УТВЕРЖДАЮ:

Руководитель управления информационных технологий министерства здравоохранения Самарской области

_____ Бондаренко В.В.

«_____» _____ 2015 г.

УТВЕРЖДАЮ:

Генеральный директор
ООО «ИК «ХОСТ»

_____ Суслов К.Ю.

«_____» _____ 2015 г.

Самарская область
Государственная информационная система

Программное обеспечение

наименование программы

«Регистр медицинских справок»

Руководство пользователя

наименование документа

Обеспечение информационной безопасности

75746556.425730.002.И3.10.3

листов: 20

объем документа

СОГЛАСОВАНО:

Директор ГБУЗ «Самарский областной медицинский информационно-аналитический центр»

_____ Сорокин С.Г.

«_____» _____ 2015 г.

СОГЛАСОВАНО:

Менеджер проекта
ООО «ИК «ХОСТ»

_____ Колташева А.С.

«_____» _____ 2015 г.

Аннотация

Настоящий документ представляет собой руководство пользователя по обеспечению информационной безопасности программного обеспечения государственной информационной системы Самарской области «Регистр медицинских справок» (далее – *ПО*, *система, ПО «Регистр медицинских справок»*).

Документ является частью рабочей документации на ПО «Регистр медицинских справок».

Система является областным электронным регистром медицинских справок и предназначена для электронного подтверждения подлинности документа, удостоверяющего факт прохождения медицинского освидетельствования гражданином Российской Федерации, иностранным гражданином или лицом без гражданства, для проведения проверки достоверности представленных в нем сведений, контроля использования бланков строгой отчетности в МО, осуществления межведомственного электронного взаимодействия между МЗ СО и Управлением ГИБДД, между МЗ СО и УФМС.

Система является элементом комплексной информационной системы здравоохранения Самарской области как регионального фрагмента единой государственной информационной системы в сфере здравоохранения Российской Федерации.

Заказчик: Министерство здравоохранения Самарской области, г. Самара.

Исполнитель: Группа Компаний ХОСТ, ООО «ИК «ХОСТ», г. Екатеринбург.

Документ «Руководство пользователя по обеспечению информационной безопасности» предназначен для всех лиц, осуществляющих какую-либо деятельность с использованием ПО «Регистр медицинских справок».

Содержание

1 Введение

1.1 Список терминов и сокращений

Необходимые термины, сокращения и их определения отражены в таблице 1.

Таблица 1 – Список терминов и сокращений

Термин / Сокращение	Определение
Администратор	Специалист по обслуживанию компьютерной техники, сети и программного обеспечения (баз данных и информационных систем)
АРМ	Автоматизированное рабочее место
Аутентификация	Процедура проверки подлинности
ГИБДД	Управление Государственной инспекции безопасности дорожного движения Главного управления министерства внутренних дел Российской Федерации по Самарской области
ГИС РМС	Государственная информационная система Самарской области «Регистр медицинских справок»
ЛПУ	Лечебно-профилактическое учреждение
ОС	Операционная система
МЗ СО	Министерство здравоохранения Самарской области
МИАЦ	Государственное бюджетное учреждение здравоохранения «Самарский областной медицинский информационно-аналитический центр», находящийся по адресу: 443095, г. Самара, ул. Ташкентская, 159
ПО	Программное обеспечение государственной информационной системы Самарской области «Регистр медицинских справок»
Система	Государственная информационная система Самарской области «Регистр медицинских справок» – программно-аппаратный комплекс, предназначенный для автоматизации целенаправленной деятельности конечных пользователей, обеспечивающий (в соответствии с заложенной в него логикой обработки) возможность получения, модификации и хранения информации
СКЗИ	Средство криптографической защиты информации
СНИЛС	Страховой номер индивидуального лицевого счёта
Токен (Token)	USB-ключ, являющийся персональным средством аутентификации
УФМС	Управление Федеральной миграционной службы по Самарской области
ЭЦП	Электронно-цифровая подпись

1.2 Сведения о системе

Программное обеспечение «Регистр медицинских справок» государственной информационной системы Самарской области предназначено для автоматизации процессов прохождения медицинского освидетельствования гражданами Российской Федерации, иностранными гражданами или лицами без гражданства в медицинских организациях Самарской области.

ПО «Регистр медицинских справок» предназначено для достижения следующих целей:

1) электронное подтверждение подлинности документа, удостоверяющего факт прохождения медицинского освидетельствования гражданином Российской

Федерации, иностранным гражданином или лицом без гражданства и проведения проверки достоверности представленных в нем сведений;

2) контроль использования бланков строгой отчетности в медицинских организациях;
3) организация межведомственного электронного взаимодействия между министерством здравоохранения Самарской области и Управлением ГИБДД Главного управления Министерства внутренних дел Российской Федерации по Самарской области, между министерством и УФМС Российской Федерации по Самарской области.

1.3 Перечень эксплуатационной документации

Для общего понимания и соблюдения процедур информационной безопасности при работе с системой пользователю достаточно ознакомиться с настоящим документом перед началом работы.

1.4 Состав и содержание дистрибутивного носителя данных

Основная функциональность ПО «Регистр медицинских справок» представлена в виде web-интерфейса и не требует установки на локальный компьютер пользователя какого-либо программного обеспечения.

Для полнофункциональной работы ПО «Регистр медицинских справок» на персональном компьютере пользователя должно быть установлено и настроено специальное программное обеспечение – шифровальные (криптографические) средства, используемые для авторизации в системе и для создания ЭЦП сообщений.

Пользователь должен иметь USB-ключ, являющийся персональным средством аутентификации (токен), а также актуальный сертификат квалифицированной ЭЦП. Данный сертификат выдается авторизованным удостоверяющим центром и подтверждает принадлежность ЭЦП к конкретному пользователю, уполномоченному для работы в системе.

