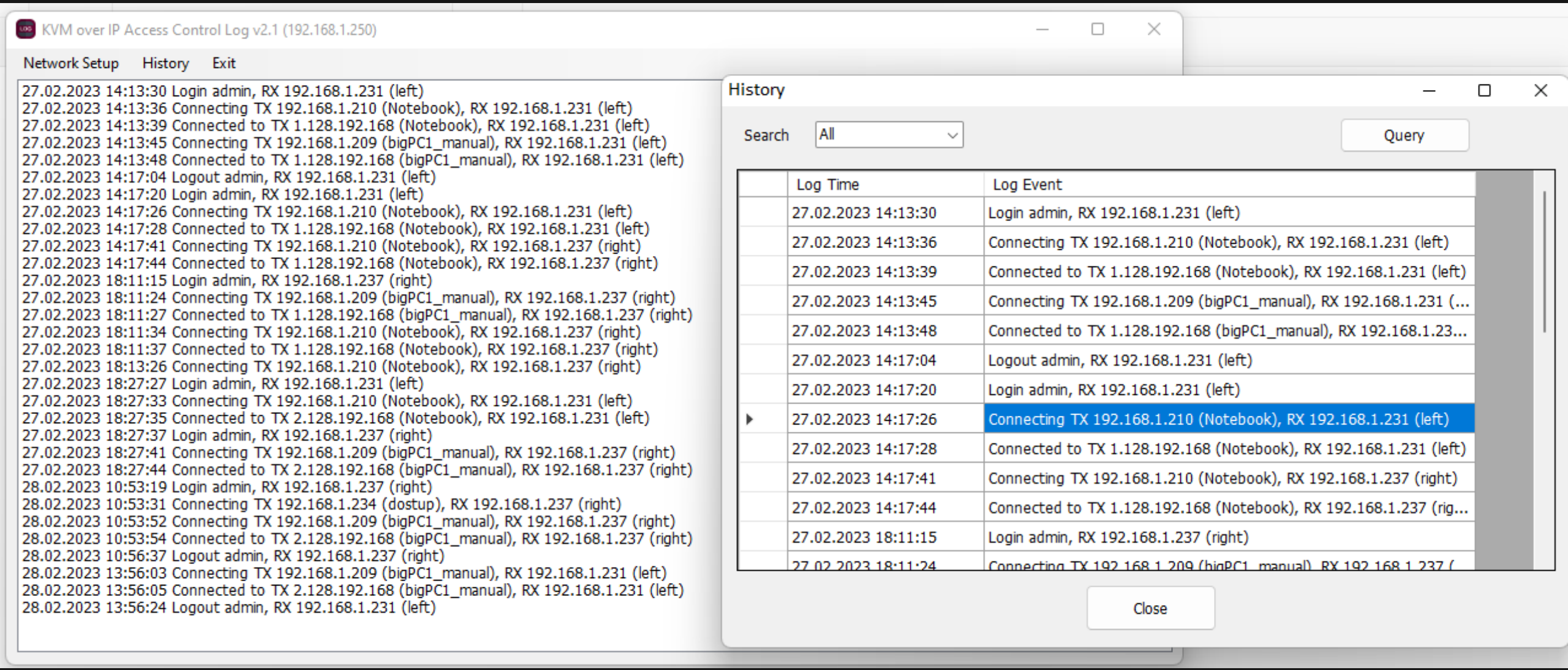
Часть 01

Вступление

Часть 02

Логирование действий операторов

«... Система должна иметь возможность логирования действий пользователей и других основных событий...»


