

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ КОНТРОЛЮ

Рекомендации по повышению защищенности информационной
инфраструктуры от угроз безопасности информации,
связанных с атаками типа «отказ в обслуживании»

В целях повышения защищенности информационной инфраструктуры от угроз безопасности информации, связанных с атаками типа «отказ в обслуживании» необходимо выполнить следующие организационные и технические меры.

1. Операторам государственных информационных и иных систем органов государственной власти, а также субъектам критической информационной инфраструктуры Российской Федерации, которым принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления необходимо:

1.1. Провести инвентаризацию служб и сервисов, доступных из сети «Интернет», используемых в информационной инфраструктуре и размещенных на её периметре, в целях определения возможной поверхности атаки.

1.2. В целях упрощения фильтрации трафика и локализации атак типа «отказ в обслуживании» произвести сегментацию сети и распределить выявленные сервисы по различным IP-адресам или подсетям.

1.3. Обеспечить мониторинг сетевого трафика (например, по технологиям NetFlow, sFlow, IPFIX) на пограничных маршрутизаторах и маршрутизаторах ядра. Для мониторинга использовать имеющиеся программные средства или использовать программное обеспечение с открытым исходным кодом (например, Zabbix, LibreNMS, ntopng).

В целях выявления аномального трафика необходимо по результатам мониторинга зафиксировать: средние значения пакетов в секунду для пользователей информационной системы, объем трафика (бит/с), количество TCP флагов, количество запросов в секунду, а также используемые протоколы. Превышение зафиксированных значений будет свидетельствовать о выявлении аномального трафика.

1.4. Обеспечить фильтрацию на уровне L3 путем создания фильтров на пограничных маршрутизаторах и межсетевых экранах («черных» или «белых» списков, фильтров маршрутов), блокирующих:

входящий трафик с адресами частных сетей (стандарт RFC1918);

входящий трафик от нераспределённых адресных пространств, зарезервированных диапазонов («bogon» сетей).

1.5. Обеспечить на уровне L4 ограничение скорости (rate limiting) на пограничных маршрутизаторах путем ограничения количества ICMP-пакетов и SYN-пакетов в секунду, а также новых соединений (например TCP-сессий), определения лимита пакетов в секунду по протоколу UDP (при необходимости ограничить 53 (DNS), 123 (NTP), 19, 111, 123, 389, 137, 138, 161, 162, 1434, 1701, 1900, 5353 и 11211 (UDP) порты).

1.6. Для облачных провайдеров на уровне L7 с использованием межсетевых экранов (или имеющих специализированных средств защиты информации) обеспечить фильтрацию трафика на предмет выявления атак типа «отказ в обслуживании».

1.7. Реализовать на серверах и межсетевых экранах защиту от SYN-флуда путем включения SYN cookies (или использовать аналогичные инструменты для защиты от атак с использованием подмены IP-адресов (spoofing)).

1.8. Реализовать с использованием межсетевых экранов (или имеющих специализированных средств защиты информации) ограничение количества соединений с одного IP-адреса, а также ограничить скорость установления соединения.

1.9. Реализовать на уровне IP-адресов и балансировщиков разделение типов трафика (веб-приложений (HTTP/HTTPS), сервиса выдачи доменных имен (DNS), IP-телефонии (VoIP), телевидения (IPTV), в случае мультисервисных сетей — обеспечить маркировку трафика), а также интерфейсов взаимодействия (API) указанных сервисов и технологических виртуальных частных сетей для подключения или интеграции со сторонними организациями для применения различных политик фильтрации.

Кроме того, реализовать на уровне IP-адресов и балансировщиков разделение авторитативных DNS-серверов и рекурсивных.

1.10. Для доступных из сети веб-сервисов обеспечить применение межсетевых экранов уровня приложений (WAF).

1.11. Организовать ограничение запросов по протоколу DNS на собственных DNS-серверах, или пограничных маршрутизаторах.

1.12. Обеспечить внедрение «анти-бот» защиты путем использования обратного прокси (reverse proxy) или балансировщиков нагрузки. Кроме того, на уровне L7 предусмотреть блокировку пустых User-Agent и User-Agent ботов.

1.13. Организовать возможность блокировки на пограничных маршрутизаторах (или имеющих специализированных средств защиты информации) трафика по принадлежности стране. Для этого необходимо обеспечить интеграцию с системой «GeoIP». Инструкция по регистрации пользователей в личном кабинете «GeoIP» (<https://geoip.noc.gov.ru/personal>) доступна по адресу: <https://geoip.noc.gov.ru/files/check-in-manual.pdf>.

