

# Безопасность DoПортала

Где хранятся данные, кто что видит, что фиксируется и как проверить это самостоятельно. Простым языком, без технических терминов там, где без них можно обойтись.

|                             |                             |                                              |                  |              |
|-----------------------------|-----------------------------|----------------------------------------------|------------------|--------------|
| РАЗРАБ.<br>Газутдинов Д.    | ИСПОЛНИТЕЛЬ<br>dioniday.dev | <b>DoПортал</b><br>Описание мер безопасности | СТАДИЯ<br>П      | ЛИСТОВ<br>11 |
| для<br>проектных институтов |                             |                                              | DOPORTAL-ИБ-2026 |              |

01

## Коротко

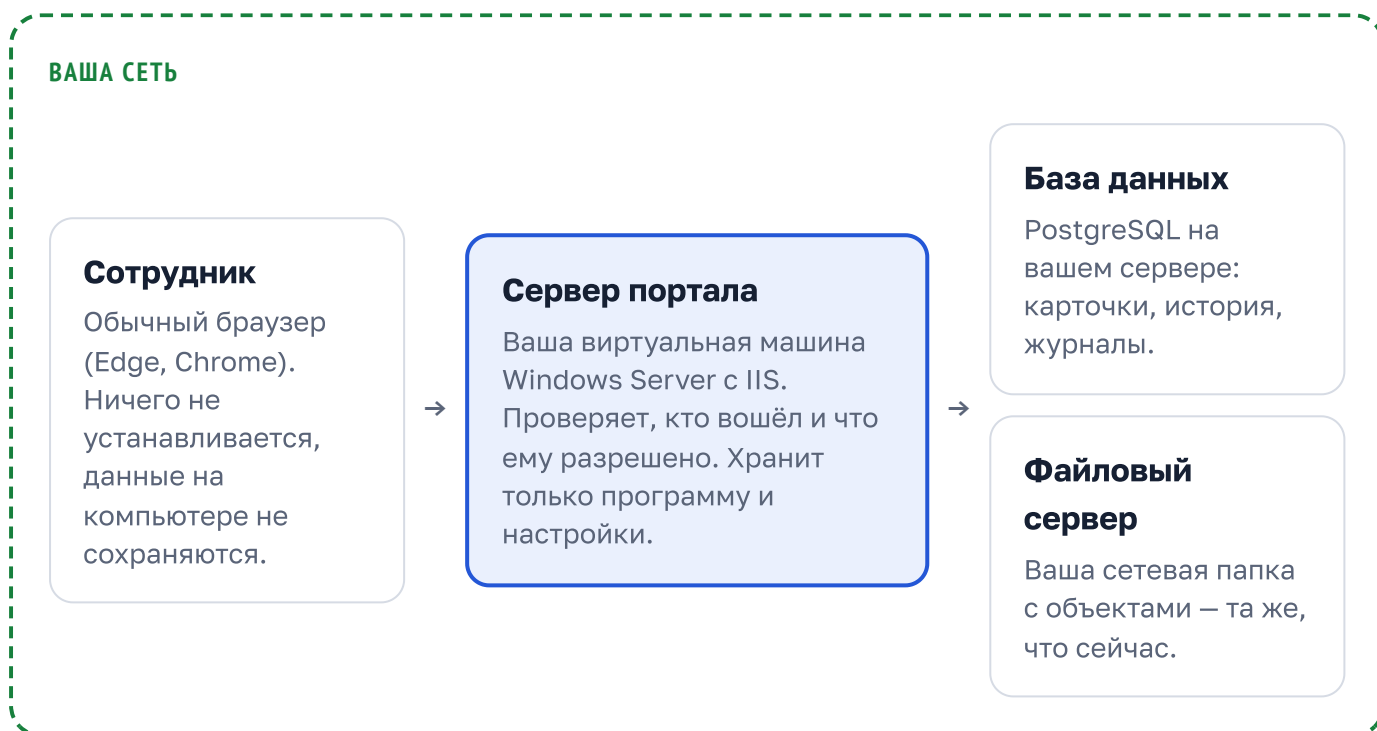
Портал – это ещё одна программа на вашем сервере. Данные не уходят за пределы вашей сети, войти можно только под доменной учётной записью, а права проверяются при каждом обращении.

|                                                                   |                                                                        |                                                                       |                                                                     |
|-------------------------------------------------------------------|------------------------------------------------------------------------|-----------------------------------------------------------------------|---------------------------------------------------------------------|
| <b>0</b><br>обращений в интернет: портал работает в закрытой сети | <b>0</b><br>собственных паролей: вход через Windows (Active Directory) | <b>100%</b><br>действий с файлами и карточками фиксируются в журналах | <b>0 ₺</b><br>доплаты за исправление замечаний независимой проверки |
|-------------------------------------------------------------------|------------------------------------------------------------------------|-----------------------------------------------------------------------|---------------------------------------------------------------------|

Мы не просим верить на слово. В разделе 7 описано, как ваш администратор может проверить каждое утверждение за полчаса, а в разделе 8 – как заказать независимую проверку.

