|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | | |
| УТВЕРЖДАЮ:  ИСПОЛНИТЕЛЬ:  Генеральный директор  ООО «СИГМА» |  | УТВЕРЖДАЮ:  ЗАКАЧИК:  Генеральный директор  ООО «ИнтерРАО – ИТ» |
|  |  |  |
|  |  |  |
|  |  |  |
| «\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2019 г. |  | «\_\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2019 г. |
|  | | |
|  | | |
| **ТИПОВАЯ ТИРАЖНАЯ СИСТЕМА «ЭЛЕКТРОННЫЙ АРХИВ»** | | |
| ТЕХНИЧЕСКие требования | | |
| Функции безопасности прикладного программного обеспечения Типовой тиражной системы «Электронный архив»  Версия 2.0 | | |
| Листов 28 | | |
| СОГЛАСОВАНО |  | СОГЛАСОВАНО |
|  |  |  |
|  |  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| «\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2019 г. |  | «\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2019 г. |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| Москва 2025 | | |

[1. Термины и сокращения 4](#_Toc32243639)

[2. Общие сведения 6](#_Toc32243640)

[2.1. Основание для разработки 6](#_Toc32243641)

[2.2. Наименование организаций-участников 6](#_Toc32243642)

[3. Общие требования к функциям безопасности ППО ТТС ЭА 6](#_Toc32243643)

[4. Требования к авторизации и аутентификации 6](#_Toc32243644)

[5. Требования к реализации прав доступа 6](#_Toc32243645)

[5.1. Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы(УПД.4) 7](#_Toc32243646)

[5.2. Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы (УПД.5) 7](#_Toc32243647)

[5.3. Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу (УПД.10) 7](#_Toc32243648)

[6. Требования к разграничению доступа по элементам организационной структуры 8](#_Toc32243649)

[6.1. Требования к функциональности 8](#_Toc32243650)

[6.2. Решения по реализации функциональности 8](#_Toc32243651)

[7. Требования к логированию действий пользователей и администраторов 8](#_Toc32243652)

[7.1. Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения (РСБ.3) 9](#_Toc32243653)

[8. Требования к безопасной конфигурации Веб-компонентов ТТС ЭА 9](#_Toc32243654)

[9. Требования к шифрованию каналов передачи информации управления ключами 9](#_Toc32243655)

[10. Требования к исходному коду приложений 9](#_Toc32243656)

[11. Требования к контролю целостности программного обеспечения 9](#_Toc32243657)

[11.1. Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации (ОЦЛ.1) 10](#_Toc32243658)

[11.2. Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций (ОЦЛ.3) 10](#_Toc32243659)

[12. Требования к уничтожению персональных данных 10](#_Toc32243660)

[12.1. Удаление персональных данных по запросу пользователя 10](#_Toc32243661)

[12.1.1. Требования к функциональности 10](#_Toc32243662)

[12.1.2. Описание бизнес-процессов 13](#_Toc32243663)

[12.1.3. Решения по реализации функциональности 14](#_Toc32243664)

[12.1.3.1. Подсистема администрирования 14](#_Toc32243665)

[12.1.3.2. Документирование 14](#_Toc32243666)

[12.1.3.3. Карточка документа 14](#_Toc32243667)

[12.1.3.4. Модель данных 16](#_Toc32243668)

[12.1.3.5. Интеграция 16](#_Toc32243669)

[12.1.3.6. Журналирование и уведомления 16](#_Toc32243670)

[12.2. Обезличивание персональных данных 17](#_Toc32243671)

[12.2.1. Требования к функциональности 17](#_Toc32243672)

[12.2.2. Описание бизнес-процесса 18](#_Toc32243673)

[12.2.3. Решения по реализации функциональности 18](#_Toc32243674)

[12.2.3.1. Подсистема администрирования 18](#_Toc32243675)

[12.2.3.2. Документирование 18](#_Toc32243676)

[12.2.3.3. Атрибут версии контента 18](#_Toc32243677)

[12.2.3.4. Модель данных 19](#_Toc32243678)

[12.2.3.5. Интеграция 19](#_Toc32243679)

[12.2.3.6. Журналирование 19](#_Toc32243680)

[12.3. Интерфейс ответственного за исключение 20](#_Toc32243681)

[При загрузке формы сразу может быть подгружен перечень документов (если более 50-ти строк, то делать группировку по признакам в отношении типа документа) с различными статусами на текущую обработку (на обезличивание и удаления или документы с просроченными сроками обработки) и документы задачи по которым просрочены. В верхней части интерфейсной формы 21](#_Toc32243682)

[13. Требования к перечню регистрируемых типов событий безопасности 21](#_Toc32243683)

[13.1. Требования к функциональности 21](#_Toc32243684)

[13.2. Решения по реализации функциональности 21](#_Toc32243685)

[13.2.1. Документирование 21](#_Toc32243686)

[14. Требования к функционалу управления сессиями пользователей 22](#_Toc32243687)

[14.1. Требования к функциональности 22](#_Toc32243688)

[14.2. Решения по реализации функциональности 22](#_Toc32243689)

[14.2.1. Документирование 22](#_Toc32243690)

[15. требования к функционалу обработки данных о событиях информационной безопасности 22](#_Toc32243691)

[15.1. Требования к функциональности 22](#_Toc32243692)

[15.2. Решения по реализации функциональности 23](#_Toc32243693)

[15.2.1. Задания 23](#_Toc32243694)

[15.2.2. Подсистема администрирования 25](#_Toc32243695)

[15.2.3. Документирование 26](#_Toc32243696)

[16. требования к контролю целостности и к обеспечению возможности восстановления программного обеспечения 26](#_Toc32243697)

[17. Требования к доработке инструкций и руководств 26](#_Toc32243698)