1.5 Порядок загрузки данных и программ, проверка работоспособности системы

Загрузка системы, выполненной по технологии «клиент-сервер», осуществляется автоматически через Интернет-браузер. Для начала информационного диалога достаточно указать адрес сайта системы (тестовый либо рабочий стенд) в строке адреса браузера, после чего ввести имя пользователя и соответствующий пароль. В случае работоспособности ПО на данном шаге будет открыта страница авторизации системы.

http://141.0.177.154:8080/ - Тестовый стенд (используется для обучения и проверки работоспособности версий).
http://141.0.177.154:6363/ — Рабочий стенд (в сети ТМС – **http://10.2.22.33:6363/**).

1.6 Порядок подключения к системе

Руководитель организации:

1) Обращается в:

а) **МЗ СО** (Управление лицензирования и контроля качества) с заявлением о наличии у медицинской организации лицензий на проведение медицинского освидетельствования заявителей и о подключении к ГИС РМС;

б) **МИАЦ** для организации обмена информацией между пользователями организации и МИАЦ. Обмен должен производиться в круглосуточном режиме с использованием ТМС или защищенных каналов связи с использованием криптографической защиты информации VipNet.

2) Проверяет актуальность сведений об организации в «Справочнике организаций сферы здравоохранения (LPU)». Если сведения об организации неактуальны или отсутствуют, заполняет анкету (форма анкеты приведена также на сайте МИАЦ по адресу: http://medlan.samara.ru/node/6141) и обращается в МИАЦ с заявлением об актуализации данных об организации.

3) Обращается в МИАЦ с заявлением о предоставлении доступа пользователей организации к ГИС РМС. К заявлению прилагаются:

а) сведения о должностном лице, ответственном в организации за использование системы (ФИО, контактные данные).

б) сведения о пользователях системы. Форма предоставления сведений приведена в разделе «Пользователи ГИС РМС».

МИАЦ, по предоставленным сведениям о пользователях при наличии положительных решений по ш. 1-3, осуществляет регистрацию организации и индивидуальную настройку ГИС РМС. По завершению работ информирует организацию о возможности использовать систему.

2 Общие положения

Настоящий документ разработан в соответствии с типовым документом «Положение о системе защиты информации в компьютерных и телекоммуникационных сетях» и определяет основные обязанности и ответственность пользователей ПО «Регистр медицинских справок».

Требования руководства являются обязательными для всех пользователей ПО «Регистр медицинских справок».

Цели обеспечения информационной безопасности:

- предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения пользователями, несанкционированного доступа к ней и получения защищаемой информации разведками, криминальными и коммерческими структурами;
- предотвращение несанкционированного уничтожения, искажения, копирования, блокирования информации в информационной системе;
- предотвращение утрат, уничтожения или сбоев функционирования носителей информации;
- соблюдение правового режима использования информационных ресурсов и системы, обеспечение полноты, целостности, достоверности информации в информационной системе;
- сохранение возможности управления процессом обработки и пользования информацией пользователями информационной системы.

Оперативный контроль за действиями пользователей при работе в ПО «Регистр медицинских справок», методическое руководство работой пользователей, организацию антивирусного контроля, установку СКЗИ, ПО и средств антивирусного контроля на АРМ и настройку сопутствующих параметров осуществляет Администратор системы, ответственный (уполномоченный) за обеспечение информационной безопасности.

3 Установка CryptoPro CSP

3.1 Установка драйверов Рутокен

Актуальная версия драйверов Рутокен доступна для загрузки по следующей ссылке: http://www.rutoken.ru/support/download/drivers-for-windows/

Важная информация:

- перед началом установки драйверов рекомендуется закрыть все работающие приложения;
- для установки драйверов необходимы права администратора системы.

Процедура установки:

1) Перед началом установки драйверов рекомендуется отсоединить идентификаторы Рутокен от USB-портов компьютера.
2) Запустите программу установки драйверов Рутокен и следуйте ее указаниям. На рисунках 1-2 показаны основные этапы работы мастера установки.
3) Во время установки драйверов может потребоваться перезагрузка компьютера (см. рисунок 3).
4) После перезагрузки компьютера установка будет продолжена автоматически (см. рисунок 4 и рисунок 5).
5) После окончания установки драйверов подсоедините идентификатор Рутокен (токен) к USB-порту.