## Где живут данные

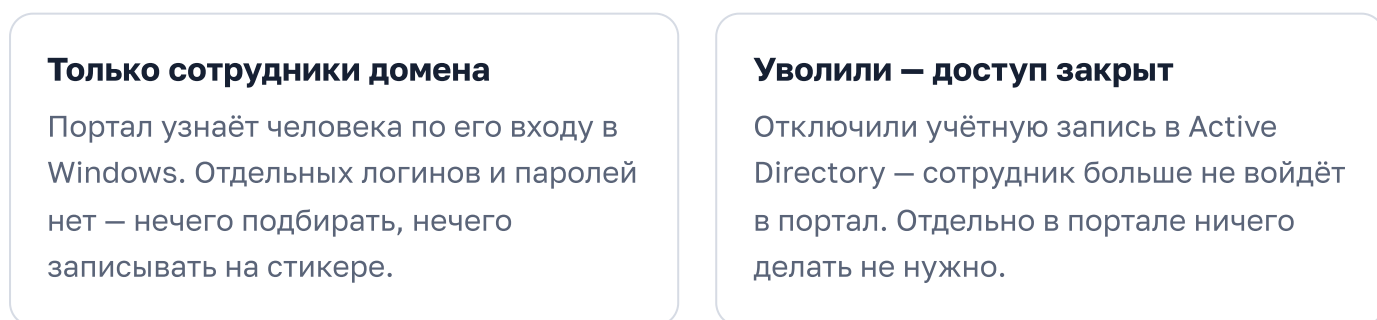
Все три части портала устанавливаются на ваши серверы. Ни одна из них не требует доступа в интернет.



- ✗ Нет облачных сервисов
- ✗ Нет «звонков домой» и телеметрии
- ✗ Нет шрифтов и скриптов из интернета

Разработчик не имеет доступа к вашим данным. Подключение для сопровождения — только по вашей заявке, через ваш VPN и под учётной записью, которую выдаёт и отключает ваш администратор (раздел 9).

## Кто может войти



### **Чужой компьютер в сети не войдёт**

Устройство без доменной учётной записи получает отказ на первой же странице.

### **Новичок получает минимум**

Сотрудник домена при первом входе получает роль «Сотрудник» своего отдела. Роли «ГИП» и «Начальник отдела» подбираются по должности из AD. Права администратора портал сам не выдаёт никому — только вручную.

### **Доступ можно закрыть отдельно**

Администратор может закрыть сотруднику вход в портал, не трогая его учётную запись в домене: например, подрядчику или на время служебной проверки. Действие попадает в журнал.

### **Роли — по группам AD**

Роли можно назначать через группы Active Directory: ваш администратор управляет доступом привычными средствами.

## Кто что видит

Принцип: каждый видит только то, что нужно ему для работы. Права проверяет сервер при каждом обращении — недостаточно знать ссылку на чужой документ, чтобы его открыть.

| РОЛЬ                               | ВИДИТ                                                                      | ФАЙЛЫ ОБЪЕКТОВ<br>(ЧЕРТЕЖИ,<br>ДОКУМЕНТАЦИЯ)            |
|------------------------------------|----------------------------------------------------------------------------|---------------------------------------------------------|
| <b>Сотрудник</b>                   | Объекты, задания и письма своего отдела                                    | Только объектов, в которых участвует его отдел          |
| <b>Начальник отдела</b>            | То же, плюс сводка «Мой отдел»                                             | Только объектов своего отдела                           |
| <b>ГИП</b>                         | Свои объекты целиком, задания и письма по ним                              | Своих объектов                                          |
| <b>Нормоконтролёр, выпускающий</b> | Комплекты, переданные им на проверку и выпуск                              | Только объектов из своей очереди                        |
| <b>Делопроизводитель</b>           | Всю входящую корреспонденцию, перечень объектов                            | Нет доступа к чертежам — не нужны для работы с письмами |
| <b>Офис-менеджер</b>               | Удостоверения по охране труда, входящую корреспонденцию, перечень объектов | Нет доступа к чертежам                                  |
| <b>Администратор</b>               | Всё, включая настройки                                                     | Все — его действия попадают в отдельный журнал          |

Матрицу прав можно ужесточить под ваши правила: что разрешено каждой роли, настраивается на странице «Права доступа».