1. Термины и Определения

|  |  |
| --- | --- |
| Термин, сокращение | Определение |
| API | Интеграционный интерфейс - описание способов (набор [классов](https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D0%B0%D1%81%D1%81_(%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5)" \o "Класс (программирование)), [процедур](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%86%D0%B5%D0%B4%D1%83%D1%80%D0%B0_(%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5)" \o "Процедура (программирование)), [функций](https://ru.wikipedia.org/wiki/%D0%A4%D1%83%D0%BD%D0%BA%D1%86%D0%B8%D1%8F_(%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5)" \o "Функция (программирование)), [структур](https://ru.wikipedia.org/wiki/%D0%A1%D1%82%D1%80%D1%83%D0%BA%D1%82%D1%83%D1%80%D0%B0_(%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5)" \o "Структура (программирование)) или [констант](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BD%D1%81%D1%82%D0%B0%D0%BD%D1%82%D0%B0_(%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5)" \o "Константа (программирование))), которыми одна компьютерная программа может взаимодействовать с другой программой ([англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA" \o "Английский язык) application programming interface). |
| RFC | Рабочее предложение (Request for Comments). Документ из серии пронумерованных информационных документов Интернета, содержащих технические спецификации и стандарты, широко применяемые во всемирной сети |
| SIEM | Класс систем сбора и централизованного анализа событий информационной безопасности (Security information and event management) |
| Syslog | Стандарт отправки и регистрации сообщений о происходящих в системе событиях |
| TCP | Протокол управления передачей данных (Transmission Control Protocol) |
| UDP | Протокол пользовательских датаграмм (User Datagram Protocol) |
| Администратор безопасности | Пользователь системы, обладающий ролями, позволяющими управлять правами доступа и осуществлять мониторинг событий информационной безопасности |
| Администратор информационной безопасности | Роль, позволяющая осуществлять мониторинг событий информационной безопасности |
| Бумажный документ | Информация, зафиксированная на бумажном носителе, на котором содержатся оригиналы всех необходимых оттисков печатей, штампов и подписей о согласовании и утверждении документа |
| ДО | Дочернее общество |
| Документ | Зафиксированная на носителе информация с реквизитами, позволяющими ее идентифицировать. Состоит из структурированной (карточки) и неструктурированной (контента) частей |
| ИБ | Информационная безопасность |
| Идентификатор | Уникальный идентификатор документа в Системе |
| Карточка | Структурированная часть документа, которая представляет собой полный, логически упорядоченный список атрибутов документа |
| Контент (скан-образ) | Неструктурированная часть документа в виде электронного файла. Файл может быть отсканированной копией (копией оригинала бумажного документа) или полученный иным путем. В системах 1С вместо термина «Контент» используется - «Печатная форма». |
| ОС | Операционная система |
| ОЦО | ООО «Интер РАО-Управление сервисами» |
| ПДн | Персональные данные |
| ППО | Прикладное программное обеспечение |
| ПО | Программное обеспечение |
| Реестр | Сгруппированный по пакетам список документов, предназначенный для подтверждения передачи документов |
| Событие ИБ, событие информационной безопасности | Идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение политики информационной безопасности, или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности [ISO/IEC 18044: 2004] |
| СУБД | Система управления базами данных |
| ТТС ЭА | Типовая тиражная система «Электронный архив» |
| ТЗ | Техническое задание |
| Электронный документ | Документ, обладающий только структурированной частью, подготовленной с помощью технических средств, и являющийся юридически значимым оригиналом.  Может состоять их XML-файла, ЭП, человеко-читаемого представления и протокола передачи. |

1. Общие сведения
   1. **Основание для разработки**

Основанием для разработки функций безопасности прикладного программного обеспечения типовой тиражной системы «Электронный архив» является Технический проект на Систему защиты персональных данных типовой тиражной системы Электронный архив (76229745.425180.001).

* 1. **Наименование организаций-участников**

Заказчик: ООО «ИнтерРАО – ИТ»

Исполнитель: ООО «СИГМА».

1. Общие требования к функциям безопасности ППО ТТС ЭА

Функции безопасности ППО ТТС ЭА должны обеспечивать выполнение следующих требований к информационной безопасности:

1. требования к авторизации и аутентификации;
2. требования к реализации прав доступа;
3. требования к логированию действий пользователя и администраторов;
4. требования к безопасной конфигурации Веб-компонентов Системы;
5. требования к шифрованию каналов передачи информации управления ключами;
6. требования к аутентификации и обработке сессий;
7. требования к исходному коду приложений;
8. требования к контролю целостности программного обеспечения;
9. требования к обработке персональных данных, в том числе:

* уничтожение персональных данных
* обезличивание персональных данных при выгрузке.

Требования к техническим решениям по реализации мер защиты информации, обеспечивающим выполнение функций безопасности ППО ТТС ЭА, описаны ниже.

1. Требования к авторизации и аутентификации

Решения по реализации мер защиты информации, обеспечивающим выполнение требований к авторизации и аутентификации, описаны в документе «Технический проект. Типовая тиражная система «Электронный архив».

Дополнительных требований к ППО ТТС ЭА по реализации функций безопасности не предъявляется.

1. Требования к реализации прав доступа

Решения по мерам защиты информации, обеспечивающим выполнение требований к реализации прав доступа, описаны в документе «Технический проект. Типовая тиражная система электронный архив».

В ППО ТТС ЭА дополнительно должны быть реализованы следующие меры защиты информации, обеспечивающие выполнение требований к реализации прав доступа:

* разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы (УПД.4);
* назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы (УПД.5);
* блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу (УПД.10).

Технические решения по реализации указанных мер защиты описаны ниже.