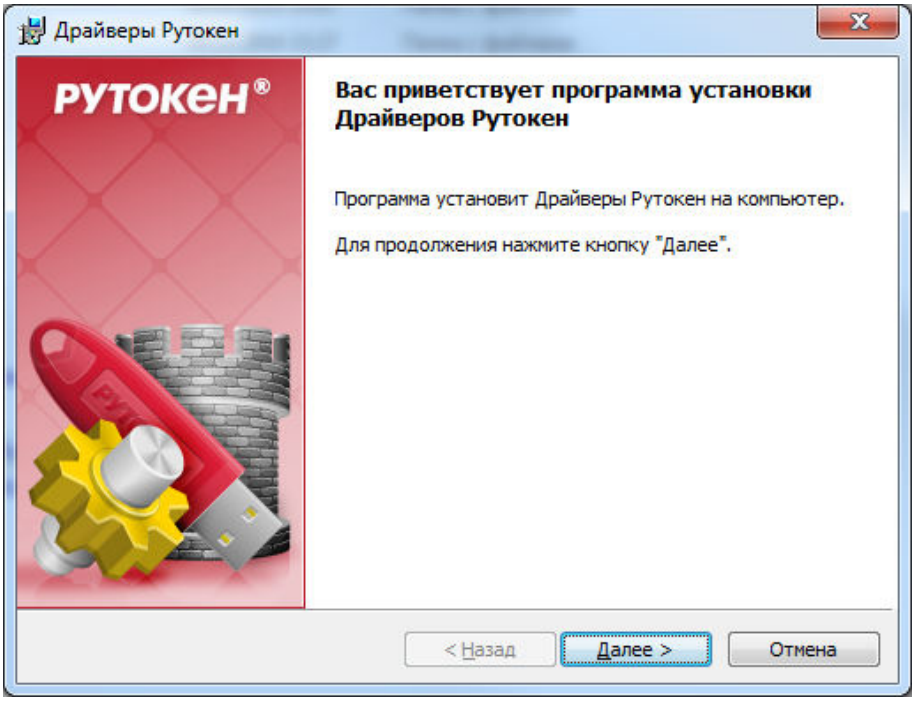

Рисунок 1 – Установка драйверов Рутокен. Инициализация

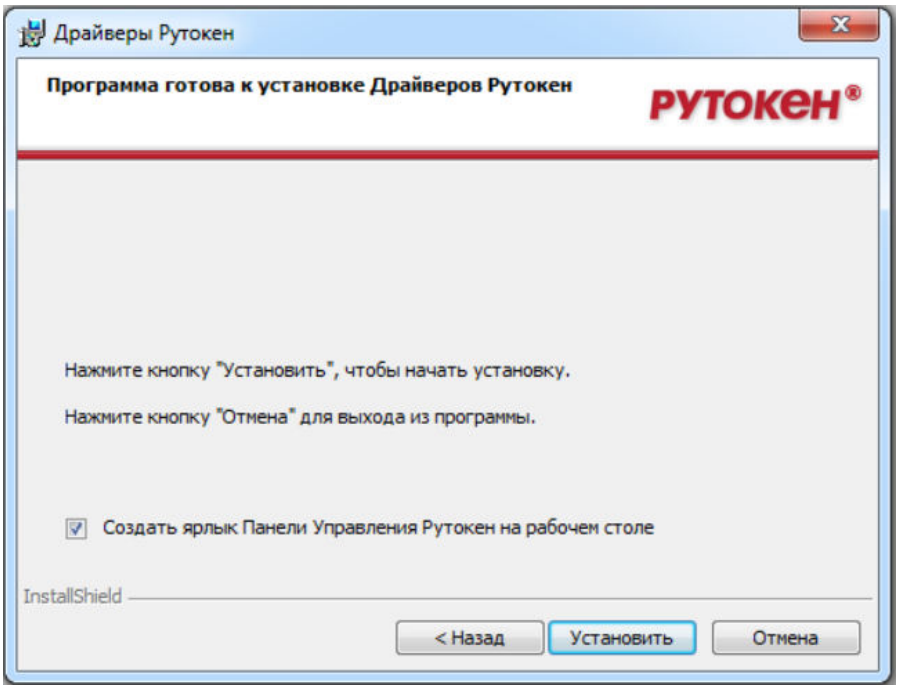

Рисунок 2 – Установка драйверов Рутокен. Продолжение

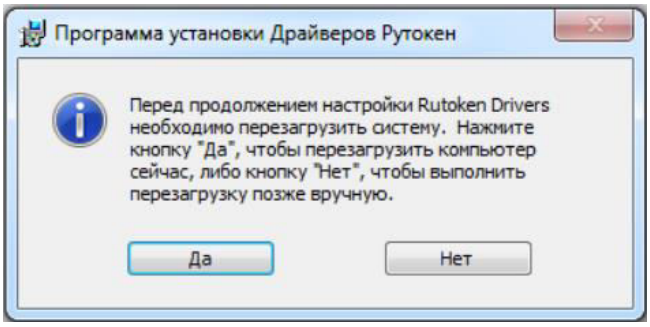

Рисунок 3 – Установка драйверов Рутокен. Перезагрузка

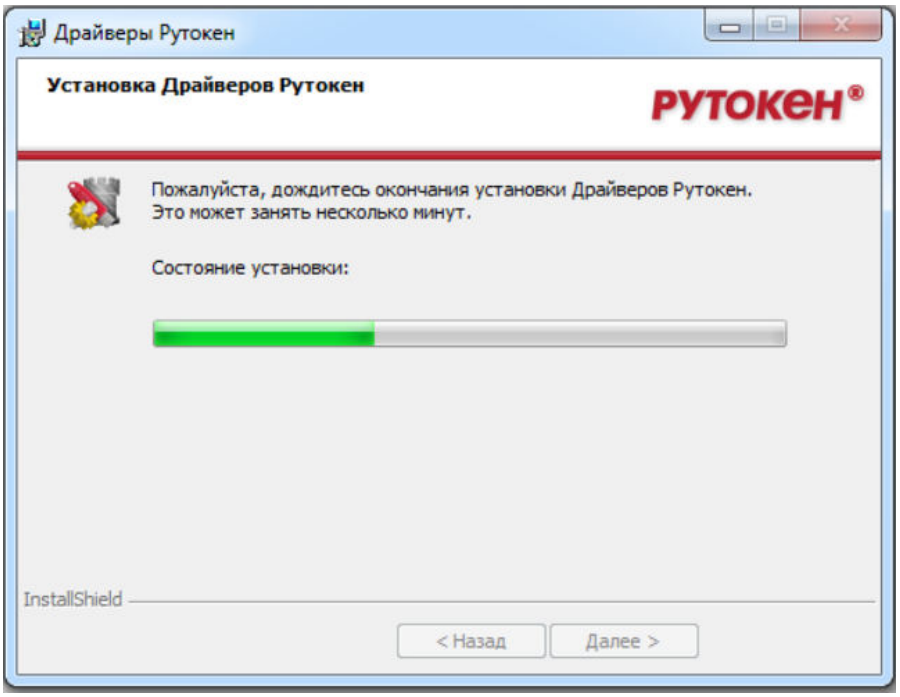

Рисунок 4 – Установка драйверов Рутокен. Инсталляция

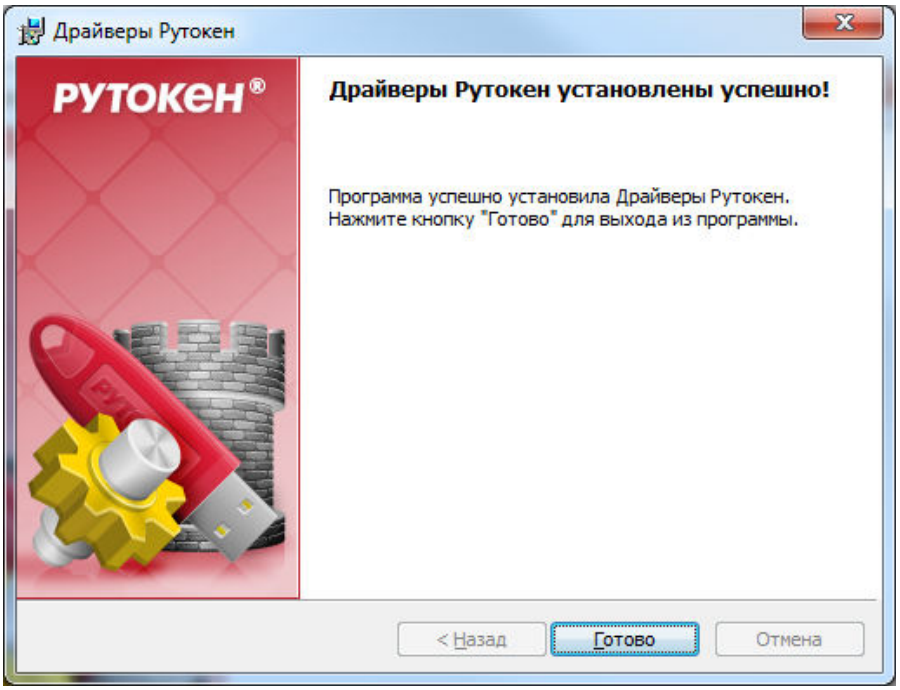

Рисунок 5 – Установка драйверов Рутокен. Окончание инсталляции

3.2 Установка КриптоПро CSP

Если на Вашем компьютере уже установлено КриптоПро CSP, то устанавливать его еще раз не требуется.

Процедура установки КриптоПро CSP:

1) Перейдите на диск с дистрибутивом КриптоПро CSP.
2) Запустите установку программы (файл `default_ru`). Откроется форма, представленная на рисунке 6.
3) Во всех последующих окнах нажмите на кнопку **Далее**.

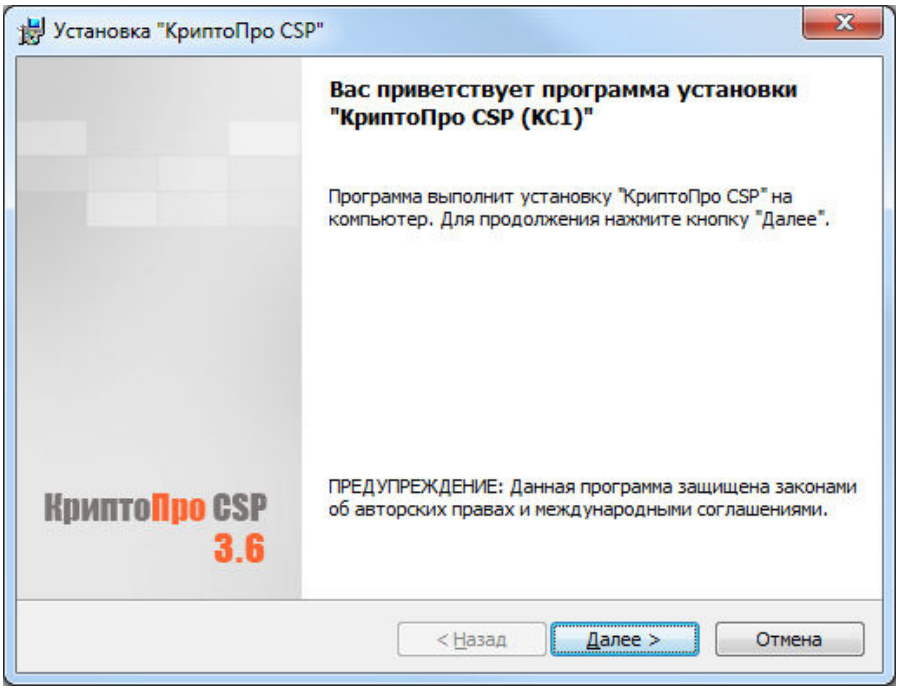

Рисунок 6 – Установка КриптоПро CSP. Инициализация

4) В окне **Безопасность Windows** (см. рисунок 7) выполните следующие действия:
   а) Поставьте галочку в поле «Всегда доверять программному обеспечению «Crypto-Pro».
   б) Нажмите на кнопку **Установить**.

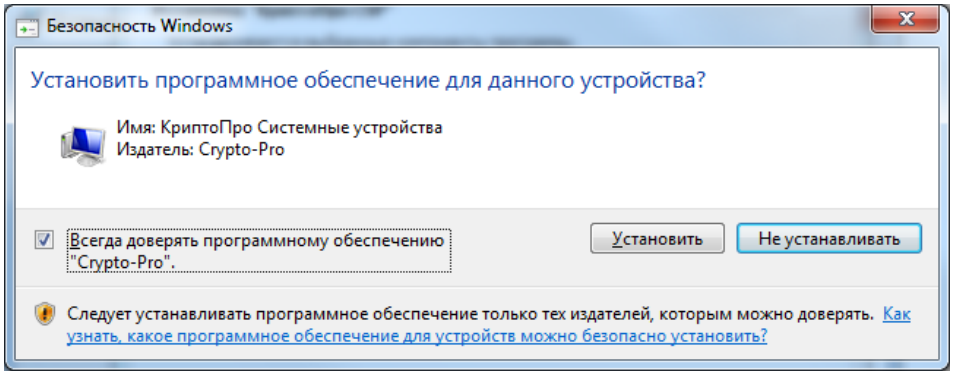

Рисунок 7 – Установка КриптоПро CSP. Безопасность Windows

5) После окончания установки (см. рисунок 8) нажмите на кнопку **Готово**.