KVM over IP Access Control Log v2.1 (192.168.1.250)
Network Setup
History
Exit
27.02.2023 14:13:30 Login admin, RX 192.168.1.231 (left)
27.02.2023 14:13:36 Connecting TX 192.168.1.210 (Notebook), RX 192.168.1.231 (left)
27.02.2023 14:13:39 Connected to TX 1.128.192.168 (Notebook), RX 192.168.1.231 (left)
27.02.2023 14:13:45 Connecting TX 192.168.1.209 (bigPC1_manual), RX 192.168.1.231 (left)
27.02.2023 14:13:48 Connected to TX 1.128.192.168 (bigPC1_manual), RX 192.168.1.231 (left)
27.02.2023 14:17:04 Logout admin, RX 192.168.1.231 (left)
27.02.2023 14:17:20 Login admin, RX 192.168.1.231 (left)
27.02.2023 14:17:26 Connecting TX 192.168.1.210 (Notebook), RX 192.168.1.231 (left)
27.02.2023 14:17:28 Connected to TX 1.128.192.168 (Notebook), RX 192.168.1.231 (left)
27.02.2023 14:17:41 Connecting TX 192.168.1.210 (Notebook), RX 192.168.1.237 (right)
27.02.2023 14:17:44 Connected to TX 1.128.192.168 (Notebook), RX 192.168.1.237 (right)
27.02.2023 18:11:15 Login admin, RX 192.168.1.237 (right)
27.02.2023 18:11:24 Connecting TX 192.168.1.209 (bigPC1_manual), RX 192.168.1.237 (right)
27.02.2023 18:11:27 Connected to TX 1.128.192.168 (bigPC1_manual), RX 192.168.1.237 (right)
27.02.2023 18:11:34 Connecting TX 192.168.1.210 (Notebook), RX 192.168.1.237 (right)
27.02.2023 18:11:37 Connected to TX 1.128.192.168 (Notebook), RX 192.168.1.237 (right)
27.02.2023 18:13:26 Connecting TX 192.168.1.210 (Notebook), RX 192.168.1.237 (right)
27.02.2023 18:27:27 Login admin, RX 192.168.1.231 (left)
27.02.2023 18:27:33 Connecting TX 192.168.1.210 (Notebook), RX 192.168.1.231 (left)
27.02.2023 18:27:35 Connected to TX 2.128.192.168 (Notebook), RX 192.168.1.231 (left)
27.02.2023 18:27:37 Login admin, RX 192.168.1.237 (right)
27.02.2023 18:27:41 Connecting TX 192.168.1.209 (bigPC1_manual), RX 192.168.1.237 (right)
27.02.2023 18:27:44 Connected to TX 2.128.192.168 (bigPC1_manual), RX 192.168.1.237 (right)
28.02.2023 10:53:19 Login admin, RX 192.168.1.237 (right)
28.02.2023 10:53:31 Connecting TX 192.168.1.234 (dostup), RX 192.168.1.237 (right)
28.02.2023 10:53:52 Connecting TX 192.168.1.209 (bigPC1_manual), RX 192.168.1.237 (right)
28.02.2023 10:53:54 Connected to TX 2.128.192.168 (bigPC1_manual), RX 192.168.1.237 (right)
28.02.2023 10:56:37 Logout admin, RX 192.168.1.237 (right)
28.02.2023 13:56:03 Connecting TX 192.168.1.209 (bigPC1_manual), RX 192.168.1.231 (left)
28.02.2023 13:56:05 Connected to TX 2.128.192.168 (bigPC1_manual), RX 192.168.1.231 (left)
28.02.2023 13:56:24 Logout admin, RX 192.168.1.231 (left)
History
Search
All
Query
Log Time
Log Event
27.02.2023 14:13:30
Login admin, RX 192.168.1.231 (left)
27.02.2023 14:13:36
Connecting TX 192.168.1.210 (Notebook), RX 192.168.1.231 (left)
27.02.2023 14:13:39
Connected to TX 1.128.192.168 (Notebook), RX 192.168.1.231 (left)
27.02.2023 14:13:45
Connecting TX 192.168.1.209 (bigPC1_manual), RX 192.168.1.231 (...
27.02.2023 14:13:48
Connected to TX 1.128.192.168 (bigPC1_manual), RX 192.168.1.23...
27.02.2023 14:17:04
Logout admin, RX 192.168.1.231 (left)
27.02.2023 14:17:20
Login admin, RX 192.168.1.231 (left)
27.02.2023 14:17:26
Connecting TX 192.168.1.210 (Notebook), RX 192.168.1.231 (left)
27.02.2023 14:17:28
Connected to TX 1.128.192.168 (Notebook), RX 192.168.1.231 (left)
27.02.2023 14:17:41
Connecting TX 192.168.1.210 (Notebook), RX 192.168.1.237 (right)
27.02.2023 14:17:44
Connected to TX 1.128.192.168 (Notebook), RX 192.168.1.237 (rig...
27.02.2023 18:11:15
Login admin, RX 192.168.1.237 (right)
Close

