

# НЕЙРОСС АТМ

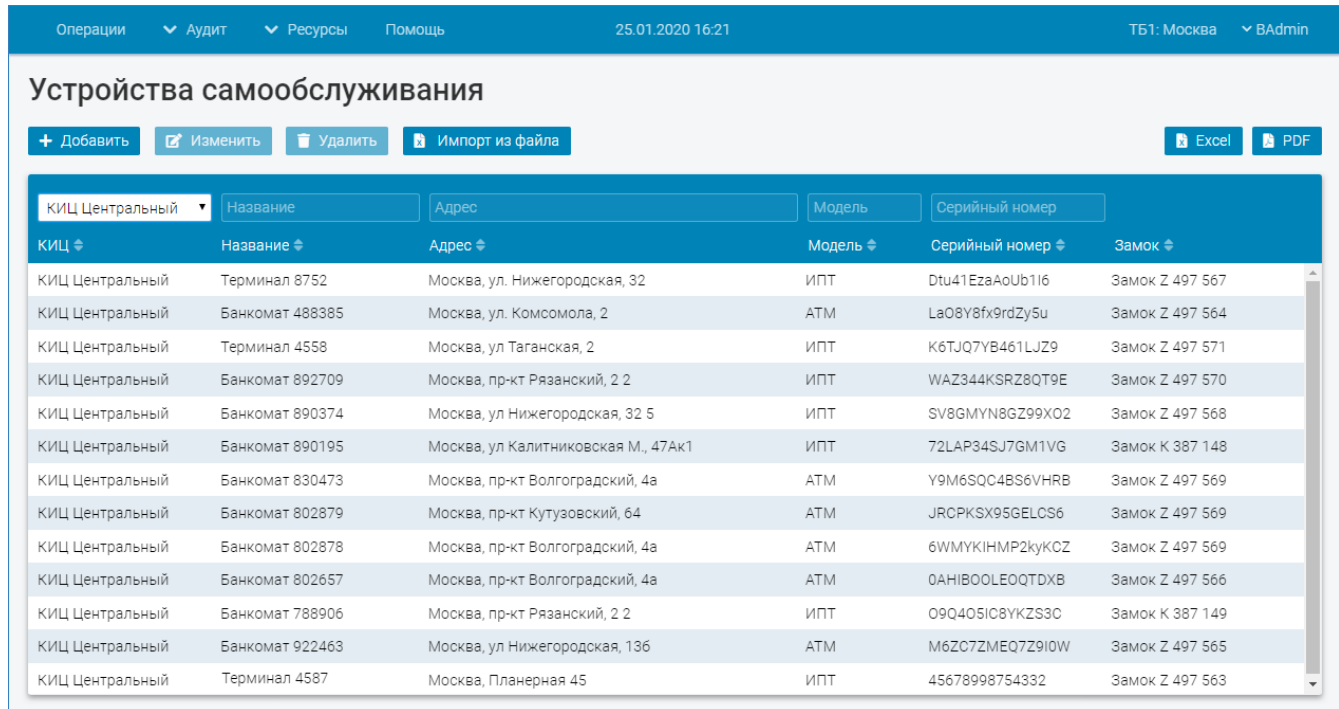
[Общие сведения](#) · [Ключевые особенности](#) · [Системные требования](#)

[Руководство системного администратора](#) · [Руководство пользователя](#)

## Общие сведения

Программный комплекс НЕЙРОСС АТМ (АТМ – Автоматизированный Территориально-распределенный Менеджер) предназначен для построения системы управления электромагнитными замками устройств самообслуживания; обеспечивает оперативный и защищенный доступ сотрудников банка к устройствам самообслуживания (УС) для инкассации и выполнения технологических операций.

Принцип работы системы заключается в генерации *одноразовых временных кодов* (ОВК) доступа к замкам УС, действующих в ограниченный период времени и предназначенных для однократного использования на определенном замке сотрудником, предъявившим авторизованный электронный ключ и пин-код. Таким образом обеспечивается многофакторная защита от несанкционированных действий как со стороны сотрудников банка, так и со стороны сторонних лиц.



The screenshot shows the 'Устройства самообслуживания' (Self-service devices) management interface. At the top, there are navigation tabs: 'Операции', 'Аудит', 'Ресурсы', and 'Помощь'. The current date and time are '25.01.2020 16:21', and the user is logged in as 'ТБ1: Москва' with 'BAdmin' permissions. Below the navigation is a title bar 'Устройства самообслуживания' and a toolbar with buttons: '+ Добавить', 'Изменить', 'Удалить', 'Импорт из файла', 'Excel', and 'PDF'. A search and filter section includes a dropdown for 'КИЦ Центральный' and input fields for 'Название', 'Адрес', 'Модель', and 'Серийный номер'. The main content is a table with columns: 'КИЦ', 'Название', 'Адрес', 'Модель', 'Серийный номер', and 'Замок'. The table contains 15 rows of device data.