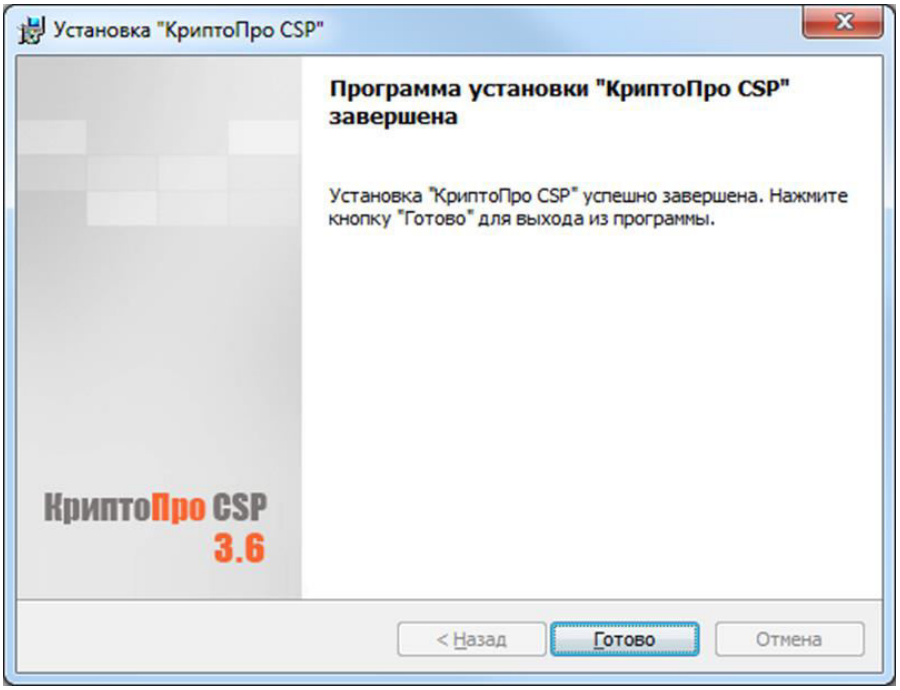

Рисунок 8 – Установка КриптоПро CSP. Безопасность Windows

6) После установки рекомендуется НЕ перезагружать компьютер при требовании ПО (см. рисунок 9), а дополнительно установить плагин для ЭЦП (см. п. 3.3).

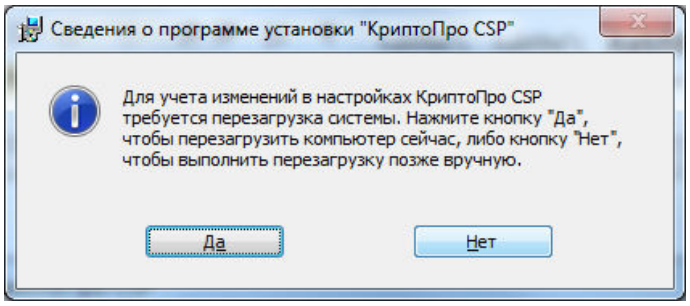

Рисунок 9 – Установка КриптоПро CSP. Перезагрузка

3.3 Установка и настройка плагина КриптоПро ЭЦП

Описание операций по установке и настройке плагина КриптоПро ЭЦП:

1) Перейдите на диск с дистрибутивом КриптоПро CSP.
2) Запустите установку плагина (файл `cadesplugin.exe`). Установка будет произведена автоматически.
3) В окне **КриптоПро ЭЦП Browser plag-in** нажмите на кнопку **ОК**.

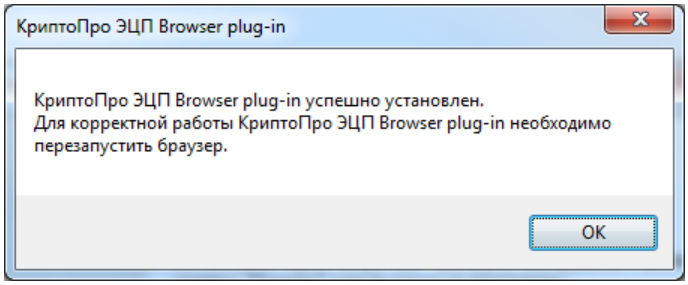

Рисунок 10 – Установка плагина КриптоПро ЭЦП

4) Чтобы перейти на страницу настроек плагина *КриптоПро* ЭЦП, выполните **Пуск —> КриптоПро —> Настройки ЭЦП Browser plag-in**. Соответствующий интерфейс страницы браузера представлен на рисунке 11.
5) Для работы *КриптоПро ЭЦП Browser plag-in* на каком-либо сайте добавьте его в доверенные узлы на странице настроек плагина (см. рисунок 12).

Примечание! Для ПО «Регистр медицинских справок » добавьте соответствующий адрес сервера и порт системы, например: **141.0.177.154:8080.**

6) После проведения всех настроек перезагрузите компьютер.