Configuration

Transmitter | Receiver | Account | Profile | Log

All logs

All Severity	All Device	All User	Time	Log Information
Information			2023/02/28 12:36:18	Connection V|A|U to channel [001074BD04380000] terminated.
Warning			2023/02/28 12:36:18	Device disconnected with manager (id=001074BE08C30000).
Information			2023/02/28 12:36:16	Connection V|A|U to channel [001074BD044F0000] terminated.
Warning			2023/02/28 12:36:16	Device disconnected with manager (id=001074BE08AB0000).
Information			2023/02/28 07:45:28	Device is up (id=001074BD0A020000).
Warning			2023/02/28 07:45:18	Device disconnected with manager (id=001074BD0A020000).
Warning			2023/02/28 07:45:14	Device lost (id=001074BD0A020000).
Information			2023/02/28 00:13:26	Device is up (id=001074BD04490000).
Information			2023/02/28 00:13:26	Connection V to channel [001074BD04490000] established.
Information			2023/02/28 00:13:15	Connection V|A|U to channel [001074BD04490000] terminated.
Warning			2023/02/28 00:13:15	Device disconnected with manager (id=001074BD04490000).
Warning			2023/02/28 00:13:10	Device lost (id=001074BD04490000).
Warning			2023/02/28 00:01:00	To keep the system log within 150 days.
Information			2023/02/27 22:17:50	Connection V|A|U|S to channel [001074BD0A380000] terminated.
Information			2023/02/27 22:17:50	Connection V|A|U to channel [001074BD0A3E0000] established.
Information			2023/02/27 22:17:16	Connection V|A|U to channel [001074BD0A3E0000] terminated.
Information			2023/02/27 22:17:16	Connection V to channel [001074BD0A380000] established.
Information			2023/02/27 15:21:49	Connection V|A|U to channel [001074BD0A050000] terminated.
Information			2023/02/27 15:21:49	Connection V|A|U to channel [001074BD0A060000] established.
Information			2023/02/27 15:18:58	Connection V to channel [001074BD0A050000] established.

Log Information

Connection V|A|U to channel [001074BD04380000] terminated.

Device disconnected with manager (id=001074BE08C30000).

Connection V|A|U to channel [001074BD044F0000] terminated.

Device disconnected with manager (id=001074BE08AB0000).

Device is up (id=001074BD0A020000).

Device disconnected with manager (id=001074BD0A020000).

Device lost (id=001074BD0A020000).

Device is up (id=001074BD04490000).

Connection V to channel [001074BD04490000] established.

Connection V|A|U to channel [001074BD04490000] terminated.

Device disconnected with manager (id=001074BD04490000).

Device lost (id=001074BD04490000).

To keep the system log within 150 days.

Connection V|A|U|S to channel [001074BD0A380000] terminated.

Connection V|A|U to channel [001074BD0A3E0000] established.

Connection V|A|U to channel [001074BD0A3E0000] terminated.

Connection V to channel [001074BD0A380000] established.

Connection V|A|U to channel [001074BD0A050000] terminated.

Connection V|A|U to channel [001074BD0A060000] established.

Connection V to channel [001074BD0A050000] established.

К основным событиям обычно относится

- авторизация пользователя
- завершение сессии пользователя
- подключение источника

К техническим событиям могут относится

- загрузка устройства
- перезагрузка устройства
- изменение текущих настроек

К производным от базовых событий могут относится

- команда PUSH, подключение источника
- активация пресета, подключение источников
- изменение шаблона видеостены, подключение источников

«... Система должна иметь возможность логирования действий пользователей и других основных событий...»

Для чего и для кого необходимо логирование?

