Privacy Advocates

Правовые и практические аспекты надлежащего уничтожения персональных данных

ООО «Лекс Инжиниринг»

+7 (903) 762-64-15 | corp@privacy-advocates.ru | t.me/prv_adv

Privacy Advocates

Алексей Мунтян

Основатель и CEO в компании Privacy Advocates

+7 (903) 762-64-15

alexey.muntyan@privacy-advocates.ru

- 16 лет опыта в защите персональных данных
- Внешний Data Protection Officer в нескольких транснациональных холдингах
- Соучредитель в Regional Privacy Professionals Association - RPPA.pro
- Со-председатель Privacy & Legal Innovation кластера РАЭК

Privacy Advocates

Уничтожение/Удаление

Блокирование

Архивирование

Обезличивание

Способ защиты ПД, а не прекращения обработки

Уничтожение, удаление и блокирование

УНИЧТОЖЕНИЕ ПД

Действия, в результате которых становится невозможным восстановить содержание ПД в ЭВМ и (или) в результате которых уничтожаются материальные носители ПД

п.8 ст.3 152-ФЗ

УДАЛЕНИЕ ПД

Изъятие ПД из ЭВМ с сохранением последующей возможности их восстановления

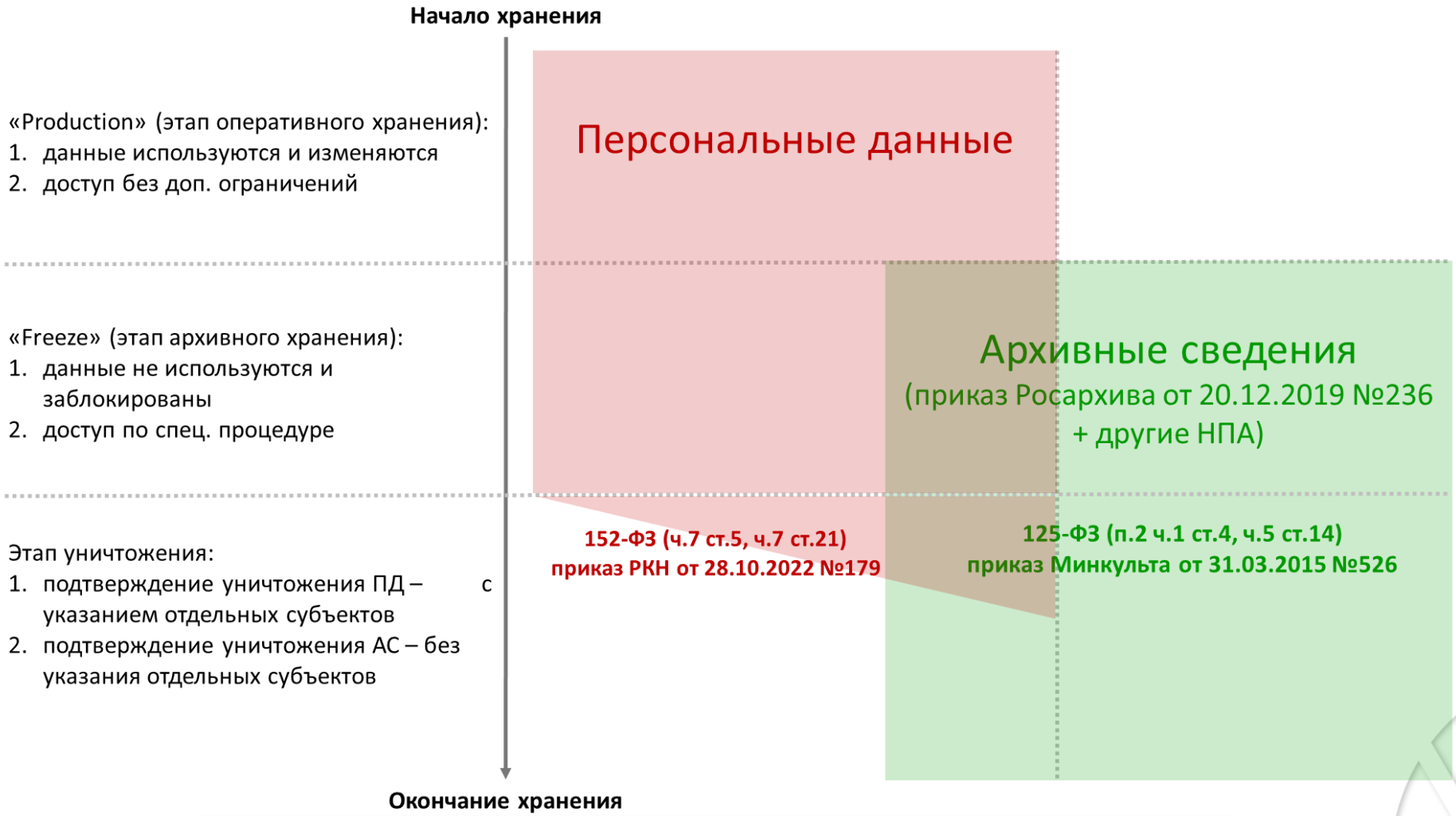
Информационное письмо АРБ от 02.12.2011 №5