1.14. Обеспечить резервирование каналов связи, сетевого оборудования и средств защиты информации.

1.15. Ограничить использование из внешних и соседних сетей управляющих протоколов (SSH, SNMP, RDP, VNC, Telnet, NetBios, SMB, RPC) на пограничных маршрутизаторах.

1.16 Организовать удаленный административный доступ к сетевому

оборудованию только из внутренней сети.

1.17. Активировать функции (по возможности в автоматическом режиме) защиты (при наличии таких) от атак типа «отказ в обслуживании» на средствах межсетевого экранирования и других имеющихся средствах защиты информации.

1.18. В случае публикации тестовых сервисов на сетевом периметре обеспечить доступ к ним в рамках «белых списков» IP-адресов или сетей (AS).

1.19. Обеспечить блокировку трафика, поступающего из «теневого Интернета» (список узлов, которые необходимо заблокировать, содержится по адресу <https://www.dan.me.uk/torlist/>).

1.20. В случае обнаружения атаки типа «отказ в обслуживании» на инфраструктуру необходимо обеспечить взаимодействие со специалистами оператора связи по нейтрализации возникающих угроз безопасности информации.

1.21. В случае обнаружения атаки типа «отказ в обслуживании» необходимо руководствоваться порядком действий по обеспечению безопасности объектов критической информационной инфраструктуры и технической защиты информации при реализации атаки типа «отказ в обслуживании» (прилагается).

2. Операторам связи, являющимся субъектам критической информационной инфраструктуры, которым принадлежат информационные системы, информационно-телекоммуникационные сети, необходимо:

2.1. Провести инвентаризацию служб и сервисов, доступных из сети «Интернет», используемых в информационной инфраструктуре и размещенных на её периметре в целях определения возможной поверхности атаки. Также провести инвентаризацию магистральных каналов, пограничных маршрутизаторов, а также сервисов (управления системой выдачи доменных имен (DNS), веб-сервисов, почтовых сервисов, телевидения (IPTV) и других).

2.2. В целях упрощения фильтрации трафика и локализации атак типа «отказ в обслуживании» произвести сегментацию сети и распределить выявленные сервисы по различным IP-адресам или подсетям.

2.3. Обеспечить мониторинг сетевого трафика (например, по технологиям NetFlow, sFlow, IPFIX) на пограничных маршрутизаторах и маршрутизаторах ядра. Для мониторинга использовать имеющиеся программные средства или использовать программное обеспечение с открытым исходным кодом (например, Zabbix, LibreNMS, ntopng).

В целях выявления аномального трафика необходимо по результатам мониторинга зафиксировать: средние значения пакетов в секунду (например, 1000-5000 на абонента), объем трафика (бит/с), количество TCP флагов, количество запросов в секунду, а также распределение используемых протоколов. Превышение зафиксированных значений будет свидетельствовать о выявлении аномального трафика.

2.4. Обеспечить фильтрацию на уровне L3 путем создания фильтров на пограничных маршрутизаторах и межсетевых экранах («черных» или «белых» списков, фильтров маршрутов), блокирующих:

входящий трафик с адресами частных сетей (стандарт RFC1918);

входящий трафик от нераспределённых адресных пространств, зарезервированных диапазонов («bogon» сетей).

2.5. Обеспечить реализацию защиты «анти-спуфинг» путём включения на интерфейсах абонентов проверки обратного пути (uRPF) в «strict» или «loose» режимах (в зависимости от топологии).

2.6. Обеспечить на уровне L4 ограничение скорости (rate limiting) на пограничных маршрутизаторах и узлах доступа (BRAS/BNG) путем ограничения количества ICMP-пакетов и SYN-пакетов в секунду, а также новых соединений (например TCP-сессий), определения лимита пакетов в секунду по протоколу UDP (при необходимости ограничить 53 (DNS), 123 (NTP), 19, 111, 123, 389, 137, 138, 161, 162, 1434, 1701, 1900, 5353 и 11211 (UDP) порты).

2.7. Реализовать на серверах и межсетевых экранах защиту от SYN-флуда путем включения SYN cookies (или использовать аналогичные инструменты для защиты от атак с использованием подмены IP-адресов (spoofing)).