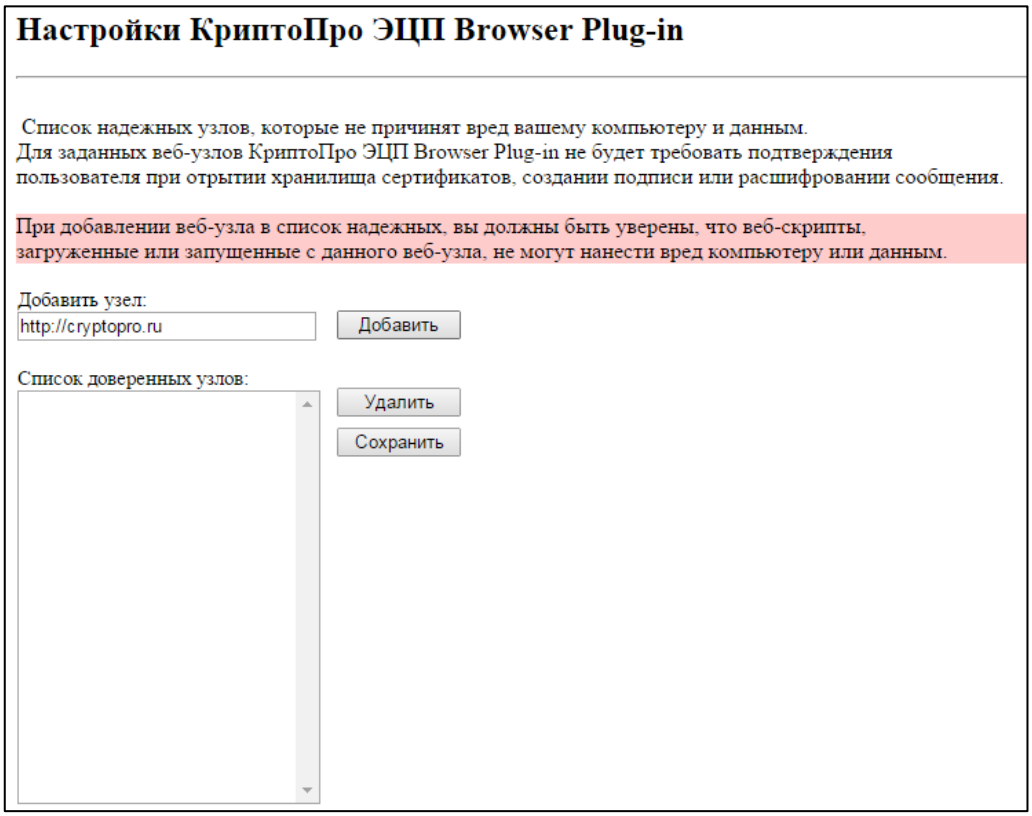

Рисунок 11 – Настройка плагина КриптоПро ЭЦП

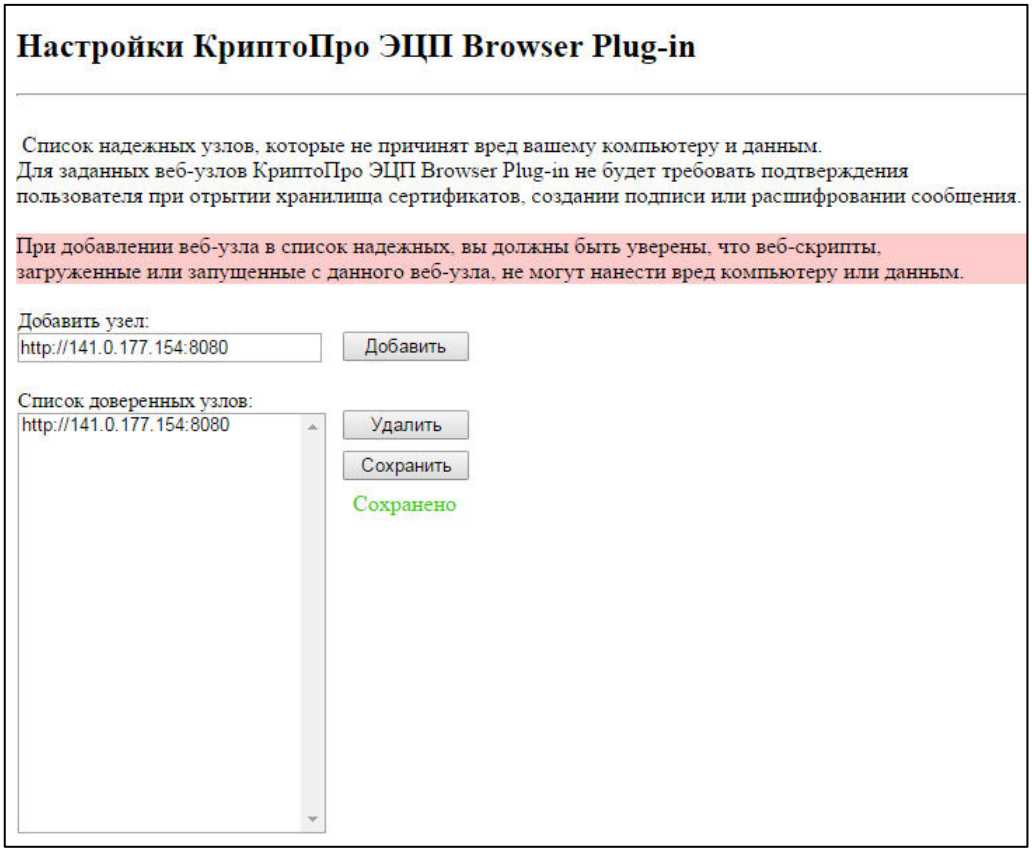

Рисунок 12 – Настройка плагина КриптоПро ЭЦП. Продолжение

4 Обеспечение информационной безопасности

Пользователю ПО «Регистр медицинских справок» устанавливаются соответствующие его полномочиям атрибуты управления доступом к информационным ресурсам.