БЛОКИРОВАНИЕ ПД

Временное прекращение обработки ПД (за исключением случаев, если обработка необходима для уточнения ПД)

п.7 ст.3 152-ФЗ

Прекращение обработки ПД путем архивирования



☑ **Преимущества режима архива по 125-ФЗ:**

- **длительные сроки хранения документов;**
- **уничтожение документов без указания сведений о субъектах ПД;**
- **отсутствие явной обязанности уведомлять об инцидентах с ПД для документов.**

Риски обезличивания ПД

1. 152-ФЗ «О персональных данных», п.9 ст.3: обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных…

2. Постановление Правительства РФ от 21.03.2012 № 211, пп.«з» п.1: в случаях, установленных нормативными правовыми актами РФ, в соответствии с требованиями и методами, установленными Роскомнадзором, осуществляют обезличивание персональных данных, обрабатываемых в информационных системах персональных данных...

3. Приказ Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных»

4. Методические рекомендации по применению приказа Роскомнадзора от 05.09.2013 № 996 "Об утверждении требований и методов по обезличиванию персональных данных" (утв. Роскомнадзором от 13.12.2013)

Данные нормативные правовые акты предназначены для операторов, являющихся государственными или муниципальными органами.

Является ли обезличивание ПД способом прекращения их обработки?

По мнению Минцифры и Роскомнадзора не является. Обезличивание – это один из способов защиты ПД.

Причина такой позиции: свойство обратимости обезличивания – возможности приведения ПД к исходному виду, позволяющему определить их принадлежность конкретному субъекту.

Обезличивание ПД возможно при одновременном выполнении 2 условий:

1. Наличие согласия человека на обезличивание его ПД или наличие иного правового основания, предусмотренного ч.1 ст.6 152-ФЗ о ПД;

2. Применение методов обезличивания ПД из закрытого перечня, установленного приказом РКН №996:

- **Введение идентификаторов;**
- **Изменение состава или семантики;**
- **Декомпозицию;**
- **Перемешивание.**

Ограничение периода хранения ПД

Privacy Advocates

ПД должны храниться не дольше, чем этого требуют цели, для которых они накапливались, и подлежат уничтожению по достижении целей или отпадению надобности в них

- Достижение целей обработки ПД и (или) истечение максимальных сроков хранения ПД
- Утрата необходимости в достижении целей обработки ПД
- Предоставление субъектом ПД сведений о том, что ПД являются незаконно полученными или не являются необходимыми для цели обработки
- Невозможность обеспечения правомерности обработки ПД
- Отзыв субъектом ПД согласия на обработку ПД, если сохранение ПД более не требуется для целей обработки ПД
- Истечение сроков исковой давности для правоотношений, в рамках которых осуществляется либо осуществлялась обработка ПД
- Ликвидация или некоторые формы реорганизации оператора

Сроки хранения ПД

Сроки хранения ПД

- 7 рабочих дней - при представлении субъектом ПД сведений, что ПД данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки ПД [152-ФЗ ст.20 ч.3]
- 10 рабочих дней - при выявлении неправомерной обработки ПД, если невозможно обеспечить ее правомерность [152-ФЗ ст.21 ч.3]
- 10+5 рабочих дней - при обращении субъекта с требованием о прекращении обработки ПД [152-ФЗ ст.21 ч.5.1]
- 30 дней - после достижения цели обработки ПД или после утраты необходимости в достижении такой цели [152-ФЗ ст.21 ч.4]
- 30 дней - при отзыве субъектом ПД согласия на обработку его ПД, если их сохранение более не требуется для целей обработки ПД [152-ФЗ ст.21 ч.5]
- 6 месяцев - хранение ПД в блокированном виде, если у оператора отсутствует возможность своевременного уничтожения ПД [152-ФЗ ст.21 ч.6]
- 3 года - общий срок исковой давности с момента прекращения действия договора, стороной которого либо выгодоприобретателем является субъект ПДн [ГК РФ ст. 196]
- 5 лет - после отчетного года создания первичных учетных документов [402-ФЗ «О бухгалтерском учете» ст.29] и обеспечения сохранности документов, необходимых для исчисления, уплаты или удержания, перечисления налогов [НК РФ ст.23, ст.24]
- **более 5 лет, при условии прохождения теста «Почему именно такие сроки?»**

! Перечень типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения (утв. Росархивом от 20.12.2019 № 236).