2.8. Реализовать с использованием межсетевых экранов (или имеющихся специализированных средств защиты информации), маршрутизаторов широкополосного удаленного доступа или технологии трансляции сетевых адресов ограничение количества соединений с одного IP-адреса, а также ограничить скорость установления соединения.

2.9. Реализовать на уровне IP-адресов и балансировщиков разделение типов трафика (веб-приложений (HTTP/HTTPS), сервиса выдачи доменных имен (DNS), IP-телефонии (VoIP), телевидения (IPTV)), а также интерфейсов взаимодействия (API) указанных сервисов и технологических виртуальных частных сетей для подключения или интеграции со сторонними организациями для применения различных политик фильтрации.

Кроме того, реализовать на уровне IP-адресов и балансировщиков разделение авторитативных DNS-серверов и рекурсивных.

2.10. Для доступных из сети веб-сервисов обеспечить применение межсетевых экранов уровня приложений (WAF).

2.11. Организовать ограничение запросов по протоколу DNS на собственных DNS-серверах, или пограничных маршрутизаторах.

2.12. Обеспечить внедрение «анти-бот» защиты путем использования обратного прокси (reverse proxy) или балансировщиков нагрузки. Кроме того, на уровне L7 предусмотреть блокировку пустых User-Agent и User-Agent ботов.

2.13. Обеспечить реализацию на пограничных маршрутизаторах на границе

с аплинками (upstream) технологии BGP Remote Triggered Black Hole, а также реализацию пункта 2.4. настоящих рекомендаций. При обнаружении атаки типа «отказ в обслуживании» необходимо обеспечить взаимодействие с аплинком в части ее нейтрализации.

2.14. Обеспечить на пограничных маршрутизаторах перенаправление трафика на очистку (scrubbing) к центру очистки для реализации многоуровневой фильтрации. Для этого необходимо организовывать BGP-сессии с scrubbing-провайдером и выделенный канал или IPsec туннель (виртуальный GRE туннель).

2.15. Организовать возможность блокировки на пограничных маршрутизаторах (или имеющихся специализированных средств защиты информации) трафика по принадлежности стране. Для этого необходимо обеспечить интеграцию с системой «GeoIP». Инструкция по регистрации пользователей в личном кабинете «GeoIP» (<https://geoip.noc.gov.ru/personal>) доступна по адресу: <https://geoip.noc.gov.ru/files/check-in-manual.pdf>.

2.16. Обеспечить резервирование каналов связи, сетевого оборудования и средств защиты информации.

2.17. Ограничить использование из внешних и соседних сетей управляющих протоколов (SSH, SNMP, RDP, VNC, Telnet, NetBios, SMB, RPC) на пограничных маршрутизаторах.

2.18 Организовать удаленный административный доступ к сетевому оборудованию только из внутренней сети.

2.19. Активировать функции (по возможности в автоматическом режиме) защиты (при наличии таких) от атак типа «отказ в обслуживании» на средствах межсетевого экранирования и других имеющихся средствах защиты информации.

2.20. В случае публикации тестовых сервисов на сетевом периметре обеспечить доступ к ним в рамках «белых списков» IP-адресов или сетей (AS).

2.21. Обеспечить блокировку трафика, поступающего из «теневого Интернета» (список узлов, которые необходимо заблокировать, содержится по адресу <https://www.dan.me.uk/torlist/>).

2.22. В случае обнаружения атаки типа «отказ в обслуживании» необходимо обеспечить взаимодействие со специалистами аплинк оператора.

2.23. В случае обнаружения атаки типа «отказ в обслуживании» необходимо руководствоваться порядком действий по обеспечению безопасности объектов критической информационной инфраструктуры и технической защиты информации при реализации атаки типа «отказ в обслуживании» (прилагается).

3. Для защиты от атак на пропускную способность (объемных атак), к которым относятся: UDP-флуд, ICMP-флуд, DNS- (NTP-) амплификация, необходимо:

3.1 Обеспечить на пограничных маршрутизаторах перенаправление трафика

на очистку (scrubbing) к центру очистки для реализации многоуровневой фильтрации. Для этого необходимо организовывать BGP-сессии с scrubbing-провайдером и выделенный канал или IPsec туннель (виртуальный GRE туннель).