Начальной процедурой управления регистрацией пользователей ПО «Регистр медицинских справок» в системе является процедура авторизации. Каждому пользователю Администратором по информационной безопасности назначаются персональный идентификатор (логин: *СНИЛС-код ЛПУ*) и соответствующий пароль.

В процессе эксплуатации ПО устройства отображения и вывода информации (дисплей, принтер) должны устанавливаться с учетом исключения несанкционированного доступа к выводимой информации лицами, не имеющими к ней соответствующего допуска. В случае невозможности выполнения указанных требований по размещению технических средств должны приниматься дополнительные организационные и технические меры по исключению несанкционированного доступа к информации. Изменение места расположения основных технических средств без согласования с Администратором по информационной безопасности запрещено.

В процессе эксплуатации ПО «Регистр медицинских справок» должно быть обеспечено непрерывное функционирование установленных средств защиты информации от несанкционированного доступа и антивирусного программного обеспечения; должны использоваться исключительно штатные технические средства.

Внесение пользователем самостоятельных изменений в аппаратно-программную конфигурацию ПО «Регистр медицинских справок» категорически запрещено.

Средства защиты, используемые в ПО «Регистр медицинских справок»:

- **СКЗИ «КриптоПро JSP»** – средство криптографической защиты информации, реализующее российские криптографические стандарты, разработанное в соответствии со спецификацией JCA;
- **USB-Токен** – компактное устройство, предназначенное для обеспечения информационной безопасности пользователя, также используется для идентификации его владельца, безопасного удаленного доступа к информационным ресурсам и т.д. Как правило, это физическое устройство, используемое для упрощения аутентификации.

Типовой порядок работы пользователя в ПО «Регистр медицинских справок» с точки зрения безопасности информации:

1) Перед началом обработки информации пользователь обязан убедиться в отсутствии в помещении посторонних лиц, а также в том, что средства защиты включены и работоспособны.
2) Осуществить вход в ПО «Регистр медицинских справок», используя личные идентификатор и пароль.
3) После окончания работы в ПО «Регистр медицинских справок» пользователю рекомендуется произвести полное выключение АРМ.

5 Права и обязанности пользователя

Пользователь ПО «Регистр медицинских справок» для обеспечения информационной безопасности при использовании в работе АРМ **ОБЯЗАН**:

1) Знать и соблюдать требования настоящего документа и других документов по информационной безопасности при работе с АРМ (в том числе требования организационно-технических и распорядительных документов *в области защиты персональных данных*), имеющим доступ к информационным ресурсам ПО «Регистр медицинских справок» и / или Интернет;
2) Знать и уметь использовать аппаратно-программное обеспечение, которое установлено на его АРМ, а также строго выполнять правила работы со средствами защиты информации, установленными на них;
3) Знать штатные режимы работы ПО «Регистр медицинских справок»;
4) Помнить личные пароли и идентификаторы либо хранить их в тайне;
5) Выполнять требования по антивирусному контролю:
   а) В процессе работы обязательному антивирусному контролю подлежит любая информация (текстовые и графические файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (USB-устройствам, CD-ROM и т.п.). Разархивирование и контроль входящей информации должны проводиться непосредственно после ее приема. Контроль исходящей информации должен проводиться непосредственно перед архивированием и отправкой (записью на съемный носитель).
   б) Устанавливаемое (изменяемое) на АРМ пользователя программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения на АРМ лицом, установившим (изменившим) программное обеспечение, в присутствии пользователя или Администратором по информационной безопасности рекомендовано выполнение антивирусной проверки.
   в) При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь самостоятельно или вместе с Администратором по информационной безопасности должен провести внеочередной антивирусный контроль своего АРМ.
   г) В случае обнаружения (при проведении антивирусной проверки) зараженных компьютерными вирусами файлов пользователь обязан:
      I) приостановить работу;
      II) немедленно поставить в известность о факте обнаружения зараженных вирусом файлов Администратора по информационной безопасности, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;
      III) провести лечение или уничтожение зараженных файлов.
6) Присутствовать при работах по внесению изменений в программно-аппаратную конфигурацию закрепленного за ним АРМ;

7) Немедленно вызывать Администратора по информационной безопасности при подозрении компрометации личных паролей или их утери, а также при обнаружении:
   а) Нарушений целостности пломб, наклеек на аппаратных средствах АРМ или иных фактов совершения попыток несанкционированного доступа к АРМ в отсутствие пользователя;
   б) Несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств АРМ;
   в) Отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов АРМ или периферийных устройств (дисководов, принтера и т.п.);
   г) Непредусмотренных формуляром АРМ отводов кабелей и подключенных устройств (при наличии соответствующего формуляра);
   д) Прочих фактов нарушения требований инструкций по обеспечению защиты информации.

Пользователю ПО «Регистр медицинских справок» **категорически ЗАПРЕЩАЕТСЯ**:

1) Использовать компоненты программного и аппаратного обеспечения АРМ в неслужебных целях.
2) Самовольно вносить какие-либо изменения в конфигурацию программно-аппаратных средств АРМ или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные формулярами на АРМ (при наличии).
3) Оставлять включенными без присмотра свое АРМ, не активировав средства защиты от несанкционированного доступа (временную блокировку экрана и клавиатуры), если таковые имеются.
4) Оставлять без личного присмотра на рабочем месте или где бы то ни было машинные носители и распечатки, содержащие конфиденциальную информацию.
5) Осуществлять обработку конфиденциальной информации в присутствии посторонних (не допущенных к данной информации) лиц.
6) Осуществлять обработку конфиденциальной информации при подключенном АРМ к сети Интернет при отсутствии установленного антивирусного ПО.
7) Записывать и хранить конфиденциальную информацию на неучтенных носителях информации.
8) Разглашать сведения о применяемых средствах защиты ПО «Регистр медицинских справок» и содержание документов лицам, не имеющим отношения к проводимым работам.
9) Использовать учтенные служебные машинные носители информации для хранения информации, не имеющей отношения к выполняемым работам.
10) Фиксировать на любых носителях персональный пароль или персональный идентификатор, передавать его сторонним лицам.
11) Проводить обработку информации в ПО «Регистр медицинских справок» при неработоспособных или отключенных средствах защиты информации.