Трудности уничтожения ПД

ГРАФИК УНИЧТОЖЕНИЯ

- Фактический срок
- Желаемый срок
- Законный срок
- Установленный срок
- Триггеры/периоды

БАЗЫ ДАННЫХ

- Основные/резервные
- Разработки
- Тестирования
- Логирования

Приказ Роскомнадзора от 28.10.2022 №179

Подтверждение факта уничтожения ПД [1/3]

Акт об уничтожении ПД

- наименование или ФИО и адрес оператора ПД
- наименование или ФИО и адрес обработчика ПД (при поручении обработки ПД)
- ФИО или иные идентификаторы субъектов, ПД которых уничтожены
- ФИО, должность и подпись (собственноручная или электронная) лиц (лица), уничтоживших ПД
- перечень категорий уничтоженных ПД
- наименование и количество листов каждого уничтоженного материального носителя ПД (при неавтоматизированной обработке ПД)
- наименование ИСПД, в которых уничтожены ПД (при автоматизированной обработке ПД)
- способ уничтожения ПД
- причина уничтожения ПД
- дата уничтожения ПД
- **составляется при уничтожении ПД как на материальных носителях, так и в ИСПД**
- **хранится 3 года с момента уничтожения ПД**

Подтверждение факта уничтожения ПД [2/3]

Выгрузка из журнала регистрации событий в ИСПД

- ФИО или иные идентификаторы субъектов, ПД которых уничтожены
- перечень категорий уничтоженных ПД
- наименование ИСПД, в которой уничтожены ПД
- причина уничтожения ПД
- дата уничтожения ПД
- **выгружается при уничтожении ПД в ИСПД**
- **при отсутствии в выгрузке необходимых сведений, они вносятся в акт об уничтожении**
- **хранится 3 года с момента уничтожения ПД**

Подтверждение факта уничтожения ПД [3/3]

Комментарии РКН
t.me/prv_adv/1555

- выгрузка из журнала регистрации событий в ИСПД является подтверждением уничтожения ПД, обрабатываемых с использованием средств автоматизации, и не подменяет собой необходимость составления акта об уничтожении ПД
- сведения, которые технически не могут быть реализованы в выгрузке из журнала регистрации событий в ИСПД, могут быть отражены в акте об уничтожении ПД
- указание ФИО субъектов ПД в акте об уничтожении ПД является обязательным при наличии у оператора таких ФИО
- указание в акте об уничтожении ПД «иной информации, относящейся к определенному(ым) физическому(им) лицу(ам), чьи ПД были уничтожены» (конкретные идентификаторы (атрибуты), относящиеся к конкретному физическому лицу) отнесено к тем случаям, когда у оператора отсутствует ФИО субъекта ПД
- действие приказа РКН не распространяется на отношения, возникающие при организации хранения, комплектования, учета и использования содержащих ПД документов Архивного фонда РФ и других архивных документов в соответствии с законодательством об архивном деле в РФ

Составление акта об уничтожении ПД

Privacy Advocates

Акт об уничтожении (прекращении обработки) ПД[1]

[*Место составления акта*] «__» _____ 20__ года

Комиссия в составе:

(1) [*Фамилия Имя Отчество*], [*Наименование должности*] – председатель комиссии;
(2) [*Фамилия Имя Отчество*], [*Наименование должности*] – член комиссии;
(3) [*Фамилия Имя Отчество*], [*Наименование должности*] – член комиссии;

провела отбор (сортировку) подлежащих уничтожению (прекращению обработки) персональных данных и установила, что в соответствии с достижением целей обработки персональных данных или утратой необходимости в достижении этих целей персональные данные, содержащиеся на следующих материальных носителях, подлежит уничтожению:

№	Наименование носителя[2]	Тип носителя[3]	Регистрационный № носителя[4]	ФИО субъекта ПД	Перечень уничтоженных категорий ПД	ИСПД, откуда были уничтожены ПД	Способ уничтожения ПД[5]	Причина уничтожения ПД
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*

После утверждения акта, перечисленные носители сверены с записями в акте и уничтожены или возвращены для дальнейшего (повторного) использования. Уничтоженные носители с журналов учета (при наличии таковых) списаны.