3.2 Организовать возможность блокировки на пограничных маршрутизаторах (или имеющихся специализированных средств защиты информации) трафика по принадлежности стране. Для этого необходимо обеспечить интеграцию с системой «GeoIP». Инструкция по регистрации пользователей в личном кабинете «GeoIP» (<https://geoip.noc.gov.ru/personal>) доступна по адресу: <https://geoip.noc.gov.ru/files/check-in-manual.pdf>.

3.3. Обеспечить на уровне L4 ограничение скорости (rate limiting) на пограничных маршрутизаторах путем ограничения количества ICMP-пакетов и SYN-пакетов в секунду, а также новых соединений (например TCP-сессий), определения лимита пакетов в секунду по протоколу UDP (при необходимости ограничить 53 (DNS), 123 (NTP), 19, 111, 123, 389, 137, 138, 161, 162, 1434, 1701, 1900, 5353 и 11211 (UDP) порты).

3.4. По возможности (с привлечением провайдера) организовать anycast-распределение сетевого трафика для собственной инфраструктуры.

3.5. Запросить у провайдера (по возможности) активацию услуг по защите от атак с использованием подмены IP-адресов (spoofing).

3.6. Для защиты от атак типа UDP-флуд необходимо:

3.6.1. Реализовать в информационной инфраструктуре меры из пункта 3.3. настоящих рекомендаций;

3.6.2. На пограничных маршрутизаторах включить списки контроля доступа (использовать «черные» или «белые» списки), ограничить (по возможности) политиками принятие UDP-пакетов, отключить неиспользуемые UDP-сервисы;

3.6.3. На серверах (на базе операционных систем Linux) с использованием утилиты iptables (nftables) реализовать ограничение UDP-пакетов на портах;

3.6.4. На серверах (на базе операционных систем Linux) с использованием утилиты sysctl уменьшить буферы очередей путем изменения значений параметров net.core.rmem_max, net.core.wmem_max, net.core.netdev_max_backlog в файле конфигурации etc/sysctl.conf.

3.7. Для защиты от атак типа ICMP-флуд необходимо:

3.7.1 Реализовать на пограничных маршрутизаторах и серверах в информационной инфраструктуре меры из пункта 3.3. настоящих рекомендаций;

3.7.2. Ограничить использование ICMP-протокола в инфраструктуре и разрешить использование только необходимых служебных протоколов;

3.7.3. На серверах (на базе операционных систем Linux) с использованием утилиты sysctl ограничить широковещательные ICMP-запросы путем присвоения значения «1» параметру net.ipv4.icmp_echo_ignore_broadcasts в файле

конфигурации `etc/sysctl.conf`.

3.8. Для защиты от атак DNS- (NTP-) амплификации необходимо:

3.8.1. Реализовать на пограничных маршрутизаторах и серверах в информационной инфраструктуре меры из пункта 3.3. настоящих рекомендаций;

3.8.2. На DNS-серверах разрешить доступ только для доверенных IP-адресов Российской Федерации (в случае если указанное не ограничит деятельность органа (организации) и действия легитимных пользователей);

3.8.3. На NTP-серверах (на базе операционных систем Linux) отключить функцию `monlist` с использованием утилиты `ntpd` путем добавления в файл конфигурации `/etc/ntp.conf` следующих запретов:

```
restrict default kod nomodify nopeer noquery notrap
restrict -6 default kod nomodify nopeer noquery notrap
```

4. Для защиты от протокольных атак, к которым относятся: SYN-флуд и фрагментационные атаки, необходимо:

4.1. Реализовать на серверах и межсетевых экранах защиту от SYN-флуда путем включения SYN cookies (или использовать аналогичные инструменты для защиты от атак с использованием подмены IP-адресов (spoofing)).

Кроме того, указанную функцию можно включить и на уровне операционной системы на базе Linux с использованием утилиты `sysctl`:

```
sysctl -w net.ipv4.tcp_syncookies=1
```

4.2. Включить (при наличии) функцию «stateful inspection» на имеющихся межсетевых экранах.

4.3. На серверах (на базе операционных систем Linux) с использованием утилиты `iptables` реализовать «stateful inspection» с использованием модуля отслеживания соединений:

```
iptables -A INPUT -m conntrack -ctstate ESTABLISHED,RELATED -j ACCEPT
```

А также разрешить новые соединения правилом:

```
iptables -A INPUT -p tcp --syn -m conntrack -ctstate NEW -j ACCEPT
```

4.4. Реализовать с использованием межсетевых экранов (или имеющихся специализированных средств защиты информации) ограничение количества соединений с одного IP-адреса, а также ограничить скорость установления соединения.

