НЕЙРОСС ATM

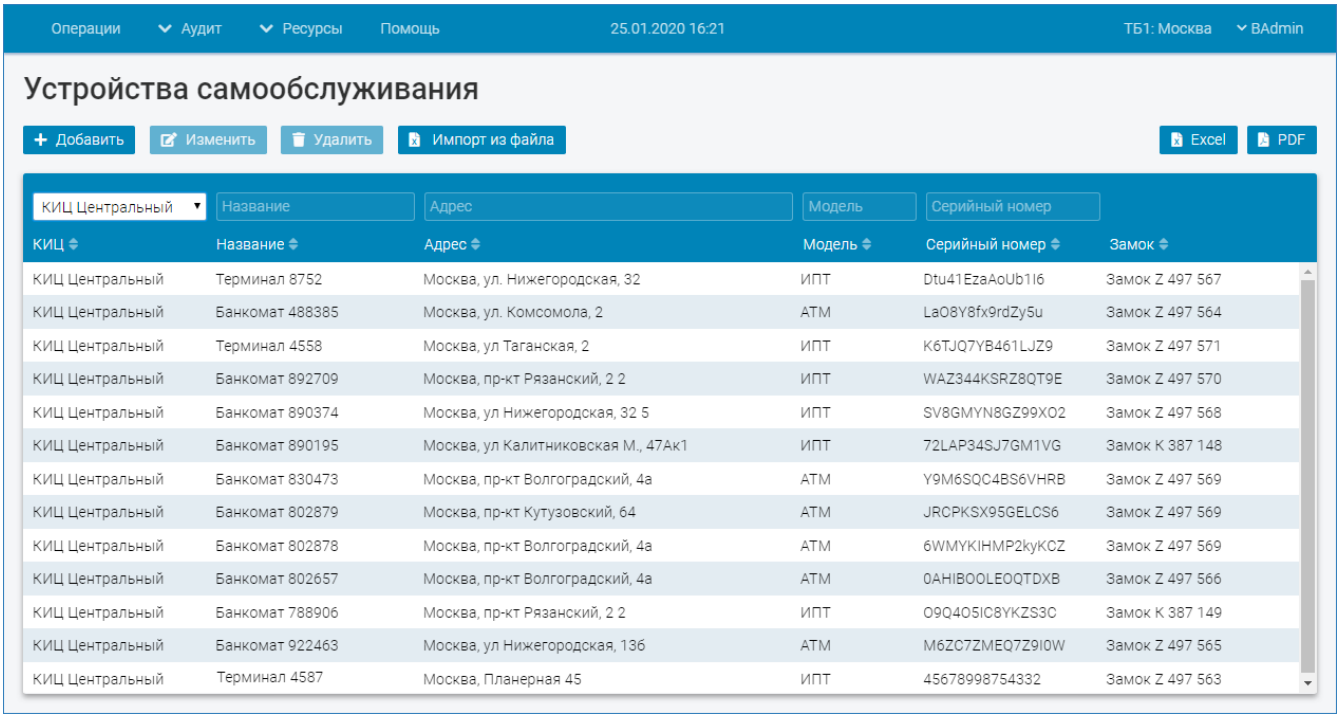
Общие сведения · Ключевые особенности · Системные требования

Руководство системного администратора · Руководство пользователя

Общие сведения

Программный комплекс НЕЙРОСС ATM (ATM – 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.



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 ATM.

Программные средства как сервис

Программный комплекс НЕЙРОСС ATM 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.