## Что фиксируется

Записи журналов только добавляются. В интерфейсе портала нет функции их правки или удаления — ни у кого, включая администратора.

### История карточек

Кто и когда зарегистрировал письмо, передал его в отдел, сменил статус объекта, выдал задание или замечание, согласовал.

### Журнал файлов

Кто просмотрел, скачал или открыл каждый файл объекта, с датой и временем. Последние действия видны прямо на странице объекта.

### Журнал администрирования

Изменения прав, ролей, справочников и настроек — отдельно от рабочих действий.

Пример вопроса, на который теперь есть ответ: «Кто скачивал чертежи по объекту за последний месяц?» При работе только через сетевую папку ответить на него обычно невозможно, а портал хранит каждое такое действие.

## Защита от типовых угроз

| ЧТО МОЖЕТ СЛУЧИТЬСЯ                                                 | ЧТО СДЕЛАНО В ПОРТАЛЕ                                                                                                                                                            |
|---------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Подбор или кража пароля к portalу                                   | Паролей портала нет — вход только через Windows. Действует ваша политика паролей домена.                                                                                         |
| Сотрудник открывает чужой объект, подставив номер в адресную строку | Сервер сверяет права при каждом открытии карточки, файла и вложения. Без прав — «Нет доступа».                                                                                   |
| Кто-то из сотрудников заводит себе отдельную учётную запись         | Регистрация отключена. Страницы входа по паролю, оставшиеся от стандартного шаблона, удалены из доступа.                                                                         |
| В папку объекта подложили вредоносный файл                          | Портал не запускает программы: открываются только чертежи и документы Office. Изображения показываются в «песочнице», файлы SVG, где может прятаться скрипт, только скачиваются. |
| Подмена страницы, внедрение чужого кода                             | Браузеру запрещено загружать что-либо, кроме файлов самого портала, и показывать портал внутри чужих сайтов.                                                                     |
| Взлом через поля ввода (SQL-инъекции)                               | Все обращения к базе формируются стандартной библиотекой с параметрами, а не склейкой текста.                                                                                    |
| Пароль к базе данных в файле настроек                               | Пароли к базе и сетевой папке хранятся зашифрованными ключом конкретного сервера. Скопированный на другой компьютер файл настроек бесполезен.                                    |
| Перехват данных в сети                                              | Портал работает по HTTPS с сертификатом вашего домена (настраивается при установке).                                                                                             |

**Ошибка при обучении или проверке обновления**

Тестовый режим: отдельная база и отдельное хранилище, рабочие данные не затрагиваются.

## Самопроверка перед предложением

Перед подготовкой предложения код портала был проверен на типовые уязвимости веб-приложений. Найденное исправлено:

- ✓ **Отключены страницы регистрации и входа по паролю**  
Остались от стандартного шаблона Microsoft и позволяли завести учётную запись в обход домена.
- ✓ **Добавлены защитные заголовки**  
Политика безопасности содержимого (CSP), запрет встраивания в чужие сайты, запрет «угадывания» типа файла браузером.
- ✓ **Убрана загрузка шрифта из интернета**  
Портал не делает ни одного внешнего запроса.
- ✓ **Файлы из папок объектов показываются безопасно**  
SVG не открывается в браузере, изображения и текст — в «песочнице».
- ✓ **Сужены права на файлы**  
Делопроизводитель и офис-менеджер больше не видят чертежи всех объектов.
- ✓ **Ограничен запуск файлов на сервере**  
Только чертежи и документы Office, никаких программ.
- ✓ **Добавлена блокировка сотрудника в портале**  
Доступ закрывается одним флажком, даже если учётная запись в домене действует.

07

## Как проверить самим

Эти проверки ваш системный администратор выполнит на опытной установке без помощи разработчика.

- **Чужой компьютер не войдёт**  
Откройте портал с ноутбука, не включённого в домен. Ожидается отказ во входе.
- **Чужой объект не откроется**  
Войдите сотрудником отдела, не участвующего в объекте, и вставьте ссылку на этот объект или его файл. Ожидается «Нет доступа».