Председатель комиссии: _____/_____/
подпись *расшифровка подписи*

Члены комиссии: _____/_____/
подпись *расшифровка подписи*

_____/_____/
подпись *расшифровка подписи*

[1] Срок хранения – 3 года (в соответствии с Приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28.10.2022 № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных»)
[2] Например, «ИСПД "_____"», «Корпоративный ноутбук», «Служебная карта памяти» или «Договор об оказании услуг от __.__.____ № _____».
[3] Информационная система, автоматизированное рабочее место, отчуждаемый машинный носитель (HDD, USB Flash Card и т.д.), бумажный носитель и др. с указанием количества.
[4] При наличии.
[5] Общие способы уничтожения ПД при условии дальнейшего (повторного) использования: вымарывание ПД на бумажных носителях, необратимое удаление ПД в информационных системах, на автоматизированных рабочих местах или на машинных носителях информации с помощью программных и (или) аппаратных средств. Общие способы уничтожения ПД без дальнейшего (повторного) использования: разрезание, сжигание, механическое уничтожение, сдача предприятию по утилизации вторичного сырья и т.д.

Акт об уничтожении материальных носителей с персональными данными

Город Москва __ _____ 202_ года

Комиссия ООО «_____» в составе следующих лиц:

(1) _____, ассистент – председатель комиссии;
(2) _____, менеджер проекта – член комиссии;
(3) _____, бизнес ассистент – член комиссии,

провела отбор (сортировку) подлежащих уничтожению материальных носителей с персональными данными и установила, что, в связи с утратой необходимости в дальнейшем хранении отобранных носителей, следующие материальные носители подлежит уничтожению:

№	Наименование носителя(ей)	Тип носителя(ей)	Способ уничтожения персональных данных
1	Письменные согласия субъектов на обработку персональных данных по списку, приведённому в электронном файле, который: • адресуется как «Список согласий ПД на утилизацию.xlsx» • имеет размер в 273452 байт • идентифицируется по хеш-сумме (алгоритм MD5) 703809f03cb56d78d3a0f3468b33b70b • идентифицируется по хеш-сумме (алгоритм SHA-1) 468366672fb3e0e539a07436c644930372668763 • зафиксирован на компакт-диске, который хранится вместе с настоящим Актом	Бумажный носитель	Измельчение в шредере

После утверждения акта, перечисленные носители сверены с записями в акте и уничтожены. Уничтоженные носители с журналов учета (при наличии таковых) списаны.

Председатель комиссии: _____/_____/
подпись *расшифровка подписи*

Члены комиссии: _____/_____/
подпись *расшифровка подписи*

_____/_____/
подпись *расшифровка подписи*

[Криптографические хэш-функции для контроля целостности и неизменности документа]