* 1. **Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы(УПД.4)**

В ТТС ЭА должны быть реализованы отдельные роли администраторов:

* Администратор информационной безопасности, управляющий правами доступа и осуществляющей мониторинг событий безопасности;
* Администратор ППО.
  1. **Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы (УПД.5)**

В ТТС ЭА базы данных (хранилища) различных операторов ПДн должны быть разделены: должна быть реализована ролевая модель доступа, учитывающая принадлежность пользователей и данных к конкретному ДО. При настройке системы по умолчанию пользователи должны иметь доступ только к данным «своего» ДО.

* 1. Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу (УПД.10)

В ТТС ЭА должно быть реализовано завершение сеанса и блокирование доступа пользователя к ТТС ЭА после периода бездействия пользователя, установленного администратором.

Настройка параметров завершения сеанса и блокирования доступа пользователя при наступлении периода бездействия должна осуществляться Администратором безопасности средствами штатных утилит сервера приложений ТТС ЭА.

При осуществлении доступа к ТТС ЭА по временной ссылке со стороны ТТС ЭА должно обеспечиваться ограничение предельного срока действия ссылки.

Настройка предельного срока действия ссылки должна осуществляться Администратором безопасности средствами штатных утилит сервера приложений ТТС ЭА.

Порядок настройки завершения сеанса и блокирования доступа пользователя и ограничения предельного срока действия ссылки описан в Руководстве администратора ППО ТТС ЭА.

1. Требования к разграничению доступа по элементам организационной структуры
   1. **Требования к функциональности**

Цель разграничение доступа по ДО – закрыть доступ к документам, сформированным в системе-источнике «своего» ДО, сотрудникам «чужих» ДО.

Пользователь считается «своим»:

* если является сотрудником того же филиала, который соотнесен с внешней системой-источником документа;
* если имеет роль, для которой открыт доступ к данным этого филиала.

Во всех остальных случаях пользователь считается «чужим».

Функционал следует создавать поэтапно:

Этап 1 – индикативный контроль доступа. Любой пользователь технически может получить документ из любого филиала. Правомерный и неправомерный доступ к документам соответствующим образом отражается в логах событий информационной безопасности.

Этап 2 – блокирующий контроль доступа. «Чужой» пользователь не должен видеть неразрешенных для него документов.

Настройки, разграничивающие доступ по ДО, делаются в справочнике «Роли» - для филиальных ролей в поле «Филиал» указываются идентификаторы филиалов, к документам которых роль должна иметь доступ.

Идентификаторы могут задаваться как в явном, так и в неявном (через место в иерархии – например, элемент и его потомки) виде.

* 1. **Решения по реализации функциональности**

Решений по реализации функциональности не требуется – функционал в ТТС ЭА уже существует.

1. Требования к логированию действий пользователей и администраторов

Решения по мерам защиты информации, обеспечивающим выполнение требований к логированию действий пользователей и администраторов, описаны в документе «Технический проект. Типовая тиражная система «Электронный архив».

В ППО ТТС ЭА дополнительно должны быть реализованы следующие меры защиты информации, обеспечивающие выполнение требований к логированию действий пользователей и администраторов:

* сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения (РСБ.3);
* мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них (РСБ.5);
* защита информации о событиях безопасности (РСБ.7).

Технические решения по реализации указанных мер защиты описаны ниже.

* 1. **Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения (РСБ.3)**

ППО ТТС ЭА должно обеспечивать возможность отправки событий безопасности за определенный промежуток времени во внешние системы (в SIEM).

В ППО ТТС ЭА должна быть реализована возможность просмотра и анализа информации о действиях отдельных пользователей в Системе.

1. Требования к безопасной конфигурации Веб-компонентов ТТС ЭА

Решения по реализации мер защиты информации, обеспечивающим выполнение требований к безопасной конфигурации Веб-компонентов ТТС ЭА, описаны в документе «Технический проект. Типовая тиражная система «Электронный архив».

Дополнительных требований к решениям по безопасной конфигурации Веб-компонентов ТТС ЭА не предъявляется.

1. Требования к шифрованию каналов передачи информации управления ключами

Решения по реализации мер защиты информации, обеспечивающим выполнение требований к шифрованию каналов передачи информации управления ключами, описаны в документе «Технический проект. Типовая тиражная система «Электронный архив».

Дополнительных требований к ППО ТТС ЭА по реализации требований к шифрованию каналов передачи информации управления ключами не предъявляется.

1. Требования к исходному коду приложений

Решения по реализации мер защиты информации, обеспечивающим выполнение требований к исходному коду приложений, описаны в документе «Технический проект. Типовая тиражная система «Электронный архив».

Дополнительных требований к ППО ТТС ЭА по реализации требований к исходному коду приложений не предъявляется.

1. Требования к контролю целостности программного обеспечения

Решения по реализации мер защиты информации, обеспечивающим выполнение требований к контролю целостности программного обеспечения, описаны в документе «Технический проект. Типовая тиражная система «Электронный архив».

В ППО ТТС ЭА дополнительно должны быть реализованы следующие меры защиты информации, обеспечивающие выполнение требований к контролю целостности программного обеспечения:

* контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации (ОЦЛ.1)
* обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций (ОЦЛ.3).

Технические решения по реализации указанных мер защиты описаны ниже.

* 1. **Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации (ОЦЛ.1)**

В инструкции администратора системы и администратора безопасности должен быть добавлен пункт «Перечень компонент ППО ТТС ЭА устанавливаемых на контроль целостности». В инструкциях необходимо перечислить исполняемые компоненты и неизменяемые библиотеки или скрипты, связанные с работой функций безопасности (ролевая модель, журналирование, интерфейс администратора) устанавливаемых на контроль целостности.

* 1. **Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций (ОЦЛ.3)**

В инструкции администратора системы и администратора безопасности должен быть добавлен пункт «Порядок восстановления ППО ТТС ЭА». Должна быть разработана отдельная «Инструкция по восстановлению ППО ТТС ЭА».

