BASTION

ИНТЕГРИРОВАННАЯ СИСТЕМА БЕЗОПАСНОСТИ

Бастион - Персональные данные

Версия 1.7.4

ассоциация Электронные системы

Оглавление

1 Список принятых сокращений и обозначений

ПДн – персональные данные;

ИС – информационная система;

ИСПДн – информационная система персональных данных;

ПМВ – программно-математическое воздействие;

АПК – аппаратно-программный комплекс;

СКУД – система контроля и управления доступом.

2 Нормативное обеспечение

Под организацией обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных понимается формирование и реализация совокупности согласованных по цели, задачам, месту и времени организационных и технических мероприятий, направленных на минимизацию ущерба от возможной реализации угроз безопасности персональных данных.

Согласно Федеральному закону №152-ФЗ «О персональных данных» все информационные системы персональных данных (ИСПДн) должны быть приведены в соответствие с требованиями закона до 1.01.2010 года. Ответственность за исполнение мер по обеспечению безопасности ПДн законом возложена на операторов персональных данных.

Государственными регуляторами в указанной сфере являются:

- ФСТЭК РФ (техническая защита),
- ФСБ РФ (криптография),
- Россвязькомнадзор РФ (защита прав субъектов персональных данных).

К нормативному обеспечению необходимости защиты персональных данных можно отнести следующие документы:

1. Федеральный закон от 27 июля 2006 г. №152-ФЗ "О персональных данных". Принят Государственной Думой 8 июля 2006 года. Одобрен Советом Федерации 14 июля 2006 года
2. Постановление Правительства РФ от 17 ноября 2007 г. №781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных"
3. Приказ Федеральной службы по техническому и экспортному контролю, ФСБ РФ и Министерства информационных технологий и связи РФ от 13 февраля 2008 г. №55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных"

3 Классификация информационных систем персональных данных

3.1 Общие данные

При проведении классификации любой информационной системы персональных данных учитываются следующие исходные данные:

- категория обрабатываемых в информационной системе персональных данных - $X_{пд}$;
- объем обрабатываемых персональных данных (количество субъектов персональных данных, персональные данные которых обрабатываются в информационной системе) - $X_{нпд}$;
- заданные оператором характеристики безопасности персональных данных, обрабатываемых в информационной системе;
- структура информационной системы;
- наличие подключений информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена;
- режим обработки персональных данных;
- режим разграничения прав доступа пользователей информационной системы;
- местонахождение технических средств информационной системы.

3.2 Категории персональных данных

Определяются следующие категории обрабатываемых в информационной системе персональных данных $(X_{пд})$:

- категория 1 - персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;
- категория 2 - персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1;
- категория 3 - персональные данные, позволяющие идентифицировать субъекта персональных данных;
- категория 4 - обезличенные и (или) общедоступные персональные данные.

3.3 Объем обрабатываемых персональных данных

$X_{нпд}$ может принимать следующие значения:

- 1 - в информационной системе одновременно обрабатываются персональные данные более чем 100 000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах субъекта Российской Федерации или Российской Федерации в целом;
- 2 - в информационной системе одновременно обрабатываются персональные данные от 1000 до 100 000 субъектов персональных данных или персональные данные субъектов персональных данных, работающих в отрасли экономики Российской Федерации, в органе государственной власти, проживающих в пределах муниципального образования;

- 3 - в информационной системе одновременно обрабатываются данные менее чем 1000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах конкретной организации.

3.4 Дополнительные классифицирующие данные

По заданным оператором характеристикам безопасности персональных данных, обрабатываемых в информационной системе, информационные системы подразделяются на типовые и специальные информационные системы.

- Типовые информационные системы - информационные системы, в которых требуется обеспечение только конфиденциальности персональных данных.
- Специальные информационные системы - информационные системы, в которых вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).

По структуре информационные системы подразделяются:

- на автономные (не подключенные к иным информационным системам) комплексы технических и программных средств, предназначенные для обработки персональных данных (автоматизированные рабочие места);
- на комплексы автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи без использования технологии удаленного доступа (локальные информационные системы);
- на комплексы автоматизированных рабочих мест и (или) локальных информационных систем, объединенных в единую информационную систему средствами связи с использованием технологии удаленного доступа (распределенные информационные системы).