- ☐ **Регистрации нет**  
Откройте адрес портала с окончанием **/Account/Register**. Ожидается «Страница не найдена».
- ☐ **Портал не ходит в интернет**  
Запретите серверу портала выход в интернет на межсетевом экране. Работа портала не изменится.
- ☐ **Журнал всё помнит**  
Скачайте файл объекта и обновите страницу объекта. В списке «кто работал с файлами» ожидается запись с вашим именем и временем.
- ☐ **Заблокированный не войдёт**  
Закройте тестовому сотруднику доступ в конфигураторе («Пользователи и роли»). Ожидается отказ во входе, а в журнале администрирования — запись о блокировке.
- ☐ **Пароли не лежат открыто**  
Откройте файл настроек на сервере. Пароли к базе и сетевой папке — в зашифрованном виде.

## Чего нет — честно

Ни одна программа не бывает «полностью безопасной», и обещать это было бы неправдой. Вот чего у портала нет и как это закрывается.

- **Сертификата ФСТЭК**  
Для внутренней системы документооборота проектного института сертификация, как правило, не требуется. Если ваша организация относится к субъектам КИИ или у вас есть требования головной структуры — это нужно оценить до внедрения. Мы предоставим описание системы для такой оценки.
- **Собственного резервного копирования**  
Резервные копии делаются вашими средствами — так же, как для остальных серверов. Копировать нужно две вещи: базу данных PostgreSQL и папку данных портала (вложения и шаблоны). Чертежи и так лежат на файловом сервере, который вы уже копируете.
- **Собственного антивируса**  
Файлы объектов лежат на вашем файловом сервере и проверяются вашим антивирусом, как и сейчас.
- **Внешнего аудита (пока)**  
Портал проверен разработчиком, но не сторонней организацией. Это предлагаем исправить — ниже.

### ПРЕДЛОЖЕНИЕ

#### Независимая проверка — исправления без доплаты

- Проверяющего выбираете и приглашаете вы: компанию по информационной безопасности или специалиста, которому доверяете. Проверку оплачивает заказчик.
- Для проверки предоставляются опытная установка и документация.
- Все найденные замечания исполнитель исправляет **без доплаты** в срок, согласованный в договоре. Критичные — до перевода портала в промышленную эксплуатацию.
- Отчёт проверяющего и перечень исправлений остаются у вас.

### Рекомендации для вашего администратора при установке

- Выпустить для портала сертификат HTTPS вашего домена.
- Запускать портал под отдельной служебной учётной записью с доступом только к папке объектов.
- Завести для портала отдельного пользователя PostgreSQL с правами только на его базу. Закрывать порт базы данных для всех, кроме сервера портала.

- Включить портал в ежедневное резервное копирование: база данных и папка данных портала.
- Устанавливать обновления Windows и .NET в обычном порядке.

09

## Сопровождение и гарантии

Безопасность — это не только программа, но и то, что будет с ней через год.

**Всё закреплено в договоре**

Сроки реакции, состав работ по сопровождению и порядок передачи дел при его завершении фиксируются в договоре, а не в устных обещаниях.

**Доступ только по заявке**

Удалённое подключение — через ваш VPN, под учётной записью, которую вы выдаёте на время работ и отключаете после. Все подключения видны в ваших журналах.

**Передача знаний**

Ваш ИТ-специалист получает руководство администратора, участвует в установке и проходит обучение: перезапуск, обновление, резервное копирование, восстановление, диагностика.

**Обновления безопасности**

Уязвимости в используемых компонентах (.NET, PostgreSQL, библиотеки) отслеживаются, обновления выпускаются в рамках сопровождения. Каждое обновление сначала проверяется в тестовом режиме.

| ОБРАЩЕНИЕ | ПРИМЕР                                       | РЕАКЦИЯ     | РЕШЕНИЕ         |
|-----------|----------------------------------------------|-------------|-----------------|
| Критичное | Портал недоступен; найдена уязвимость        | 2 ч         | 1 раб. день     |
| Важное    | Не работает одна функция, есть обходной путь | 1 раб. день | 5 раб. дней     |
| Обычное   | Вопрос, консультация, мелкая доработка       | 2 раб. дня  | по согласованию |

Время — в рабочие часы заказчика. Сроки в таблице — типовые; конкретные условия сопровождения закрепляются в договоре.