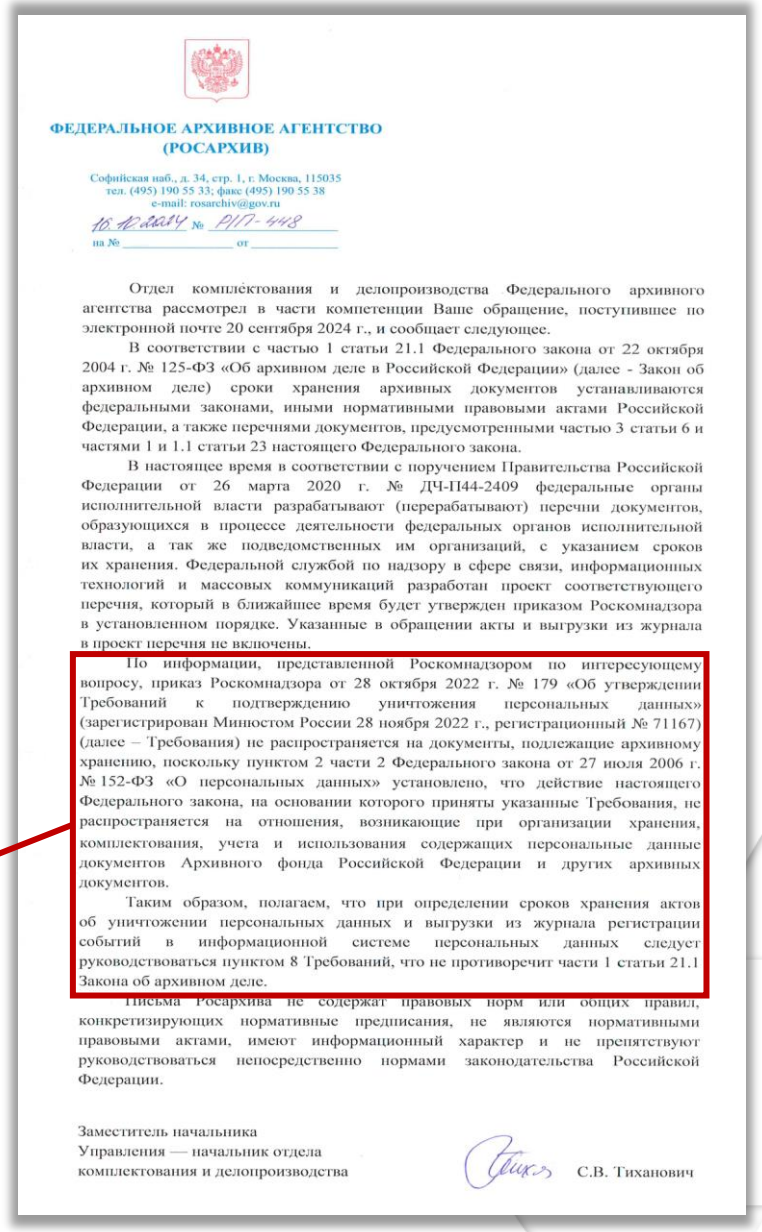
Хранение акта об уничтожении ПД

💡 **Вопрос:** В соответствии с п.8 приказа Роскомнадзора №179 от 28.10.2022 акт об уничтожении ПД и выгрузка из журнала регистрации событий в ИСПД подлежат хранению в течение 3 лет с момента уничтожения ПД. Перечень ТУАД (утв. приказом Росархива №236 от 20.12.2019) не упоминает таких документов.

◇ Следует ли рассматривать установленный приказом Роскомнадзора №179 срок в 3 года как срок архивного хранения?

◇ Если указанный срок в 3 года не является сроком архивного хранения, то в течение какого срока следует хранить вышеупомянутые документы по истечении указанных 3 лет?

🏛 **Росархив:** Приказ Роскомнадзора №179 не распространяется на документы, подлежащие архивному хранению (см. п.2 ч.2 152-ФЗ от 27.07.2006 «О персональных данных»). При определении сроков хранения актов об уничтожении ПД и выгрузки из журнала регистрации событий в ИСПД следует руководствоваться п.8 приказа Роскомнадзора №179, что не противоречит ч.1 ст.21.1 125-ФЗ об архивном деле.



ФЕДЕРАЛЬНОЕ АРХИВНОЕ АГЕНТСТВО
(РОСАРХИВ)

Софийская наб., д. 34, стр. 1, г. Москва, 115035
тел. (495) 190 55 33; факс (495) 190 55 38
e-mail: rosarchiv@gov.ru

16.10.2024 № РП-448
на № _____ от _____

Отдел комплектования и делопроизводства Федерального архивного агентства рассмотрел в части компетенции Ваше обращение, поступившее по электронной почте 20 сентября 2024 г., и сообщает следующее.

В соответствии с частью 1 статьи 21.1 Федерального закона от 22 октября 2004 г. № 125-ФЗ «Об архивном деле в Российской Федерации» (далее - Закон об архивном деле) сроки хранения архивных документов устанавливаются федеральными законами, иными нормативными правовыми актами Российской Федерации, а также перечнями документов, предусмотренными частью 3 статьи 6 и частями 1 и 1.1 статьи 23 настоящего Федерального закона.

В настоящее время в соответствии с поручением Правительства Российской Федерации от 26 марта 2020 г. № ДЧ-П44-2409 федеральные органы исполнительной власти разрабатывают (перерабатывают) перечни документов, образующихся в процессе деятельности федеральных органов исполнительной власти, а так же подведомственных им организаций, с указанием сроков их хранения. Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций разработан проект соответствующего перечня, который в ближайшее время будет утвержден приказом Роскомнадзора в установленном порядке. Указанные в обращении акты и выгрузки из журнала в проект перечня не включены.

По информации, представленной Роскомнадзором по интересующему вопросу, приказ Роскомнадзора от 28 октября 2022 г. № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных» (зарегистрирован Минюстом России 28 ноября 2022 г., регистрационный № 71167) (далее – Требования) не распространяется на документы, подлежащие архивному хранению, поскольку пунктом 2 части 2 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» установлено, что действие настоящего Федерального закона, на основании которого приняты указанные Требования, не распространяется на отношения, возникающие при организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других архивных документов.

Таким образом, полагаем, что при определении сроков хранения актов об уничтожении персональных данных и выгрузки из журнала регистрации событий в информационной системе персональных данных следует руководствоваться пунктом 8 Требований, что не противоречит части 1 статьи 21.1 Закона об архивном деле.

Письма Росархива не содержат правовых норм или общих правил, конкретизирующих нормативные предписания, не являются нормативными правовыми актами, имеют информационный характер и не препятствуют руководствоваться непосредственно нормами законодательства Российской Федерации.

Заместитель начальника
Управления — начальник отдела
комплектования и делопроизводства С.В. Тиханович

Способы уничтожения ПД

Оператор определяет способы уничтожения ПД и фиксирует порядок уничтожения ПД в локальном акте

- удаление или вымарывание данных на бумажном носителе
- разрезание бумажного носителя
- сжигание бумажного носителя
- измельчение бумажного носителя
- механическое уничтожение машинного носителя
- стирание данных на машинном носителе с помощью штатного ПО
- стирание данных на машинном носителе с помощью специализированного ПО или устройств
- нарушение функциональных возможностей машинного носителя
- сдача носителей предприятию по утилизации вторсырья

!