По наличию подключений к сетям связи общего пользования и (или) сетям международного информационного обмена информационные системы подразделяются на системы, имеющие подключения, и системы, не имеющие подключений.

По режиму обработки персональных данных в информационной системе информационные системы подразделяются на однопользовательские и многопользовательские.

По разграничению прав доступа пользователей информационные системы подразделяются на системы без разграничения прав доступа и системы с разграничением прав доступа.

Информационные системы в зависимости от местонахождения их технических средств подразделяются на системы, все технические средства которых находятся в пределах Российской Федерации, и системы, технические средства которых частично или целиком находятся за пределами Российской Федерации.

3.5 Классы информационных систем

В целях дифференцированного подхода к обеспечению безопасности персональных данных в зависимости от объема обрабатываемых персональных данных и угроз безопасности жизненно важным интересам личности, общества и государства ИСПДн подразделяются на следующие классы:

1. Класс 1 (К1) - ИСПДн, для которых нарушение заданной характеристики безопасности ПДн, обрабатываемых в них, может привести к *значительным негативным* последствиям для субъектов персональных данных;
2. Класс 2 (К2) - ИСПДн, для которых нарушение заданной характеристики безопасности ПДн, обрабатываемых в них, может привести к *негативным* последствиям для субъектов персональных данных;
3. Класс 3 (К3) - ИСПДн, для которых нарушение заданной характеристики безопасности ПДн, обрабатываемых в них, может привести к *незначительным негативным* последствиям для субъектов персональных данных;
4. Класс 4 (К4) - ИСПДн, для которых нарушение заданной характеристики безопасности ПДн, обрабатываемых в них, *не приводит к негативным* последствиям для субъектов персональных данных.

По результатам анализа исходных данных типовой информационной системе присваивается один из вышеуказанных классов в соответствии с таблицей:

Хпд \ Хнпд	3	2	1
категория 4	К4	К4	К4
категория 3	К3	К3	К2
категория 2	К3	К2	К1
категория 1	К1	К1	К1

4 Классификация ИС на основе АПК «Бастион» для работы с персональными данными

Отнесение ИС на основе АПК «Бастион» к тому или другому классу ИСПДн во многом зависит от способов использования АПК «Бастион». Далее будут рассмотрены параметры АПК «Бастион», позволяющие провести классификацию.

ИС на основе АПК «Бастион» можно отнести к Хпд = 2 (персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни) или Хпд = 3 (персональные данные, позволяющие просто идентифицировать субъекта персональных данных).

АПК «Бастион» позволяет, но не обязывает хранить и получать дополнительную информацию субъекта персональных данных (например, данные о транспортных средствах, материальных пропусках, паспортные данные, место жительства, фотографию).

По объему обрабатываемых данных ИС на основе АПК «Бастион» может быть отнесена как к 2-му (в информационной системе одновременно обрабатываются персональные данные от 1000 до 100 000 субъектов персональных данных или персональные данные субъектов персональных данных, работающих в отрасли экономики Российской Федерации, в органе государственной власти, проживающих в пределах муниципального образования), так и к 3-му классам (до 1000 субъектов), в зависимости от конкретного применения.

Бастион можно отнести к специальной информационной системе, в которой вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий). В случае АПК «Бастион» требуется защитить изменение уровня доступа и доступ сотрудников к функциям управления аппаратурой.

Бастион можно отнести к комплексу автоматизированных рабочих мест и (или) локальных информационных систем, объединенных в единую информационную систему средствами связи с использованием технологии удаленного доступа (распределенные информационные системы).

Бастион можно отнести к системе, не имеющей подключения к сетям связи общего пользования или международного информационного обмена.

Бастион относится к многопользовательской системе с разграничением прав доступа.

Таким образом, ИС на основе АПК «Бастион» могут быть отнесены к классам К2 и К3, в зависимости от объема и содержания информации, обрабатываемой оператором ПД.

5 Роль АПК «Бастион» в ИСПДн

АПК «Бастион» версии 1.7.4 может использоваться как компонент комплексной системы защиты персональных данных для ИСПДн классов К2 и К3. Для обеспечения соответствия всей системы, построенной на АПК «Бастион», требованиям Федерального закона №152-ФЗ «О персональных данных», должна быть создана соответствующая защищенная среда. На Рис. 1 наглядно представлена роль и функции АПК «Бастион» в общей системе защиты. Зеленым цветом обозначены требования, предъявляемые к системам класса К3, желтым – к системам класса К2.