1. Требования к уничтожению персональных данных

В ППО ТТС ЭА дополнительно должны быть реализованы следующие меры защиты информации, обеспечивающие уничтожение персональных данных:

* удаление персональных данных по запросу пользователя;
* предложения к удалению документов из реестра и пакета в случае удаления одного из документов, входящих в реестр.

Технические решения по реализации указанных мер защиты описаны ниже.

* 1. **Удаление персональных данных по запросу пользователя или удаление контента по запросу его владельца**
     1. **Требования к функциональности**

Должен быть реализован функционал логического удаления (исключения из обработки) документов, содержащих персональные данные физического лица или удаление контента по запросу его владельца.

Для работы с нижеописанным функционалом, во внешних системах должно быть предусмотрено три режима работы:

1. режим отладки обработки ПДн. В этом режиме обработка состояний документа должна проводится с подтверждением каждого шага сотрудником с ролью «Ответственный за обработку» на стороне ТТС ЭА;
2. режим автоматической обработки ПДн. В этом режиме исключение документов по запросу из внешних систем происходит без подтверждения оператором ТТС ЭА.
3. режим принудительного исключения документа из обработки по причинам в том числе, не связанным с требованиями законодательства или внешними запросами. Например, по решению владельца документа (внешней системы).

В ТТС ЭА исключение документа из обработки необходимо обеспечить путем реализации следующих сценариев работы с электронным архивом:

* Отладка/Принудительно – на основании полученного при помощи API из внешних систем списка идентификаторов документов. В этом сценарии исключение документов по запросу из внешней системы происходит только при подтверждении списка или отдельных документов оператором в интерфейсе ТТС ЭА со специально выделенной ролью - «Ответственный за исключение».
* Автоматически – на основании полученного при помощи интеграционного интерфейса (далее – API) ТТС ЭА из внешних систем списка идентификаторов документов для определенных внешней системой документов, а также по истечению срока давности документа. В этом сценарии исключения документов по запросу из внешней системы происходит без необходимости действий со стороны оператора ТТС ЭА с ролью «Ответственный за исключение». При этом у оператора с ролью «Ответственный за исключение» должна быть возможность посмотреть статусы автоматически исключённых документов.

Сценарий «Отладка/Принудительно» так же может использоваться и для отдельных документов, не связанных с обработкой ПДн (например, когда по решению владельца документа его электронная копия должна быть сделана недоступной из электронного архива для внешних систем).

В API ТТС ЭА при обращении из внешней системы следует предусмотреть возможность передачи следующих параметров для каждого уникального идентификатора документа (id):

* «Сценарий работы». Параметр должен предусматривать следующие возможные значения: «Отладка», «Принудительное исключение» и «Автоматическое».
* «Срок хранения, дней, текст». Параметр носит справочный характер и должен предусматривать следующие возможные значения: дни (тип данных: кол-во дней до окончания обработки) и «Бессрочно». В карточку документа этот параметр должен передаваться из внешней системы в качестве дополнительного. При первичном внесении документа в ТТС ЭА параметр не заполняется только в случае, если не известно, с какого момента времени необходимо вести по нему отсчёт (например, для копий договоров, этот срок должен начинаться с даты подписания финансового акта, а для «отгрузочных документов», например – счёта и счёта-фактуры с момента их подписания).

Параметр «Срок хранения, дней, текст» со установленным значением «Бессрочно», предполагает неограниченный срок обработки документа (хранения) (для случаев, установленных законодательством и определяемых внешней системой).

По этому полю должна быть обеспечена возможность поиска для типа поиска «Документы».

Исключение документов должно начинаться с систем-источников (бухгалтерские, кадровые документы и другие интегрируемые с ТТС ЭА внешние системы). В системе-источнике существует связь между документами и физическими лицами, чьи персональные данные в них фигурируют.

В системах-источниках также должны быть предусмотрены механизмы:

* фиксации начала отсчёта срока хранения документа, установленного локальными нормативными актами или ФЗ РФ;
* отслеживание события фиксации начала отсчёта срока хранения, при наступлении этого события данные о сроке хранения должны быть переданы в ТТС ЭА, в параметр «Срок хранения, дней».

При осуществлении логического удаления документов в системах-источниках, с помощью API в ТТС ЭА передаются идентификаторы документов.

В ТТС ЭА обработка документов проводится в зависимости от сценария работы.

Документы, для которых исключение происходит автоматически, должны периодически просматриваться пользователем ТТС ЭА с ролью «Ответственный за исключение» в части контроля перечня таких документов и корректности их исключения из обработки (проверка статусов).

Документы, для которых исключение происходит в сценарии «отладка» и «принудительное исключение», документы исключаются пользователем ТТС ЭА с ролью «Ответственный за исключение» после их анализа.

Если документ содержит персональные данные более чем одного физического лица, этот документ не исключается – в нем осуществляется обезличивание персональных данных (см. раздел «12.2. Обезличивание персональных данных»).

* + 1. **Описание бизнес-процессов**



В случае если исключаемый документ будет содержать ПДн нескольких субъектов, то должно производиться обезличивание такого документа по процедуре описанной в п.п. 12.2.1.



Анализ импортированного из внешней системы списка документов, подлежащих исключению в принудительном (ручном) порядке; определение документов, подлежащих исключению, а также контроль автоматически исключенных документов осуществляется в интерфейсной форме «Поиск и обработка» интерфейса пользователя с ролью «Ответственный за исключение».

* + 1. **Решения по реализации функциональности**
       1. Подсистема администрирования

В подсистеме администрирования требуется добавить функцию «Управление исключением документов» (раздел «Управление сервисами», п. 4.3.3.2.1 Технического задания).