- **ГОСТ Р 54471-2011/ISO/TR 15801:2009 – пункт 6.11**
- **Руководящий документ от 30.03.1992 «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»**

Уничтожение ПД с помощью СЗИ [1/2]

Часть 2 статьи 19 152-ФЗ была дополнена (*233-ФЗ от 08.08.2024*) пунктом 3.1 о применении для уничтожения ПД прошедших в установленном порядке процедуру оценки соответствия средств защиты информации (СЗИ), в составе которых реализована функция уничтожения информации.

Требование об использовании СЗИ для уничтожения ПД:

1. не распространяется на обработку ПД, осуществляемую без использования средств автоматизации;
2. определено как мера по обеспечению безопасности ПД при их обработке (ст.19 152-ФЗ), а не как мера, направленная на обеспечение выполнения оператором предусмотренных 152-ФЗ обязанностей (ст.18.1 152-ФЗ), или как обязанность оператора по обеспечению надлежащего уничтожения ПД (ст.21 152-ФЗ);
3. не отнесено Минцифрой и Роскомнадзором к собственной компетенции [*см. следующий слайд*].

👉 Пункт 33 проверочного листа, применяемого РКН при осуществлении федерального государственного контроля (надзора) за обработкой ПД (утв. приказом РКН от 24.12.2021 №253), предусмотрена проверка РКН только факта выполнения оператором организационных мер для защиты ПД от неправомерных действий – в рамках требования ч.1 ст.19 152-ФЗ, т.е. РКН в принципе не проверяет выполнение оператором технических мер защиты ПД в рамках ч.2 ст.19 152-ФЗ.

Уничтожение ПД с помощью СЗИ [2/2]

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ (МИНЦИФРЫ РОССИИ)

Пресненская наб., д.10, стр.2, Москва, 123112
Справочная: +7 (495) 771-8000

10.09.2024 № П25-21859-ОГ

На № _____ от _____

О перенаправлении обращения

Департамент обеспечения кибербезопасности Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации (далее – Министерство) в соответствии с частью 3 статьи 8 Федерального закона от 2 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» направляет по принадлежности обращения Мунтяна А., зарегистрированные в Министерстве 5 сентября 2024 г., для рассмотрения и ответа заявителю в установленном порядке.

Заявителю направляется в порядке информирования.

Приложение: на 2 л. только в первые два адреса.

Врио директора Департамента обеспечения кибербезопасности

Минцифры России — Документ подписан электронной подписью
СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП
Сертификат: 0186564D4B11A0DF4905CF1354CCAFC9
Владелец: Хасин Евгений Владимирович
Действителен с 12-07-2024 до 05-10-2025

Е.В. Хасин

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Китайгородский проезд, д. 7, стр. 2, Москва, 109992
тел.: (495) 198-65-01; факс: (495) 587-44-68; https://rkn.gov.ru/

12.09.2024 № 08-377683

На

О рассмотрении обращения

Управление по защите прав субъектов персональных данных Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций рассмотрело Ваше обращение от 05.09.2024 № б/н (вх. № 02-11-35507 от 05.09.2024) и сообщает следующее.

Пункт 3.1 части 2 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ) устанавливает, что обеспечение безопасности персональных данных достигается, в том числе посредством применения средств защиты информации, прошедших процедуру оценки соответствия, в составе которых реализована функция уничтожения информации.

Учитывая то, что в соответствии с частью 8 Федерального закона № 152-ФЗ, контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных статьей 19 Федерального закона № 152-ФЗ, осуществляются ФСБ России и ФСТЭК России в пределах установленных полномочий, полагаем, что вопрос, поставленный в Вашем обращении, относится к компетенции указанных федеральных органов исполнительной власти.

Начальник Управления по защите прав субъектов персональных данных

Ю.Е. Контемиров

Документ подписан электронной подписью в системе электронного документооборота Роскомнадзора
СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП
Сертификат: 452dc4e4c7c064f216509d25c30b625c
Владелец: Контемиров Юрий Евгеньевич
Действителен: с 08.05.2024 по 01.08.2025

Когда нужно применять СЗИ для уничтожения ПД [1/2]

◇ Согласно п.4 ПП-1119 от 01.11.2012 выбор СЗИ для системы защиты ПД осуществляется оператором в соответствии с нормативными правовыми актами, принятыми ФСБ и ФСТЭК во исполнение ч.4 ст.19 152-ФЗ. В пп.«г» п.13 ПП-1119 и п.4 приказа ФСТЭК от 18.02.2013 №21 предусмотрено, что для обеспечения всех уровней защищенности ПД при их обработке в ИСПД применяются СЗИ, прошедшие в установленном порядке процедуру оценки соответствия, в случаях, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности ПД [*см. следующий слайд – ответ ФСТЭК*].