#01 Для технического обслуживания системы

- для службы безопасности
- для анализа действий оператора
- для анализа работы информационных систем заказчика
- для оптимизации работы операторов и информационных систем
- для обучения сотрудников, работе с типовыми задачами

Логирование для анализа

>> 10:00 попытка авторизации, Иванов – отказ

>> 10:02 попытка авторизации, Иванов – отказ

>> 10:03 авторизация, Иванов

>> 10:04 подключение источника: Top Secret

>> ЗфыыЦщкв

>> PasWord

>> PassWord

>> 123456

>> Admin

>> PassWord

>> Password

>> passWord

>> PassworD

Также может быть использовано для:

- для анализа действий оператора
- для анализа работы информационных систем заказчика
- для оптимизации работы операторов и информационных систем
- для обучения сотрудников, работе с типовыми задачами

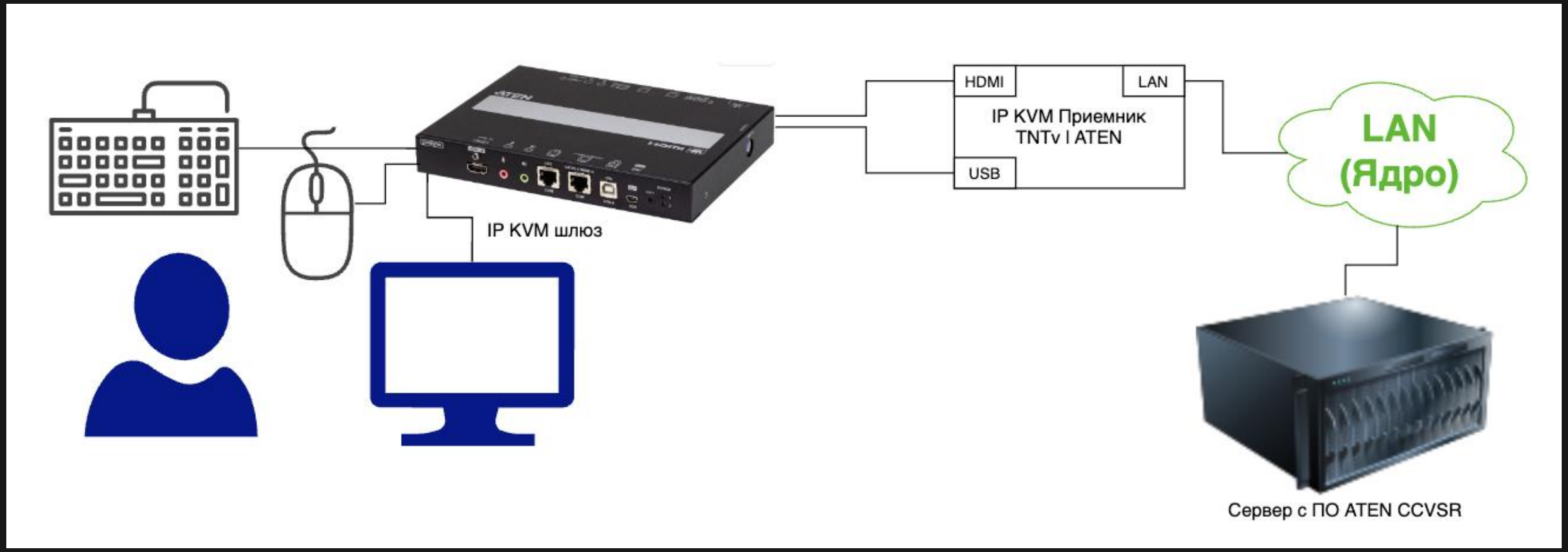
Намеренные, вредоносные действия пользователей

Как получить запись действий оператора?

Оператор под камерой

Программно-аппаратный комплекс записи действий оператора

ATEN CCVSR + ATEN IP-KVM или TNTv IP-KVM


HDMI
LAN
IP KVM Приемник
TNTv I ATEN
USB
LAN
(Ядро)
IP KVM шлюз
Сервер с ПО ATEN CCVSR