Функция должна предполагать:

* ручное проставление статуса «Исключен» в атрибутах документов;
* ручной откат (возврат к предшествующему) статуса «Исключен» в атрибутах документов – присвоенного как вручную, так и автоматически;
* доступ на чтение к атрибутам контента;
* доступ к интерфейсу (функциям) пользователя с ролью «Ответственный за исключение»;
* доступ к атрибуту контента «Срок хранения, дней» на редактирование;
* доступ к атрибуту контента «Тип исключения» на редактирование;
* доступ к атрибуту контента «Основание для исключения»;
* право на принудительное исключение документов.

Требуется создать роль «Ответственный за исключение» для пользователей, выполняющих функцию управления исключением документов. Роль может быть «филиальной», т.е. назначаться сотруднику филиала, который управляет контентом архива относящегося к своему ДО.

* + - 1. Документирование

Должна быть подготовлена инструкция пользователя для роли «Ответственный за исключение».

* + - 1. Атрибуты версии контента

В список возможных статусов документа (см. п. 4.3.1.5.1.3 Технического задания) добавить статус «Исключен», предполагающий исключение документа из всех видов обработки (логическое удаление документа). Статус присваивается после подтверждения пользователем с ролью «Ответственный за исключение» документа на удаление.

Заполняемые сведения в атрибутах документа необходимы для возможности дополнительного контроля со стороны пользователя ТТС ЭА с ролью «Ответственный за исключение» или администратора ТТС ЭА сведений, связанных со сведениями о временных характеристиках исключения документа (удаления) и попытками обращения к документу пользователей внешних систем при сценарии «Отладка/принудительно».

Список полей и логика заполнения атрибутов представлены в таблице 1.

**Таблица 1. Поля атрибутов документа**

| **№ п.п.** | **Наименование** | **Тип данных** | **Описание** | **Обязательность заполнения пользователем** |
| --- | --- | --- | --- | --- |
| 1 | Дата начала хранения | Дата | Дата начала хранения документа | - |
| 2 | Срок хранения, дней | Числовой | Срок хранения документа; по истечении этого срока документ подлежит логическому удалению | - |
| 3 | Дата последней активности | Дата | Дата последних действий с контентом | - |
| 4 | Период невостребован-ности, дней | Числовой | Длительность периода невостребованности (отсутствия активностей) контента | - |

Атрибут «Период невостребованности, дней» является расчетным. Формула расчета:

*Текущая дата - Дата последней активности*

Атрибут «Дата последней активности» и «Период невостребованности, дней» предназначены для повышения информированности ответственного за исключения – с тем, чтобы решение о логическом удалении документа было более обоснованным.

Для заполнения атрибута «Дата последней активности» используется дата последнего из действий:

− Создание контента.

− Изменение статуса документа (кроме изменения статуса на «Исключен» и отката от статуса «Исключен»).

− Изменение в атрибутах контента.

− Изменение контента.

− Обращение к контенту из внешней системы:

• Предоставление прав на контент.

• Обращение к документу при помощи запроса на архивную версию контента.

• Обращение к контенту при загрузке атрибутов (в т.ч. «Дата начала хранения» или «Срок хранения, дней», статус документа) из внешней системы.

• Обращение к контенту при загрузке файла из внешней системы.

• Запрос из внешней системы в ТТС ЭА атрибутов.

* + - 1. Модель данных

Необходимо дополнить таблицу, хранящую атрибуты документов, полями, описанными в пункте «Атрибуты версии контента» настоящих Технических требований.

Необходимо создать таблицу, хранящую статусы процедур импорта идентификаторов документов.

* + - 1. Интеграция

API взаимодействия с системами-источниками должен быть дополнен в части, касающейся получения атрибутам контента значений полей «Дата начала хранения», «Срок хранения, дней», статус контента «Исключён», «Основание для исключения», а также идентификаторов документов, удаленных в системах-источниках.

* + - 1. Журналирование и уведомления

Взаимодействие через API ТТС ЭА c внешними системами должно журналироваться. Журнал должен содержать: дату и время события, учетную запись пользователя, идентификаторы обрабатываемых документов, время обработки, результат обработки, сообщения об ошибках ТТС ЭА, а также сообщения, полученные от операционной системы.

Для мониторинга сценариев «Отладка» и «Принудительное исключение» документов требуется генерировать письмо или уведомление в личном кабинете пользователю с ролью (уведомление) «Ответственный за исключение» или администратору безопасности в случае, если документы удалены раньше, чем допускается, исходя из значения параметра «Срок хранения, дней» (п.п. 2 таблицы 1). Для тех документов для которых определён срок хранения внешней системой. Например, в случае удаления документа с атрибутом «Срок хранения» со значением «Бессрочно». Или пришёл запрос на удаление уже помеченного контента как «Исключён». Также в интерфейсной форме «Личный кабинет» такое событие должно быть подсвечено или цветом, или отдельным значком в интерфейсе () с ссылкой на документ или список документов.

* 1. **Обезличивание персональных данных**
     1. **Требования к функциональности**

Если документ содержит персональные данные более чем одного физического лица, этот документ не исключается – в нем осуществляется обезличивание персональных данных.

Решение об обезличивании должно приниматься пользователем во внешней системе, взаимодействующей с ТТС ЭА.

Обезличиваются персональные данные одного физического лица – если физическое лицо требует удалить документы, содержащие его персональные данные.

Обезличиваются персональные данные одного и более физических лиц – если соответствующий документ необходимо выдать заявителю-одному из фигурантов (не обезличиваются только персональные данные самого заявителя).

По запросу органов государственной власти документы, содержащие персональные данные, передаются в необезличенном состоянии (такие документы подпадают под закон №125-ФЗ «Об архивном деле в Российской Федерации» при условии исключения их из процессов обработки).

В API ТТС ЭА из внешней системы должен быть передан признак типа обезличивания:

* селективное обезличивание (при обезличивании ПДн одного физического лица в документе содержащем ПДн нескольких физлиц или только одного);
* инверсионное обезличивание (при обезличивании ПДн всех физических лиц, содержащихся в списочном документе кроме одного);
* краткое описание задачи по обработке документа в части обезличивания.