◇ Разделом 4 Приложения к приказу ФСТЭК №21 предусмотрена только одна мера по обеспечению безопасности ПД путем их уничтожения – ЗНИ.8 «Уничтожение (стирание) или обезличивание ПД на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания». Машинные носители информации определены в п.8.4 приказа ФСТЭК №21 как средства обработки (хранения) ПД и съемные машинные носители ПД.

◇ Важным вопросом является выбор формы оценки соответствия СЗИ. В ч.3 ст.7 184-ФЗ «О техническом регулировании» указано, что оценка соответствия проводится в формах государственного контроля (надзора), испытания, регистрации, подтверждения соответствия, приемки и ввода в эксплуатацию объекта, строительство которого закончено, и в иной форме. Следует отметить, что для уничтожения ПД:

(1) ФСТЭК допускает применение СЗИ, прошедших процедуру оценки соответствия в предусмотренных положениями 184-ФЗ формах оценки соответствия [*см. следующий слайд – ответ ФСТЭК*];

(2) ФСБ считает допустимым применение исключительно СЗИ, сертифицированных по требованиям ФСТЭК и ФСБ [*см. следующий слайд – ответ ФСБ (8 Центр)*].

Когда нужно применять СЗИ для уничтожения ПД [2/2]

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ
КОНТРОЛЮ
(ФСТЭК России)

Старая Басманная, д. 17, Москва, 105066
Тел., факс: (495) 696-49-04
E-mail: postin@fstec.ru

4.10. 2024 № 240/24/4719

На №_____

О направлении информации

Уважаемый !

По существу вопросов, содержащихся в Вашем обращении, сообщаем следующее.

В соответствии с подпунктом 3.1 пункта 3 статьи 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» обеспечение безопасности персональных данных достигается в том числе путем применения для уничтожения персональных данных прошедших в установленном порядке процедуру оценки соответствия средств защиты информации, реализующих функцию уничтожения информации. Формы оценки соответствия средств защиты информации предусмотрены Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

В соответствии с Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденными приказом ФСТЭК России от 18 февраля 2013 г. № 21, мера защиты информации ЗНИ.8 «Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания» может быть реализована только с применением средств защиты информации, реализующих функцию уничтожения (стирания) информации и прошедших в установленном порядке процедуру оценки соответствия в любой из форм.

Таким образом, применение средств защиты информации, реализующих функцию уничтожения (стирания) информации и прошедших в установленном порядке процедуру оценки соответствия в любой из форм, предусмотренных Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании», для реализации меры защиты информации ЗНИ.8 «Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания» является обязательным.

Дополнительно сообщаем, что требование о необходимости использования в информационной системе персональных данных средств защиты информации, в том числе реализующих функцию уничтожения (стирания) информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз, установлено Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119, и Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденными приказом ФСТЭК России от 18 февраля 2013 г. № 21.

С уважением,

Начальник 2 управления Д.Щевцов

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
(ФСБ России)

8 Центр

05.10. 2024 г. № 149/7/2/6-1076

5.10

Москва

Ваши обращения по вопросу разъяснения положений подпункта 3.1 части 2 статьи 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – Закон) рассмотрены.

По результатам рассмотрения сообщаем, что в соответствии с подпунктом 3.1 части 2 статьи 19 Закона обеспечение безопасности персональных данных достигается применением для уничтожения персональных данных прошедших в установленном порядке процедуру оценки соответствия средств защиты информации, в составе которых реализована функция уничтожения информации.

К таким средствам относятся средства защиты информации, сертифицированные по требованиям, предъявляемым ФСТЭК России и ФСБ России к таким средствам, которые могут быть реализованы в программном, программно-аппаратном или аппаратном виде. С перечнем указанных средств возможно ознакомиться на официальных сайтах ФСТЭК России и ФСБ России.

В случае, если оператора персональных данных не удовлетворяют имеющиеся средства защиты информации с действующим сертификатом соответствия, то такой оператор может поставить работы в специализированных организациях, имеющих соответствующие лицензии, на разработку новых средств.

Одновременно отмечаем, что использование операторами персональных данных иных средств для уничтожения персональных данных не допускается.