12) Предпринимать попытки несанкционированного доступа к недоступным информационным ресурсам, осуществлять намеренное изменение, уничтожение, чтение, или передачу информации неавторизованным способом.
13) Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок требуется немедленно ставить в известность Администратора по информационной безопасности.
14) Разрабатывать и / или использовать программы, с помощью которых можно получить несанкционированный доступ к ПО «Регистр медицинских справок». Разработка и использование таких программ квалифицируется как попытка преднамеренного несанкционированного доступа к обрабатываемым данным.
15) Изменять или тиражировать ПО «Регистр медицинских справок».

Пользователь ПО «Регистр медицинских справок» **имеет ПРАВО**:

1) Использовать штатные программно-аппаратные средства ПО «Регистр медицинских справок» для решения профессиональных задач.
2) Давать Администратору по информационной безопасности предложения по совершенствованию мер информационной безопасности;
3) Обращаться к Администратору по информационной безопасности для оказания необходимой технической и методологической помощи в своей работе.

6 Ответственность пользователя

Пользователь ПО «Регистр медицинских справок» **несет персональную ОТВЕТСТВЕННОСТЬ** за обеспечение информационной безопасности.

Пользователь отвечает за соблюдение правил эксплуатации ПО «Регистр медицинских справок», сохранность информации, документов и электронных носителей информации, с которыми он работает.

Пользователь несет персональную ответственность за:

1) Соблюдение установленных требований по безопасности информации при обработке, копировании (уничтожении) персональных данных.
2) Использование неучтенных электронных носителей информации.
3) Несоблюдение правил использования электронных носителей информации, поступающих из сторонних организаций.
4) Правильность и полноту выполнения целей, задач, функций, прав и обязанностей, возложенных на него.
5) Сохранность сведений ограниченного распространения в соответствии с требованиями законодательства в области защиты персональных данных.
6) Выполнение указаний Администратора по информационной безопасности, касающихся защите информации при работе в ПО «Регистр медицинских справок».
7) Обеспечение сохранности и неразглашение сведений о парольной защите ПО «Регистр медицинских справок»;
8) Соблюдение технологии обработки защищаемой информации, неизменность условий обработки информации (размещение и / или состав технических средств обработки и защиты информации, состав используемого программного обеспечения) в соответствии с организационно-технической документацией на ПО «Регистр медицинских справок»;
9) Неисполнение или ненадлежащее исполнение обязанностей, предусмотренных настоящей инструкцией, в пределах, установленных законодательством Российской Федерации, а также за действия (бездействия), нарушающие права и законные интересы граждан и юридических лиц.

Выдержки из статей Уголовного кодекса РФ:

Статья 183. Незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну.

- Собирание сведений, составляющих коммерческую или банковскую тайну, путем похищения документов, подкупа или угроз, а равно иным незаконным способом в целях разглашения либо незаконного использования этих сведений – наказываются штрафов в размере от ста до двухсот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от одного до двух месяцев либо лишением свободы на срок до двух лет.
- Незаконное разглашение или использование сведений, составляющих коммерческую или банковскую тайну, без согласия их владельцев, совершенные из корыстной или иной личной заинтересованности и причинившие крупный ущерб, – наказывается штрафом в размере от двухсот до пятисот минимальных окладов оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев либо лишением свободы на срок до трех лет со штрафом в размере до пятидесяти минимальных размеров оплаты

труда или в размере заработной платы или иного дохода осужденного за период до одного месяца либо без такового.

Статья 272. Неправомерный доступ к компьютерной информации.

- Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, – наказываются штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.
- То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, – наказываются штрафом в размере от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от пяти до восьми месяцев, либо исправительным работам на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ.

- Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сетей, а равно использование либо распространение таких программ или машинных носителей с такими программами – наказываются лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.
- Те же деяния, повлекшие по неосторожности тяжкие последствия, – наказывается лишением свободы на срок от трех до семи лет.

Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

- Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, – наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.
- То же деяние, повлекшее по неосторожности тяжкие последствия, – наказывается лишением свободы на срок до четырех лет.

Статья 283. Разглашение государственной тайны.

- Разглашение сведений, составляющих государственную тайну, лицом, которому она была доверена или стала известна по службе или работе, если эти сведения стали достоянием других лиц, при отсутствии признаков государственной

измены – наказывается арестом на срок от четырех до шести месяцев либо лишением свободы на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

- То же деяние, повлекшее по неосторожности тяжкие последствия, – наказывается лишением свободы на срок от трех до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

Статья 284. Утрата документов, содержащих государственную тайну.

- Нарушение лицом, имеющим допуск к государственной тайне, установленных правил обращения с содержащими государственную тайну документами, а равно с предметами, сведения о которых составляют государственную тайну, если это повлекло по неосторожности их утрату и наступление тяжких последствий, – наказывается ограничением свободы на срок до трех лет, либо арестом на срок от четырех до шести месяцев, либо лишением свободы на срок до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

Статья 293. Халатность.

- Халатность, то есть неисполнение или ненадлежащее исполнение должностным лицом своих обязанностей вследствие недобросовестного или небрежного отношения к службе, если это повлекло существенное нарушение прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства, – наказывается штрафом в размере от ста до двухсот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от одного до двух месяцев, либо обязательными работами на срок от ста двадцати до ста восьмидесяти часов, либо исправительными работами на срок от шести месяцев до одного года, либо арестом на срок до трех месяцев.