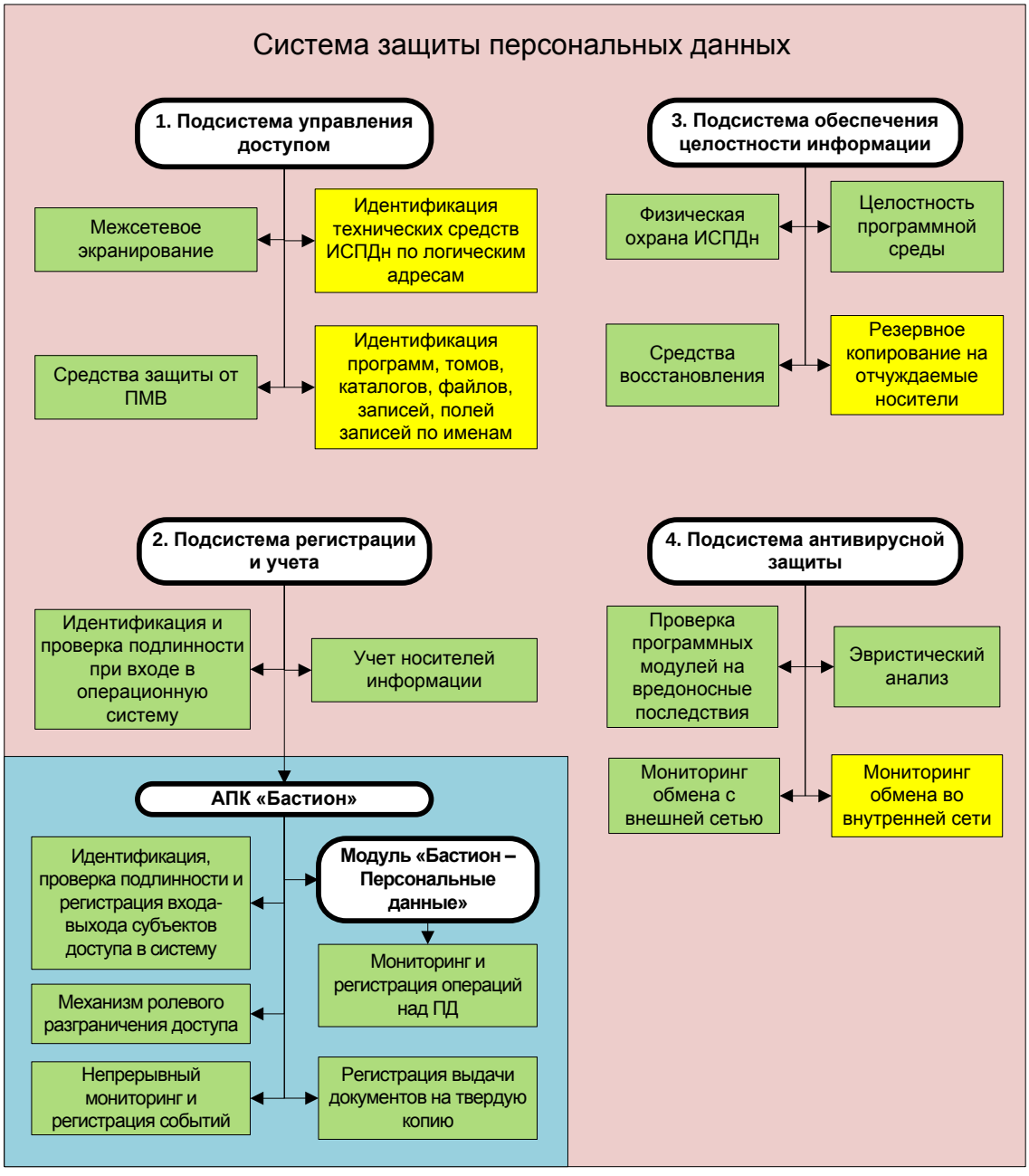


Рис. 1. Роль АПК "Бастион" в системе защиты персональных данных

Таким образом, для реализации полноценной защиты ПД должен быть проведен комплекс дополнительных мероприятий. Перечень этих мероприятий должен быть определен самим оператором ПД в соответствии с требованиями законодательства.