Первый заместитель
начальника Центра В.А. Шуринов

СЗИ, в составе которых реализована функция уничтожения информации, из Государственного реестра сертифицированных СЗИ:

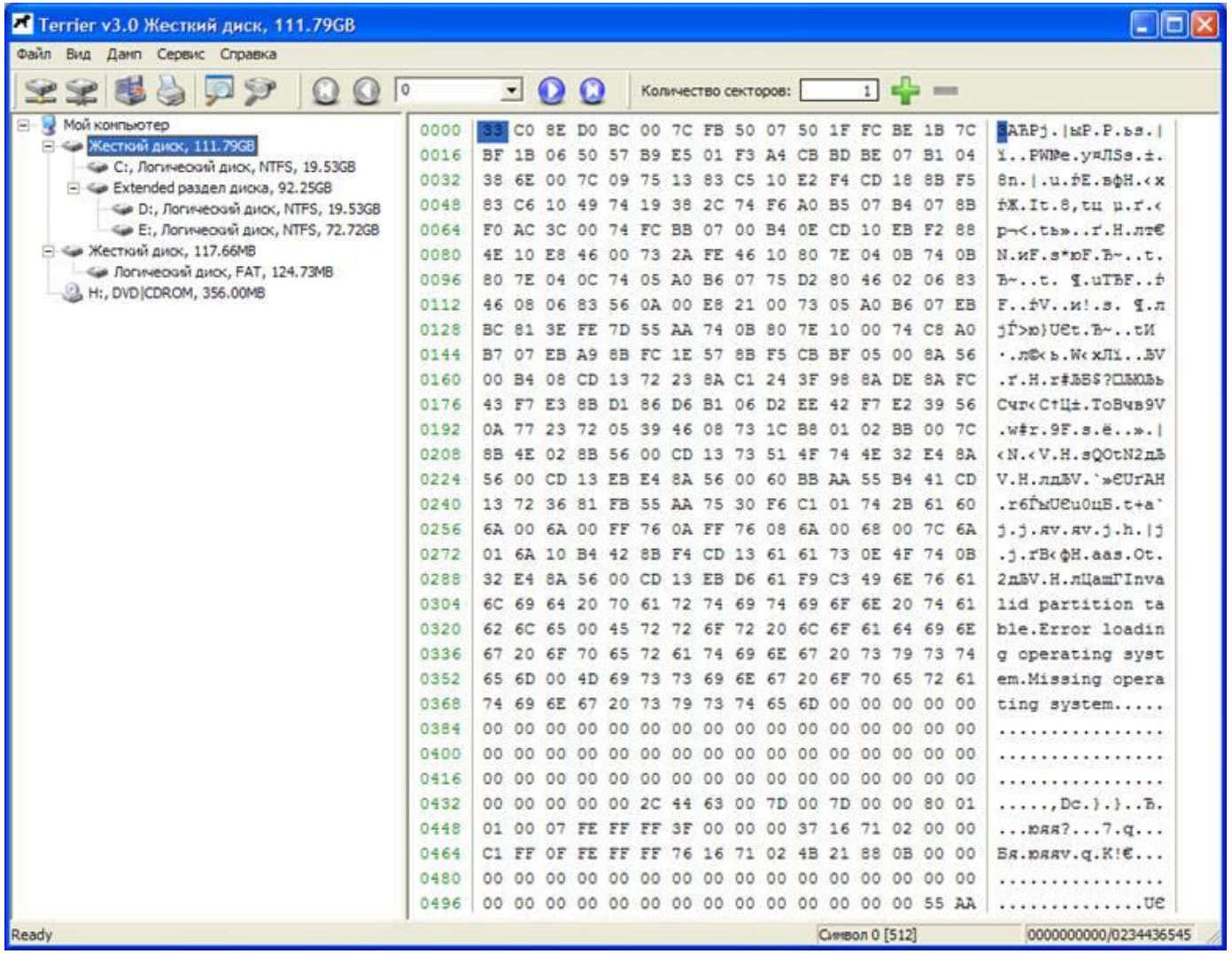
- ПО «Secret Net Studio» (ООО «Код Безопасности»);
- ПО «TERRIER версия 3.0» (АО «ЦБИ-сервис»);
- ПАК «Прибой Модуль-3.5» (ООО «Компьютерные сервисные устройства»);
- ПАК «Стек-НСЗ» (ООО «Анна»).

Privacy Advocates

Возможности Secret Net Studio

Функция уничтожения данных на носителях информации предназначена для безвозвратного затирания всей информации (включая таблицу разделов, логические тома, файловые объекты и остаточную информацию) на следующих носителях информации:

- локальные диски защищаемого компьютера (кроме системного диска);
- сменные носители информации, подключенные к защищаемому компьютеру.



Программа поиска и гарантированного уничтожения информации на дисках, являющаяся программным средством защиты и контроля эффективности применения средств защиты информации, сертифицированным ФСТЭК России.

Прибой Модуль-3.5 и Стек-НС3

Прибой Модуль-3.5

Стек-НС3

Privacy Advocates

t.me/prv_adv/3500

Privacy
Advocates

Всегда рады сотрудничеству!

+7 (903) 762-64-15 | corp@privacy-advocates.ru | t.me/prv_adv

Telegram-канал