КИЦ	Название	Адрес	Модель	Серийный номер	Замок
КИЦ Центральный	Терминал 8752	Москва, ул. Нижегородская, 32	ИПТ	Dtu41EzaAoUb1I6	Замок Z 497 567
КИЦ Центральный	Банкомат 488385	Москва, ул. Комсомола, 2	АТМ	La08Y8fx9rdZy5u	Замок Z 497 564
КИЦ Центральный	Терминал 4558	Москва, ул. Таганская, 2	ИПТ	K6TJQ7YB461LJZ9	Замок Z 497 571
КИЦ Центральный	Банкомат 892709	Москва, пр-кт Рязанский, 2 2	ИПТ	WAZ344KSRZ8QT9E	Замок Z 497 570
КИЦ Центральный	Банкомат 890374	Москва, ул. Нижегородская, 32 5	ИПТ	SV8GMYN8GZ99X02	Замок Z 497 568
КИЦ Центральный	Банкомат 890195	Москва, ул. Калитниковская М., 47Ак1	ИПТ	72LAP34SJ7GM1VG	Замок K 387 148
КИЦ Центральный	Банкомат 830473	Москва, пр-кт Волгоградский, 4а	АТМ	Y9M6SQ04BS6VHRB	Замок Z 497 569
КИЦ Центральный	Банкомат 802879	Москва, пр-кт Кутузовский, 64	АТМ	JRCPKSX95GELCS6	Замок Z 497 569
КИЦ Центральный	Банкомат 802878	Москва, пр-кт Волгоградский, 4а	АТМ	6WMYKINMP2кукCZ	Замок Z 497 569
КИЦ Центральный	Банкомат 802657	Москва, пр-кт Волгоградский, 4а	АТМ	0AHIB00LE0QTDXB	Замок Z 497 566
КИЦ Центральный	Банкомат 788906	Москва, пр-кт Рязанский, 2 2	ИПТ	O9Q4O5IC8YKZS3C	Замок K 387 149
КИЦ Центральный	Банкомат 922463	Москва, ул. Нижегородская, 136	АТМ	M6Z07ZMEQ7Z9I0W	Замок Z 497 565
КИЦ Центральный	Терминал 4587	Москва, Планерная 45	ИПТ	45678998754332	Замок Z 497 563

## Ключевые особенности

### Надёжная защита материальных ценностей

При генерации кода учитываются такие параметры, как уникальный идентификатор замка, идентификатор ключа сотрудника, пин-код сотрудника, тип операции, дата и время действия операции. Соответственно, выданный код можно успешно использовать только на соответствующем замке, с предъявлением конкретного ключа, конкретного пин-кода и только в заданное время. В зависимости от типа операции будет выполнено соответствующее действие — будет открыт замок или будет выполнена сервисная операция.

Кроме того, выданный код можно использовать только один раз — замок хранит информацию об использованных кодах и не позволяет использовать один и тот же код дважды.

Замки работают полностью автономно, без канала связи с программным комплексом — таким образом, замки защищены от дистанционного несанкционированного доступа и могут работать в условиях отсутствия подключения к сетям передачи данных.

Наконец, информация обо всех выполненных с замком операциях сохраняется в памяти замка. Этот журнал аудита можно вычитать из замка в рамках соответствующей сервисной операции, изучить и сохранить средствами программного комплекса НЕЙРОСС АТМ.

### Программные средства как сервис

Программный комплекс НЕЙРОСС АТМ разворачивается в защищённой IT-инфраструктуре центрального банка. Системные администраторы (СА) в структуре центрального банка выполняют установку, настройку, обслуживание программного комплекса, а также регистрацию и управление виртуальными сегментами (подпространствами данных) территориальных банков. Пользователи территориальных банков получают доступ только к сегменту своего территориального банка дистанционно, через веб-интерфейс программного комплекса, по защищенным каналам в сети Интернет или внутренней локальной сети банка.

Архитектура решения такова, что системные администраторы не имеют доступа к прикладным данным территориальных банков (сведениям о пользователях, ключах, замках, устройствах самообслуживания и др.), а пользователь территориального банка имеет доступ только к прикладным данным своего сегмента. Управление пользователями всех территориальных банков осуществляет межрегиональный администратор.

## **Забота о кибербезопасности**

Особое внимание в НЕЙРОСС АТМ уделено защите информации от несанкционированного доступа и кибербезопасности:

1. Компрометация какой-либо отдельной части системы (сетевого узла) не позволяет получить возможность генерации кодов доступа.
2. Значимые (критичные) данные, используемые при генерации кодов, такие как идентификаторы замков или пин-коды инкассаторов шифруются при внесении / генерации и впоследствии хранятся и передаются между составными частями комплекса только в зашифрованном виде и никогда не отображаются пользователю в открытом виде.
3. Шифрование / дешифрование значимых (критичных) данных осуществляется только на выделенном спецустройстве с применением аппаратного криптографического токена (без наличия закрытого ключа в оперативной памяти вычислительной машины).
4. Такие данные, как пароли учётных записей и коды операций надёжно хешируются, хранятся в базе данных только в захешированном виде и никогда не отображаются пользователю в открытом виде.
5. Все сетевые каналы коммуникации между составными частями программного комплекса защищены сквозным двусторонним шифрованием.
6. Механизм аутентификации использует криптостойкие токены с ограниченным временем действия.
7. Попытки подбора паролей в целях несанкционированного доступа автоматически обнаруживаются и блокируются.
8. Все события, изменения данных, запросы пользователей и пр. регистрируются в журнале аудита, который в свою очередь защищён от компрометации с применением механизмов цифровой подписи и блокчейна.