6 Цели и задачи модуля «Бастион – Персональные данные»

Модуль «Бастион - Персональные данные» предназначен для обеспечения возможности соответствия ИС на основе АПК «Бастион» Федеральному закону №152-ФЗ «О персональных данных» от 27 июля 2006 г**.**

Модуль реализует требования к ИСПДн классов К2 и К3 в части **протоколирования операций над персональными данными**.

Модуль реализует следующие задачи:

1. Протоколирование в полном объеме операций по доступу и модификации ПД. В терминологии АПК «Бастион» модуль выполняет протоколирование всех операций с персональными данными сотрудников, которым выданы карты доступа в СКУД (включая как модификацию, так и просмотр личных карт).
2. Просмотр, сохранение и печать отчетов по доступу и модификации ПД. В терминологии АПК «Бастион» модуль дает возможность построения и печати отчетов обо всех операциях, выполненных над персональными данными сотрудников (включая как модификацию, так и просмотр личных карт).
3. Печать формы информированного согласия на использование персональных данных. В терминологии АПК «Бастион» модуль дает возможность распечатать информированное согласие сотрудника об использовании своих персональных данных в СКУД.

7 Функции модуля «Бастион – Персональные данные»

7.1 Расширенное протоколирование операций

Основные операции с ПД (создание заявок на пропуска, выдача, возврат пропусков и пр.) протоколируются главным модулем Бюро пропусков АПК «Бастион» и для получения доступа к ним не требуется модуля «Бастион - Персональные данные». В версии 1.7.4 список основных протоколируемых операций был существенно расширен следующим набором событий:

1. Просмотр личной карты (закладки «Основные», «Пропуск», «Реквизиты», «Дополнительные параметры»).
2. Открытие/переключение между типами пропусков (постоянные, временные, разовые) и статусами пропусков (заявка, выдан, просрочен, в архиве).
3. Печать отчета по личной карте – либо пропуска, либо личной карты, либо списка сотрудников.
4. Просмотр истории личной карты и карты доступа.
5. Экспорт данных / импорт персональных данных.
6. Удаление карты доступа (безвозвратное, без переноса в архив).
7. Фотографирование с web-камеры.
8. Сканирование паспорта.

Тем не менее, даже этот, расширенный, набор событий не позволяет отследить конкретные изменения на уровне записей и полей таблиц. То есть, нельзя выяснить, когда и кем было сделано изменение конкретной записи, установить старое значение записи или посмотреть историю изменения полей в записи.

Для решения этих задач и предназначен модуль «Бастион – Персональные данные». Модуль позволяет формировать полный протокол всех изменений персональных данных в АПК «Бастион».

К фиксируемым изменениям относятся операции над персональными данными, выполненные:

1. С помощью простой правки полей свойств личной карты.
2. С помощью групповых операций над пропусками.
3. С помощью экспорта данных / импорта данных в форматы DBF и XML.
4. С помощью репликации данных между СКУД.

Расширенный протокол включается в общих настройках АПК «Бастион».

7.2 Просмотр истории карты доступа

Для просмотра этой истории лицензия на модуль «Бастион - Персональные данные» не требуется.

Чтобы просмотреть историю карты доступа, необходимо:

1. Открыть Бюро пропусков
2. Установить курсор на сотруднике, имеющем или имевшем раньше требуемую карту доступа.
3. Нажать на кнопку  на панели инструментов Бюро пропусков АПК «Бастион».

4. Переключиться на вторую закладку «История карты доступа».

На закладке будут отображаться события по всем личным картам, когда-либо использовавшим данную карту доступа, включая текущий выданный пропуск.

Доступна сортировка по имеющимся колонкам.

