



**ЦИТАДЕЛЬ**

## **NetBeholder**

---

**Функциональная спецификация**

ООО «Цитадель»

Все права сохраняются за правообладателем.

ООО «Цитадель» оставляет за собой право вносить изменения в содержащуюся в данном документе информацию без предварительного уведомления.

#### ИНФОРМАЦИЯ О ПРАВЕ СОБСТВЕННОСТИ

Информация, содержащаяся в данном документе, является собственностью ООО «Цитадель». Никакая часть этого документа не может быть воспроизведена или заимствована в какой бы то ни было форме или каким-либо способом – в графическом, электронном виде или механическим путем, включая фотокопирование, запись, в том числе и на магнитные носители, или любые другие устройства, предназначенные для хранения информации – без письменного разрешения ООО «Цитадель». Подобное разрешение не может быть выдано третьей стороной, будь то организация или частное лицо.

# Содержание

|   |   |
|---|---|
| <b>1. ВВЕДЕНИЕ</b> .....                              | 4 |
| 1.1. ЦЕЛЬ ДОКУМЕНТА .....                             | 4 |
| 1.2. НАЗНАЧЕНИЕ КОМПЛЕКСА .....                       | 4 |
| <b>2. ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ</b> .....            | 6 |
| 2.1. ИНТЕРФЕЙСЫ ДОСТУПА К СЕТИ ПЕРЕДАЧИ ДАННЫХ .....  | 6 |
| 2.2. ДЕКОДИРУЕМЫЕ ПРОТОКОЛЫ .....                     | 6 |
| 2.3. ПОДДЕРЖКА ПРОТОКОЛОВ АВТОРИЗАЦИИ АБОНЕНТОВ ..... | 7 |
| 2.4. ОТБОР ИНФОРМАЦИИ .....                           | 7 |
| <b>СПИСОК СОКРАЩЕНИЙ</b> .....                        | 9 |

## 1. ВВЕДЕНИЕ

### 1.1. ЦЕЛЬ ДОКУМЕНТА

В настоящем документе приведено описание функциональных возможностей аппаратно-программного комплекса «NetBeholder» (далее – АПК, комплекс).

### 1.2. НАЗНАЧЕНИЕ КОМПЛЕКСА

«NetBeholder» предназначен для обеспечения законного перехвата информации с целью осуществления уполномоченным государственным органом оперативно-розыскной деятельности на сетях документальной электросвязи (СДЭС).

Комплекс представляет собой техническое средство, обеспечивающее обнаружение, регистрацию и хранение информации о подключениях абонентов и их активности в сети Интернет.

«NetBeholder» предназначен для установки на узлах телематических служб и передачи данных (далее – ПД), использующих технологию Ethernet IEEE 802.3 и сетевой протокол передачи данных IP версий 4 или 6 (рекомендации RFC 791 и RFC 1883 соответственно), а также протоколы идентификации пользователей RADIUS (рекомендации RFC 2138 и 2059) или TACACS+, и на узлах сетей подвижной радиотелефонной связи (СПРС) стандарта GSM/GPRS, 3G, LTE.

АПК «NetBeholder» состоит из следующих основных функциональных частей:

- Съемники – аппаратно-программные средства анализа трафика. На съемники подается весь объем информации, передаваемой и принимаемой всеми абонентами оператора.
- Сервер БД – база данных и средств управления (далее – СУБД). Служит для хранения всего объема перехваченной информации АПК.
- Рабочие места пользователей (далее – РМ) – рабочие станции с установленной программой «Пульт управления «NetBeholder» (далее – ПУ), обеспечивающей графический интерфейс взаимодействия с БД АПК.

На рисунке ниже представлена схема подключения АПК «NetBeholder».



Рисунок 1 Схема подключения АПК «NetBeholder»

## 2. ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

Функциональные возможности АПК «NetBeholder» описаны в разделах ниже.

---

*Примечание: в зависимости от конфигурации комплекса функциональные возможности могут различаться.*

---

### 2.1. ИНТЕРФЕЙСЫ ДОСТУПА К СЕТИ ПЕРЕДАЧИ ДАННЫХ

- Доступ с использованием следующих интерфейсов технологии Ethernet (стандартов IEEE 802.3):
  - 10BASE-T;
  - 100BASE-T;
  - 1000BASE-T;
  - 1000BASE-X;
  - 10GBASE-SR;
  - 10GBASE-LR;
  - 100GBASE-SR4;
  - 100GBASE-LR4.