Таким образом, контент одного и того же документа при обезличивании должен храниться в двух версиях:

* версия «Необезличенная» - с необезличенными персональными данными – для предоставления по запросу органов государственной власти и для целей, предусмотренных законом №125-ФЗ «Об архивном деле в Российской Федерации»;
* версия «Обезличенная» - с обезличенными персональными данными – для прочих целей.

При возникновении у документа обезличенной версии (при запросе субъекта ПДн на удаление его персональных данных) эта версия становится активной и используется для обработки.

Для предоставления документов по запросу органов государственной власти необходимо привести все документы к необезличенной версии контента. Это целесообразно делать при помощи задания.

Обезличивание структурированной информации проводится с использованием средств автоматизации любым из методов, рекомендованных Роскомнадзором в «Методических рекомендациях по применению приказа Роскомнадзора от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных» (https://rkn.gov.ru/docs/Xerox\_Phaser\_3200MFP\_20131216122746.pdf).

Обезличивание контента проводится вручную на бумажном носителе, после чего носитель сканируется и формируется обезличенная версия контента. Подробное описание алгоритма действия оператора ТТС ЭА приведено в п.п. 12.3.2.

Предоставление обезличенных документов на бумажных носителях осуществляется в том же порядке, что и необезличенных.

* + 1. **Описание бизнес-процесса**



* + 1. **Решения по реализации функциональности**
       1. Подсистема администрирования

В подсистеме администрирования требуется дополнить функцию «Управление исключением документов» (раздел «Управление сервисами», п. 4.3.3.2.1 Технического задания) пунктом «Доступ к оригиналу обезличенного (исключённого) документа (доступ к Архиву)». Необходимо дополнить ролевую модель ТТС ЭА ролью доступа к Архивным версиям документов. Таким образом можно регулировать доступность к архивным документам из внешних систем.

* + - 1. Документирование

В инструкцию пользователя для роли «Ответственный за исключение» должны быть добавлены пункты:

* Работа с необезличенной и обезличенной версиями контента документа.
* порядок восстановления архивной версии документа (логически удалённым или необезличенным версиям).
  + - 1. Атрибут версии контента

В атрибут версии контента необходимо добавить заполняемое вручную поле «Обезличенная/Необезличенная». Возможные значения поля – «Обезличенная» и «Необезличенная». Значение «Обезличенная» выбирается для версии, содержащей обезличенный контент. Значение «Необезличенная» выбирается для версии, содержащей необезличенный контент.

В атрибут версии контента необходимо добавить заполняемое вручную на стороне внешней системы поле «Справка о ПДн». Должно быть заполнено оператором внешний системы как комментарий по постановке задачи по обезличиванию (перечень ПДн, подлежащих обезличиванию в документе или перечень ПДн, которые должны остаться в документе).

* + - 1. Модель данных

Необходимо дополнить таблицу, хранящую атрибуты версий контента, полем, описанным в пункте «Атрибут версии контента» настоящего раздела Технических требований.

* + - 1. Интеграция

В API ТТС ЭА должен быть предусмотрен параметр признака типа обезличивания:

* селективное обезличивание (при обезличивании ПДн одного физического лица в документе содержащем ПДн нескольких физлиц или только одного);
* инверсионное обезличивание (при обезличивании ПДн всех физических лиц, содержащихся в списочном документе кроме одного).
* краткое описание задачи по обработке документа в части обезличивания (перечень ПДн, словесное описания необходимой процедуры или задачи обезличивания).

В API так же должен быть предусмотрен параметр «Доступ к Архиву», позволяющий запросить оригиналы (не изменённые версии документов) из внешней системы, находящиеся в Архиве.

Так как процедура обезличивания (работа со сканированным изображением документа в части вымарывания необходимых метаданных) происходит на стороне оператора сканирования документов, то необходимо предусмотреть процедуры работы с документами в зависимости от передаваемых параметров через API в ТТС ЭА.

API взаимодействия со связанными системами должен быть дополнен в части, касающейся возможности экспорта сведений из ТТС ЭА в связанную систему значения поля «Обезличенная/Необезличенная» активной версии контента документа (получение статуса по запросу). В результате в связанной системе будет видно, обезличен ли контент документа в ТТС ЭА.

* + - 1. Журналирование

Взаимодействие через API ТТС ЭА c внешними системами должно журналироваться. Журнал должен содержать: дату и время события, учетную запись пользователя, идентификаторы обрабатываемых документов, время обработки, результат обработки, сообщения об ошибках ТТС ЭА, а также сообщения, полученные от операционной системы.

* 1. **Описание алгоритма действий оператора с ролью «Ответственный за исключение»**
     1. Описание алгоритма действий оператора при удалении документа

При передаче внешней системой список на удаление id документов в ТТС ЭА, то оператор должен:

* в случае принудительного исключения – получить уведомление, что он должен совершить действие по логическому исключению документа (-ов) путём проставления атрибута контента в статус «Исключён». При этом оператор должен проконтролировать обязательные к заполнению атрибут – «Основание для исключения».
* в случае автоматического исключения через внешний запрос – получить уведомление, что проведена процедура исключения документов и получить возможность через поиск посмотреть на список документов и основания исключения этих документов (заявление, срок обработки и т.д.).

Для документов, находящихся в процессе оформления или заведения в ТТС ЭА должны быть завершены все процедуры до его логического удаления даже если запрос пришёл на автоматическое удаление.

В результате любых действий всегда должна сохраняться оригинальная копия контента документа.

* + 1. Описание алгоритма действий оператора при обезличивании контента

При передаче из внешней системы id контента подлежащего обезличиванию (селективного или инверсного) пользователь с ролью «Ответственный за исключение» должен только контролировать процесс обезличивания путём контроля атрибутов контента и содержимого контента.