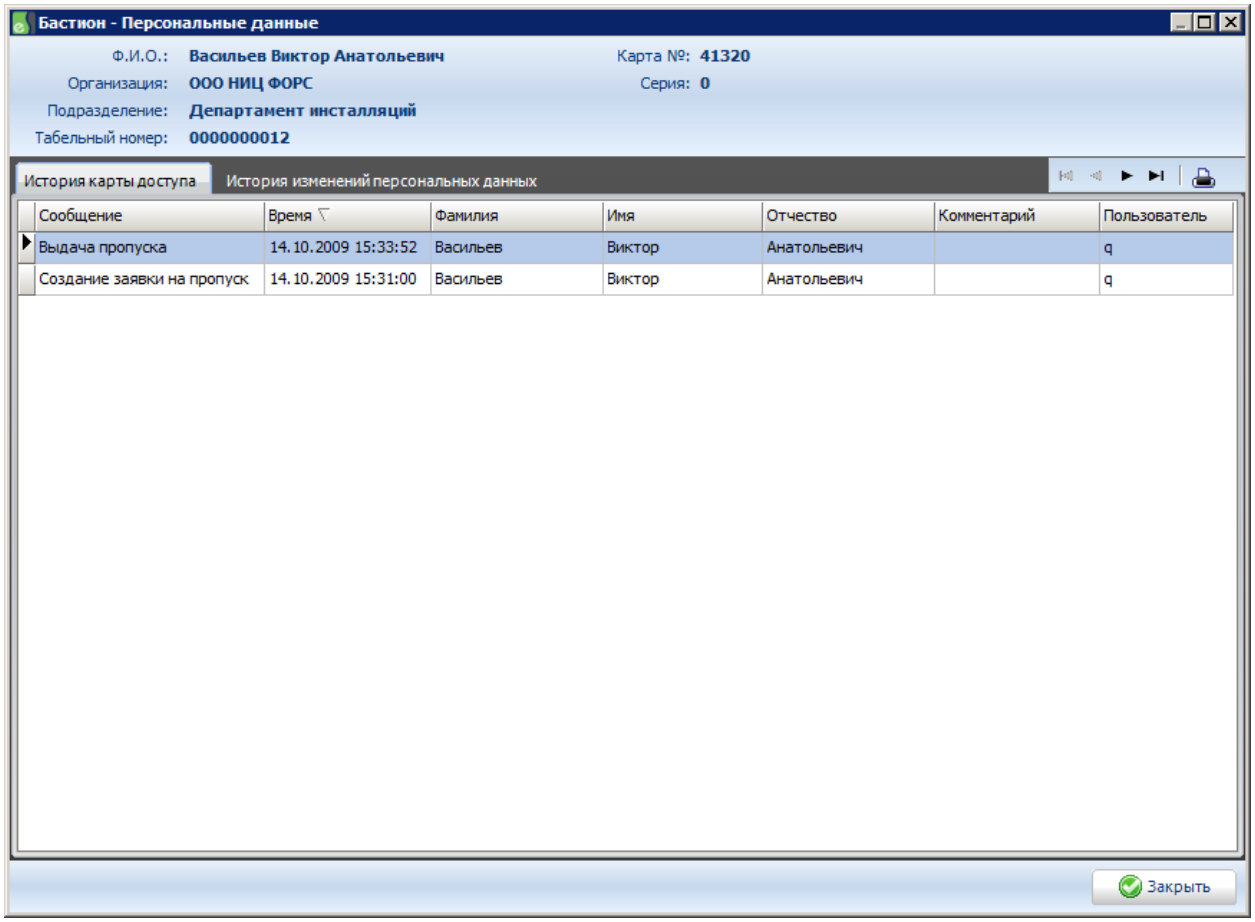


Рис. 2 - Пример просмотра истории карты доступа

7.3 Включение расширенного протокола персональных данных

Для того, чтобы включить расширенный протокол персональных данных для всех сотрудников в бюро пропусков, нужно:

1. Открыть «Общие настройки» в главном меню АПК «Бастион».
2. Перейти на вкладку «Лог изменения персональных данных».
3. Установить флажок в положение «Протоколировать изменения персональных данных».