4.5. На серверах (на базе операционных систем Linux) с использованием утилиты `iptables` реализовать ограничение «half-open» соединений путем внедрения следующих правил:

по ограничению SYN-пакетов, например:

```
iptables -A INPUT -p tcp --syn -m limit --limit 10/second --limit-burst 20 -j ACCEPT
```

```
iptables -A INPUT --syn -j DROP
```

по ограничению количества соединений на IP-адрес, например:

```
iptables -A INPUT -p tcp -m connlimit --connlimit-above 20 -j DROP
```

по ограничению возможности SYN-flood через «recent»:

```
iptables -A INPUT -p tcp --syn -m recent --name synflood --set
```

```
iptables -A INPUT -p tcp --syn -m recent --name synflood --set --update --seconds 1 --hitcount 10 -j DROP
```

4.5.1. Кроме того, для настройки таблицы состояний на серверах (на базе операционных систем Linux) необходимо с использованием утилиты sysctl выполнить ограничение conntrack командой, например:

```
sysctl -w net.netfilter.nf_conntrack_max=100000
```

4.5.2. На серверах (на базе операционных систем Linux) необходимо с использованием утилиты sysctl установить время для разрыва «half-open» соединений командой, например:

```
sysctl -w net.netfilter.nf_conntrack_tcp_timeout_syn_recv=30
```

4.5.3. Также на серверах (на базе операционных систем Linux) с использованием утилиты sysctl необходимо увеличить размер очереди half-open соединений и установить частоту повторного запроса сервера путем добавления в файл конфигурации утилиты sysctl следующих строк, например:

```
net.ipv4.tcp_max_syn_backlog=4096
```

```
net.ipv4.tcp_synack_retries=3
```

5. Для защиты от атак на уровне приложений, к которым относятся: HTTP-флуд, Slowloris, медленные POST-запросы, , необходимо:

5.1. Для доступных из сети веб-сервисов обеспечить применение межсетевых экранов уровня приложений (WAF).

5.2. Обеспечить внедрение «анти-бот» защиты путем использования обратного прокси (reverse proxy) или балансировщиков нагрузки. Кроме того, на уровне L7 предусмотреть блокировку пустых User-Agent и User-Agent ботов. Реализовать дополнительное внедрение «CAPTCHA» при доступе на сетевой ресурс для защиты от ботов.

5.3. На имеющихся средствах межсетевого экранирования включить сигнатурные правила (готовые правила, OWASP правила) для обнаружения SQL-инъекций, XSS-атак, аномальных заголовков, правила проверки структуры HTTP-запросов в части длины URL-адреса, проверки заголовков и методов запросов.

5.4. На веб-серверах, балансировщиках нагрузки реализовать блокировку больших заголовков запросов и некорректных запросов, например, для веб-сервера Nginx:

```
large_client_header_buffers 2 1k;
```

```
client_max_body_size 1m.
```

5.5. Организовать возможность блокировки на пограничных маршрутизаторах (или имеющихся специализированных средств защиты информации) трафика по принадлежности стране. Для этого необходимо обеспечить интеграцию с системой «GeoIP». Инструкция по регистрации пользователей в личном кабинете «GeoIP» (<https://geoip.noc.gov.ru/personal>) доступна по адресу: <https://geoip.noc.gov.ru/files/check-in-manual.pdf>.

5.6. Для защиты от атаки типа «Slowloris» необходимо на веб-сервере реализовать закрытие медленных соединений и ограничить возможность долгого удерживания соединений, например, для веб-сервера Nginx:

```
client_header_timeout 10s;  
client_body_timeout 10s;  
keepalive_timeout 5s.
```

В зависимости от технологических особенностей сети время можно увеличить.

6. Для защиты от мультивекторных атак, к которым относятся различные комбинации перечисленных ранее атак, необходимо:

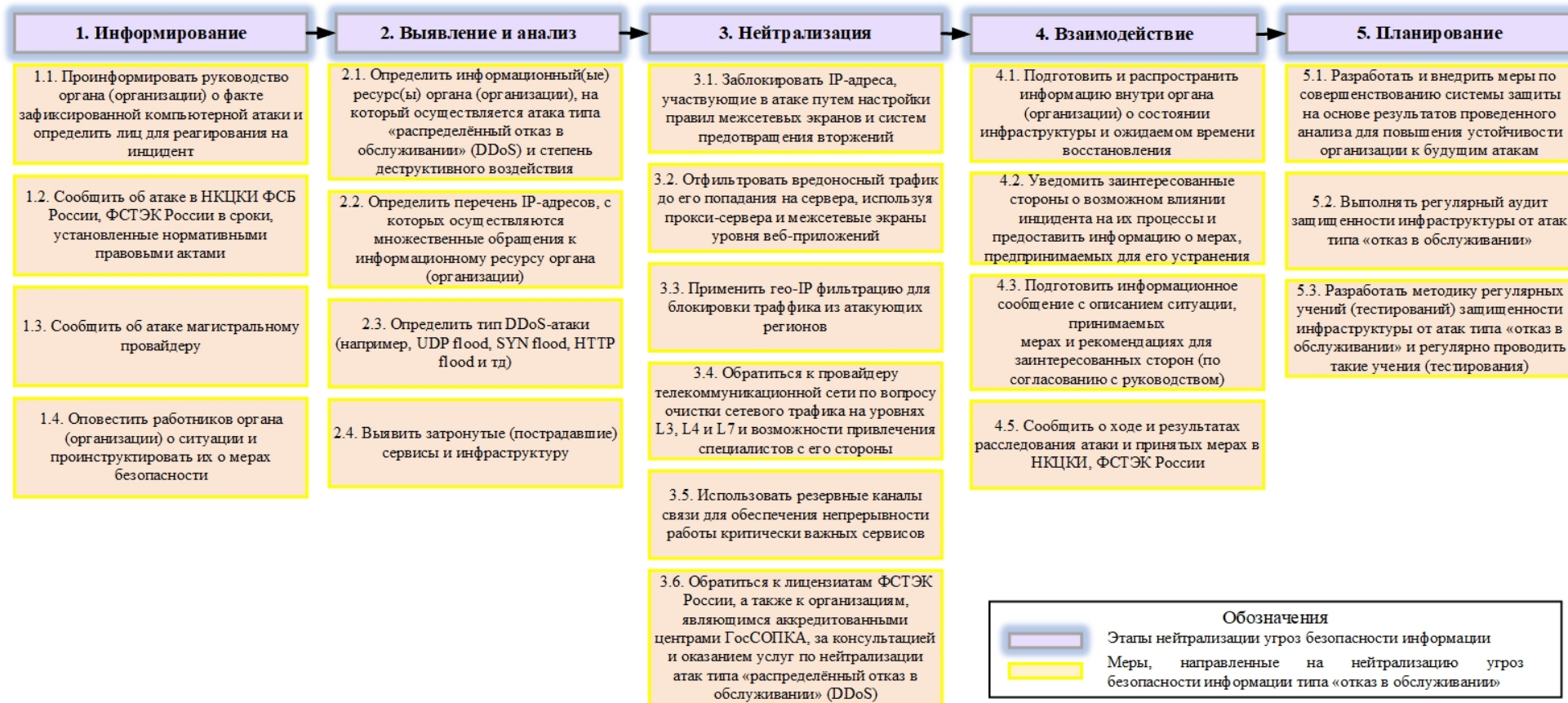
6.1. Реализовать меры указанные в пунктах 3-5 настоящих рекомендаций.

6.2. Обеспечить мониторинг сетевого трафика (например, по технологиям NetFlow, sFlow, IPFIX) на пограничных маршрутизаторах и маршрутизаторах ядра. Для мониторинга использовать имеющиеся программные средства или использовать программное обеспечение с открытым исходным кодом (например, Zabbix, LibreNMS, ntopng). Интегрировать средства мониторинга сетевого трафика с имеющимися системами мониторинга и управления событиями информационной безопасности (SIEM-системами), а также со средствами обнаружения и реагирования на уровне узла.

6.3. Обеспечить резервирование каналов связи, сетевого оборудования и средств защиты информации.

6.4. В случае обнаружения какого-либо типа атак, направленных на отказ в обслуживании, на инфраструктуру необходимо обеспечить взаимодействие со специалистами оператора связи по нейтрализации возникающих угроз безопасности информации.

Порядок действий по обеспечению безопасности объектов критической информационной инфраструктуры и технической защиты информации при реализации атаки типа «отказ в обслуживании»



* Реализация указанного порядка не должна противоречить мероприятиям, предусмотренным Планом реагирования на компьютерные инциденты, разработка и реализация которых предусмотрена нормативными правовыми актами ФСБ России