Работы по типам обезличивания должны проводить операторы, загружающие и имеющие доступ к «оригиналам» документов.

Непосредственную замену должен проводить пользователь в роли «Инициатор».

Документы должны быть переведены автоматически в статус на «исправление» с одновременным временным откреплением от учётной системы (до окончания корректировки документа) с комментарием, переданным из внешней системы через API с указанием типа обезличивания и какие именно персональные данные в пакете документов или в конкретном документе, должны быть обезличены. Далее оператор должен на этапе сканирования документов провести физическое обезличивание указанных ПДн (любым удобным способом: временно заклеить ПДн и заново отсканировать документ или напечатать документ и вымарать указанные ПДн). При этом Ответственный за обработку должен проконтролировать корректность введённых данных и установленных атрибутов. Далее процедуры должны соответствовать штатным.

Для документов, находящихся в процессе оформления или заведения в ТТС ЭА должны быть завершены все процедуры до начала процесса по его обезличиванию.

В случае если документ имеет атрибут контента «замене не подлежит», но при этом содержит ПДн подлежащие обезличиванию. Проводится процедура обезличивания, описанная выше.

В результате любых действий всегда должна сохраняться оригинальная копия контента документа.

* + 1. Описание интерфейса оператора

Интерфейс для работы пользователя с ролью «Ответственный за исключение» состоит интерфейсной формы:

* Личный кабинет - Поиск и обработка (левая колонка не показана).

Форма «Поиск и обработка» может имееть вид:



Интерфейсная форма предназначена, как для работы с текущим документами по бизнес-процессам исключения или обезличивания, так и для поиска документов по различным параметрам, в т.ч. по принадлежности к реестрам. Интерфейсная форма должна иметь стандартный интерфейс личного кабинета ТТС ЭА.

В части реализации «кнопок» указанная форма показана условно, необходимо сделать в «штатном интерфейсе»

Интерфейсная форма основана на существующем интерфейсе поиска документов. Добавлены возможности:

* поиска по версии контента документа (для поиска обезличенных и необезличенных версий контента).
* поиска по Справке о ПДн (необходимых действиях с копией документа)

Должна быть реализована возможность сортировки и настройки фильтра ко колонкам (полям) формы поиска.

При необходимости могут быть добавлены другие параметры для отображения в форме поиска (например идентификатор документа).

В верхней части интерфейсной формы находится область кнопок, инициирующих принудительное выполнение процедур «Исключение документов» и «Обезличивание документов» (указанные кнопки могут быть перенесены в штатный интерфейс слева).

При загрузке формы сразу может быть подгружен перечень документов Справке о ПДн с различными статусами на текущую обработку (на обезличивание и удаления или документы с просроченными сроками обработки) и документы задачи по которым просрочены. В верхней части интерфейсной формы

1. **Требования к перечню регистрируемых типов событий безопасности**
   1. **Требования к функциональности**

В ППО ТТС ЭА должны регистрироваться следующие типы событий безопасности:

* успешная аутентификация (для внешних систем и пользователей);
* ошибки аутентификации (для внешних систем и пользователей в том числе ошибки при аутентификации по сертификатам);
* ошибки авторизации (для внешних систем и пользователей);
* ошибки, связанные с сетевой связностью;
* ошибки файловой системы;
* создание новых учетных записей;
* удаление существующих учетных записей;
* изменение привилегий учетной записи;
* успешная обработка правил матрицы доступа (попытки доступа пользователей к функциям (набору функций, если они связанны с одной формой) в соответствии с полученными ролями в том числе по отношению к ДО);
* неуспешная обработка правил матрицы доступа (попытки доступа пользователей к функциям (набору функций, если они связанны с одной формой) в соответствии с полученными ролями по отношению к ДО).

Перечень типов событий безопасности, реквизитный состав и механизм их регистрации должны быть реализованы в программном коде ТТС ЭА.

* 1. **Решения по реализации функциональности**
     1. Документирование

В инструкцию для роли «Администратор информационной безопасности» необходимо добавить пункт «Регистрируемые типы событий информационной безопасности».

1. **Требования к функционалу управления сессиями пользователей**
   1. **Требования к функциональности**

Должен быть реализован функционал просмотра и прекращения сессий пользователей системы.

* 1. **Решения по реализации функциональности**
     1. Документирование

В инструкцию для роли «Администратор системы» ТТС ЭА необходимо добавить пункт «Просмотр и прекращение сессий пользователей системы». В этом пункте должно быть:

* указано место расположения конфигурационного файла ТТС ЭА;
* порядок настройки прекращения сессии по таймауту.

1. **требования к функционалу обработки данных о событиях информационной безопасности**
   1. **Требования к функциональности**

Необходимо обеспечить следующую функциональность работы с данными о событиях информационной безопасности:

* автоматическая передача данных в SIEM.
* хранение данных в SIEM не менее 6 мес.
* создание и хранение резервных копий журналов событий безопасности (перечень типов событий приведён в п.п. 13.1).
* мониторинг (просмотр и анализ).
* генерация сигналов администратору информационной безопасности о признаках инцидентов, в т.ч. отправка электронного письма.

Данные о событиях информационной безопасности:

* Формируются сервисом ТТС ЭА и отправляются в SIEM в порт 6514/TCP,UDP в формате протокола Syslog (RFC5424, RFC5426).
* Хранятся:
  + в репозитории SIEM;
  + в бэкапах репозитория SIEM на отдельном сервере.

Хранение данных о событиях информационной безопасности ТТС ЭА в репозитории SIEM должно продолжаться не менее 6 мес.

Бэкапы репозитория должны создаваться системой SIEM.

Системное время ТТС ЭА, SIEM и сервера хранения бэкапов репозитория SIEM должно быть синхронизировано с точностью до минуты.