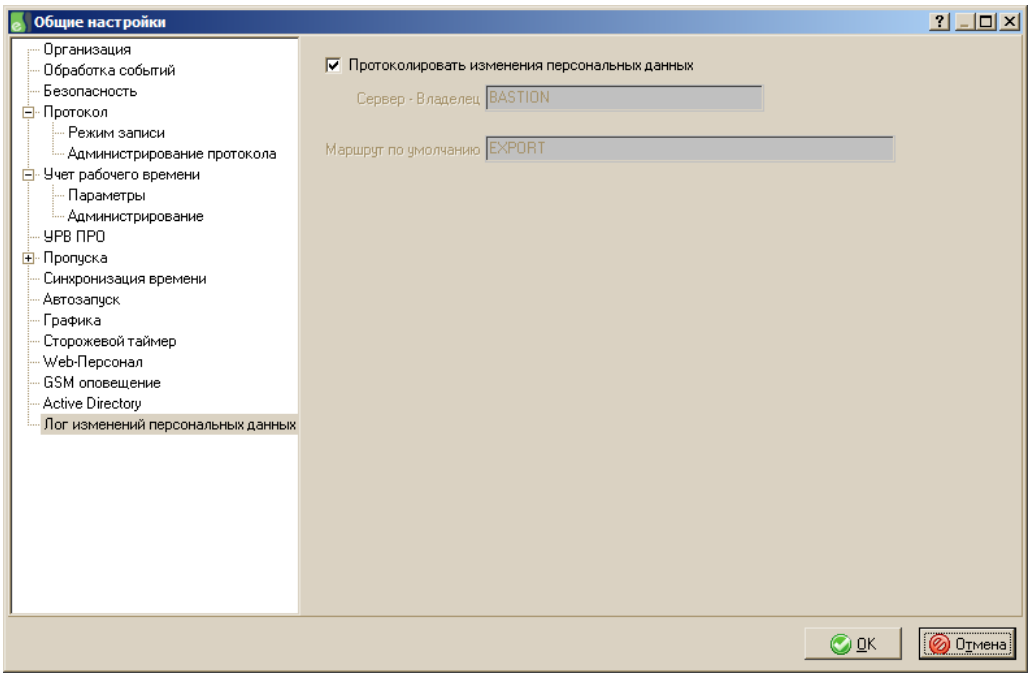


Рис. 3 - Включение расширенного протокола персональных данных

7.4 Просмотр расширенного протокола персональных данных

Для просмотра этого протокола необходимо наличие лицензии на модуль «Бастион-Персональные данные».

Чтобы просмотреть историю изменения персональных данных, необходимо:

1. Открыть Бюро пропусков;
2. Выбрать интересующего сотрудника;
3. Нажать на кнопку  на панели инструментов Бюро пропусков АПК «Бастион».
4. Переключиться на третью закладку «История изменения персональных данных».

На закладке будут отображаться события расширенного протокола.

События могут быть следующих типов:

- добавление записи;
- обновление записи;
- удаление записи.

В таблице отображаются события по следующим объектам Бюро пропусков (поле «Таблица»):

- Сотрудник;
- Пропуск;
- Карта доступа;
- Позиция словаря.

Доступны следующие операции:

- Сортировка по имеющимся колонкам;
- фильтр событий по датам;

- просмотр списка измененных оператором полей и новых значений;
- просмотр кодов интересующих записей;
- просмотр входящих событий на личную карту, если включена репликация между СКУД АПК «Бастион».

