российским требованиям. Примером является СКЗИ «Крипто БД» производства «Аладдин Р.Д.», входящее в реестр отечественного ПО и сертифицированное по требованиям ФСБ России до класса КС3.

Аладдин

Спасибо за внимание!

Вопросы

a.sabanov@aladdin.ru
8-985-924-52-09

Аладдин