---

*Примечание: Возможность съема трафика с интерфейсов 100GBASE необходимо согласовывать дополнительно.*

---

### 2.2. ДЕКОДИРУЕМЫЕ ПРОТОКОЛЫ

Декодирование следующих протоколов:

- Протоколы 2/3 уровней модели OSI: 802.3 Ethernet, включая поддержку технологий Pseudo-wire (RFC 4385, RFC 4448); Jumbo frames;
- Почтовые и новостные протоколы;
- Протоколы передачи гипертекстовой информации и файлов;
- Протоколы обмена мгновенными сообщениями (декодирование текстовой переписки (чата) и обмена файлами);
- Протокол Telnet (декодирование текстовой информации; данные перехватываются в виде потоков и в виде объектов прикладных протоколов, передаваемых через Telnet);
- Идентификация использования Skype, OM, TOR, WhatsApp, Viber, SSL.
- Протоколы декодирования VoIP-соединений, использующие протоколы RTP/RTCP в качестве транспортного протокола;
- Декодирование данных, передаваемых внутри нешифрованных туннелей протоколов;
- Декодирование протоколов аутентификации;
- Определение фактов авторизации пользователя по протоколам;
- Детектирование потоков терминального доступа;
- Перехват SMS-сообщений в сетях LTE.

## 2.3. ПОДДЕРЖКА ПРОТОКОЛОВ АВТОРИЗАЦИИ АБОНЕНТОВ

АПК «NetBeholder» позволяет осуществлять идентификацию абонентов, авторизующихся по следующим протоколам:

- RADIUS;
- TACACS+;
- Diameter.

## 2.4. ОТБОР ИНФОРМАЦИИ

- Отбор информационных сообщений и данных контролируемых пользователей на основе критериев отбора, задаваемых пользователем через ПУ.
- Возможность перехвата только статистической информации по заданным критериям отбора.
- Возможность перехвата статистики VoIP.
- Фиксирование фактов подключения и отключения пользователей сети оператора (на основе данных, извлекаемых из сообщений протоколов RADIUS, TACACS+, DIAMETER) в соответствии с установленными критериями отбора.
- Отбор TCP- и UDP-сессий (в том числе для нестандартных протоколов) по [критериям отбора](#).
- Возможность исключения из отбираемых данных информации определённого типа с разграничением по категориям.
- Отбор информации на основе комбинации критериев с использованием логических операторов «И», «ИЛИ» и «НЕ».
- Поиск ключевых слов в кодировках: Win1251, DOS-866, ISO-8859.5, KOI-8r, UTF-8, MAC, UTF-16 (LE & BE), UTF-32 (LE & BE).
- Регистрозависимый и регистронезависимый поиск ключевых слов.
- Поиск ключевых слов и фраз, в том числе в потоковых данных, сжатых по алгоритму gzip/deflate.
- Поиск ключевых слов в сообщениях электронной почты, в том числе в форматах quoted printable и Base-64.
- Для прикладных протоколов SMTP, POP3, IMAP4, NNTP, HTTP, FTP перехват протокольных заголовков, содержащих, в том числе, имя пользователя и пароль (если данные поля присутствуют в заголовке).
- Режим перехвата цепочек объектов, когда для перехваченного по заданным критериям электронного письма либо сообщения службы обмена мгновенными сообщениями ставится на контроль электронный адрес, либо идентификатор отправителя сообщения. В дальнейшем перехватываются все электронные письма или сообщения, отправленные или полученные данным адресатом (пользователем системы обмена мгновенными сообщениями).
- Режим автоматической постановки на контроль IP-адреса пользователя сети оператора, чьи информационные сообщения были отобраны по идентификаторам 3 уровня модели OSI и выше (например, IP адрес, адрес электронной почты и т.д.). В дальнейшем перехватываются все информационные сообщения, отправленные или полученные пользователем в рамках сеанса связи.

## Функциональная спецификация

- Режим перехвата извещений о подключении/отключении пользователей сети оператора, чьи информационные сообщения были отобраны по идентификаторам 3 уровня модели OSI и выше. Данный режим позволяет сопоставлять перехваченные данные с информацией о пользователях сети оператора. Например, при контроле по адресу электронной почты перехватываются не только электронные письма, отправляемые либо получаемые объектом наблюдения, но и факты начала и окончания сеанса связи.



## СПИСОК СОКРАЩЕНИЙ

В настоящем документе используются следующие сокращения и термины с соответствующими им определениями:

|      |  |
|------|--|
| АПК  | Аппаратно-программный комплекс           |
| БД   | База данных                              |
| ООО  | Общество с ограниченной ответственностью |
| ПД   | Передача данных                          |
| ПУ   | Пульт управления                         |
| РМ   | Рабочее место пользователя               |
| СУБД | Средства управления базами данных        |