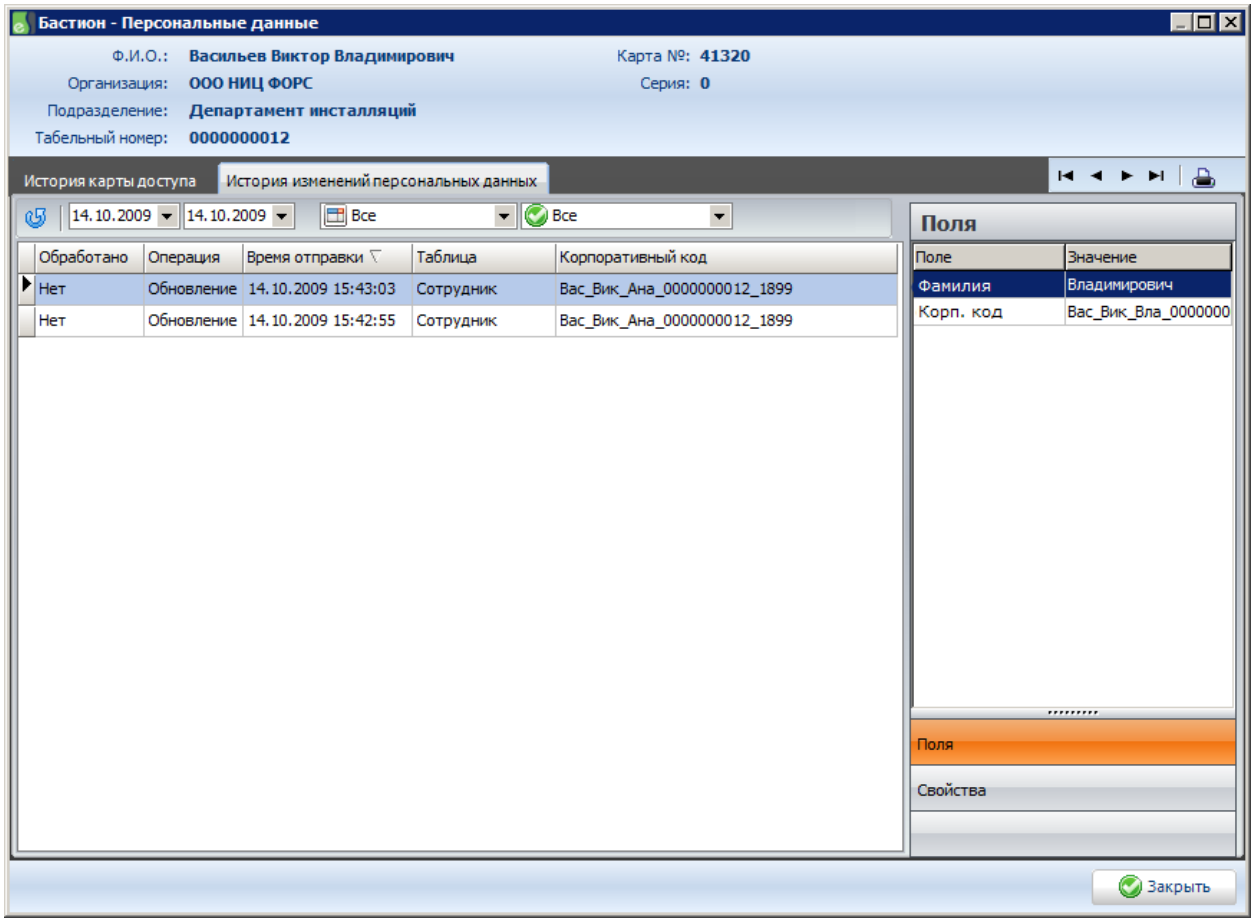


Рис. 4 - Пример просмотра расширенного протокола персональных данных

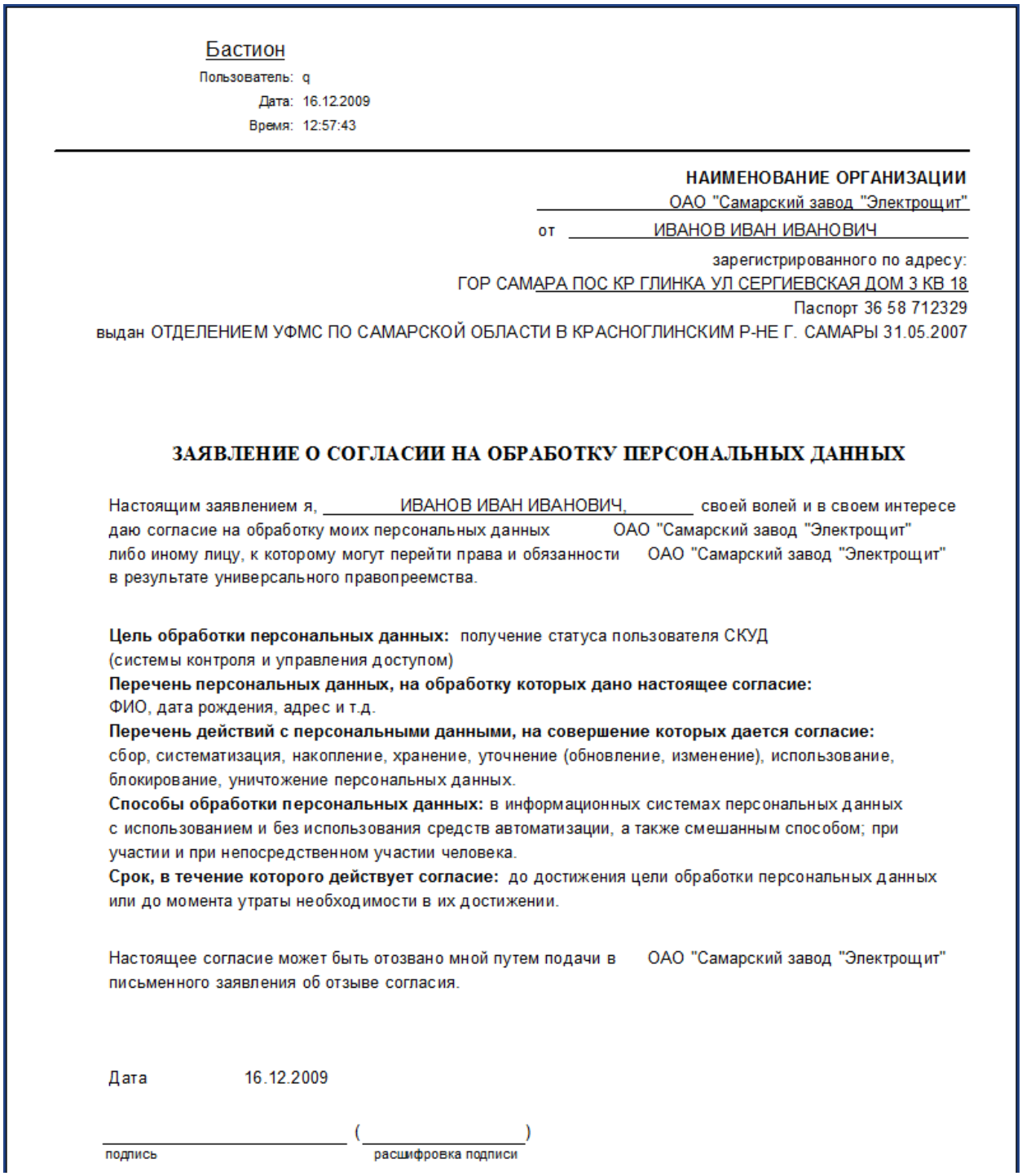
7.5 Информированное согласие

Чтобы распечатать информированное согласие пользователя СКУД необходимо:

1. Открыть Бюро пропусков;
2. Выбрать интересующего сотрудника;
3. Нажать на кнопку  на панели инструментов Бюро пропусков АПК «Бастион»;
4. Выбрать отчет с названием «Информированное согласие».

Отчет представляет собой бланк, представленный на Рис. 5.

Бюро пропусков выполнит подстановку фамилии, имени, отчества и даты рождения в бланк. После этого информированное согласие должно быть распечатано и подписано новым пользователем СКУД.



Бастион

Пользователь: q
Дата: 16.12.2009
Время: 12:57:43

НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ
ОАО "Самарский завод "Электрощит"
от ИВАНОВ ИВАН ИВАНОВИЧ
зарегистрированного по адресу:
ГОР САМАРА ПОС КР ГЛИНКА УЛ СЕРГИЕВСКАЯ ДОМ 3 КВ 18
Паспорт 36 58 712329
выдан ОТДЕЛЕНИЕМ УФМС ПО САМАРСКОЙ ОБЛАСТИ В КРАСНОГЛИНСКИМ Р-НЕ Г. САМАРЫ 31.05.2007

ЗАЯВЛЕНИЕ О СОГЛАСИИ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Настоящим заявлением я, ИВАНОВ ИВАН ИВАНОВИЧ, своей волей и в своем интересе даю согласие на обработку моих персональных данных ОАО "Самарский завод "Электрощит" либо иному лицу, к которому могут перейти права и обязанности ОАО "Самарский завод "Электрощит" в результате универсального правопреемства.

Цель обработки персональных данных: получение статуса пользователя СКУД (системы контроля и управления доступом)
Перечень персональных данных, на обработку которых дано настоящее согласие: ФИО, дата рождения, адрес и т.д.
Перечень действий с персональными данными, на совершение которых дается согласие: сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, блокирование, уничтожение персональных данных.
Способы обработки персональных данных: в информационных системах персональных данных с использованием и без использования средств автоматизации, а также смешанным способом; при участии и при непосредственном участии человека.
Срок, в течение которого действует согласие: до достижения цели обработки персональных данных или до момента утраты необходимости в их достижении.

Настоящее согласие может быть отозвано мной путем подачи в ОАО "Самарский завод "Электрощит" письменного заявления об отзыве согласия.

Дата 16.12.2009

_____ (_____)
подпись расшифровка подписи

Рис. 5. Форма информированного согласия на использование ПД

Бланк информированного согласия МОЖЕТ быть отредактирован как обыкновенный шаблон отчета Бюро пропусков. Сделать это можно в режиме дизайнера. Целесообразно заполнить шапку, логотип организации и ввести информацию о руководителе. Незаполненные поля заполняются от руки новым пользователем СКУД.