Логика взаимодействия программных продуктов, используемых при работе с данными о событиях информационной безопасности ТТС ЭА, представлена на рисунке:



* 1. **Решения по реализации функциональности**
     1. Задания

В ТТС ЭА требуется создать сервис, обеспечивающий отправку данных о событиях информационной безопасности в SIEM - в порт 6514/TCP, UDP в формате протокола Syslog (RFC5424, RFC5426).

Syslog использует три концептуальных уровня:

* на уровне «содержимого» (content) находится управляющая информация, помещаемая в сообщения Syslog или извлекаемая из них;
* на уровне «приложений» (application) осуществляется создание, интерпретация, маршрутизация и сохранение сообщений Syslog;
* на уровне «транспорта» (transport) выполняется прием и передача сообщений Syslog по каналам связи.

Некоторые типы функций, исполняющихся на этих уровнях:

* «источник» (originator) генерирует содержимое, которое будет помещено в отправляемые сообщения Syslog;
* «коллектор» (collector) собирает содержимое сообщений Syslog для последующего анализа;
* «ретранслятор» (relay) пересылает сообщения Syslog, принимая их от источников или других ретрансляторов и направляя их коллекторам или другим ретрансляторам;
* «отправитель» (transport sender) посылает сообщения Syslog по указанному транспортному протоколу;
* «получатель» (transport receiver) получает сообщения Syslog по указанному транспортному протоколу.

При обмене сообщениями Syslog применяются следующие принципы:

* протокол Syslog не предусматривает механизма подтверждения доставки сообщений. Хотя некоторые транспортные протоколы могут предоставлять информацию о состоянии, концептуально Syslog является чисто симплексным коммуникационным протоколом;
* источники и ретрансляторы сообщений могут отправлять одно и то же сообщение нескольким коллекторам и ретрансляторам;
* функционально источник, ретранслятор и коллектор могут располагаться в одной и той же системе.

Администраторы должны протестировать сетевые пути между устройствами, ретрансляторами и коллекторами. Создаваемые сообщения Syslog не должны обрушивать ни одно из сетевых устройств.

Длина сообщения. Ограничения на размер сообщений Syslog диктуются используемым транспортным механизмом. Не существует верхнего предела как такового. Нижний предел находится на уровне 480 байт.

Для достижения наилучшей производительности и надежности, сообщения должны быть настолько короткими, насколько это возможно. Важная информация должна размещаться как можно ближе к началу сообщения, так как, в этом случае, менее вероятно, что она будет отброшена из-за ограничений транспортного механизма получателя.

Желательно использовать функции ограничения частоты отправки сообщений источниками и ретрансляторами. Это может уменьшить потенциальные проблемы заторов, когда случаются скачки количества передаваемых сообщений.

Сервис, обеспечивающий отправку данных о событиях информационной безопасности в SIEM, должен отправлять данные следующего содержания:

* дата и время события в формате ДД.ММ.ГГГГ ЧЧ:ММ:СС;
* компонент, на котором произошло событие;
* адрес источника события (узел или host);
* учетная запись аутентифицированного пользователя или внешней системы;
* служебные заголовки;
* тип события (согласно справочнику событий информационной безопасности);
* критичность события;
  + err (ошибка) – указывает на любую ошибку неисправность,
  + warn (предупреждение) – предупреждение о некоторой потенциальной проблеме,
  + info (информация) - информационное сообщение, сообщающее о некоем, несерьезном происшествии;
  + debug (отладка) - отладочная информация, которая может быть безболезненно игнорирована.
* идентификатор события;
* описание события (при необходимости расшифровки).

Сервис не должен отправлять:

* пароли в открытом виде или их хеши;
* персональные данные (ФИО в явном виде, дата рождения, место жительства и т.д.);
* токены аутентификации сессий.

Пример вывода сообщения о неверном пароле в формате RFC5424:

*Sep 3 15:25:49 box sshd[23076]: Failed password for invalid user root from 8.8.8.8 from 127.0.0.1 port 54460 ssh2*

* + 1. Подсистема администрирования

Роли «Администратор информационной безопасности» ТТС ЭА должен быть предоставлен доступ:

* к администрированию сервиса отправки данных о событиях информационной безопасности в ТТС ЭА;
* к SIEM.
  + 1. Документирование

В инструкцию администратора безопасности ТТС ЭА необходимо внести информацию:

* о сервисе, обеспечивающем отправку данных о событиях информационной безопасности в SIEM;
* об инструменте, применяемом для бэкапирования репозитория с данными о событиях информационной безопасности (SIEM), а также о сервере и каталоге, в котором создаются и хранятся бэкапы.

1. **Требования к контролю целостности и к обеспечению возможности восстановления программного обеспечения**

Должен быть сформирован перечень компонентов программного обеспечения, изменение/модификация которых не допустимы в процессе функционирования Системы.

Должна быть разработана инструкция по восстановлению программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций.

1. Требования к доработке инструкций и руководств

Должны быть разработаны или дополнены следующие инструкции и руководства:

1. руководство администратора по информационной безопасности ТТС ЭА (требования п.п. 11.1, 15.2.3);

* список файлов, устанавливаемых на контроль целостности;
* перечень регистрируемых типов событий безопасности средствами ППО ТТС ЭА;
* настройки SIEM в части подключения источника в формате RFC5424;

1. руководство администратора ППО ТТС ЭА (требования п.п. 11.1, 11.2, 12.1.3.2, 13.2.1, 14.2.1);

* перечень регистрируемых типов событий безопасности;
* список файлов, устанавливаемых на контроль целостности и их контрольные суммы;
* порядок восстановления ППО ТТС ЭА;
* описание работы с интерфейсом роли «Ответственный за исключение»;
* описание функционала просмотра и прекращения сессий пользователей в ППО ТТС ЭА и обеспечивающих общесистемных приложениях;

1. инструкция по восстановлению ППО ТТС ЭА (требования п.п. 16).