|  |
| --- |
| **SPBRC** |
| Федеральное государственное бюджетное учреждение науки Санкт-Петербургский научный центр Российской академии наук  **СПбНЦ РАН** | |

|  |  |  |
| --- | --- | --- |
|  |  | **Утверждаю**  **Заместитель Председателя СПбНЦ РАН**  **по научной работе (приемка)**  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Говорухин В.П.**  **«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2021г.** |

**Методические рекомендации по обеспечению информационной и сетевой безопасности при планировании, построении и поддержке корпоративной сети научного учреждения, подведомственного Минобрнауки России - участника сети РОКСОН.**

**Выпуск 1.**

**Методические рекомендации**

**МР 2.2.3.в.1-2020**

**Санкт-Петербург**

**2020г.**

# Предисловие

1. РАЗРАБОТАНЫ ВПЕРВЫЕ Федеральным бюджетным учреждением науки Санкт-Петербургский научный центр Российской академии наук (СПбНЦ РАН) Грудкиным Д.Г.

2. ВНЕСЕНЫ Сектором междисциплинарных исследований СПбНЦ РАН

3. РАЗМЕЩЕНЫ на портале СПбНЦ РАН по адресу <http://spbrc.ru/ru/nir>

# Лист согласования

«Методические рекомендации по обеспечению информационной и сетевой безопасности при планировании, построении и поддержке корпоративной сети научного учреждения, подведомственного Минобрнауки России - участника сети РОКСОН.».

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Научный руководитель СПбНЦ РАН | |  | Академик РАН В.А. Румянцев |
|  | | Руководитель Научно-исследовательского отдела СПбНЦ РАН |  | Д.э.н. А.Г. Бездудная |
|  | | Главный ученый секретарь СПбНЦ РАН |  | Д.и.н. В.А. Попов |

Оглавление

[Предисловие 2](#_Toc62655486)

[Лист согласования 3](#_Toc62655487)

[Аннотация 5](#_Toc62655488)

[Введение 6](#_Toc62655489)

[Термины и определения 7](#_Toc62655490)

[1. Рекомендации по конфигурации коммутируемой сети 9](#_Toc62655491)

[2. ﻿Рекомендации по настройкам граничного маршрутизатора 9](#_Toc62655492)

[3. Рекомендации по управлению серверными ресурсами в сети 9](#_Toc62655493)

[4. Рекомендации по мониторингу ресурсов сети 10](#_Toc62655494)

[Список литературы 11](#_Toc62655495)

[Приложение 1. Пример сегментации локальной сети 12](#_Toc62655496)

[Приложение 2. Пример использования неправильно настроенныхdns-сервероввDDOSатаках 13](#_Toc62655497)

[Приложение 3. Препятствие работе паразитных dhcp-серверов, dhcp-snooping 14](#_Toc62655498)

[Приложение 4. Примеры ПО мониторинга. 15](#_Toc62655499)

# Аннотация

Настоящий документ определяет рекомендации по обеспечению информационной и сетевой безопасности при планировании, построении и поддержке корпоративной сети научного учреждения, подведомственного Минобрнауки России - участника сети РОКСОН.Рекомендации разрабатывались с учетом имеющегося опыта работы академической сети, построения и поддержки корпоративной сети НЦ РАН и взаимодействия с корпоративными сетями организаций – участников сети РОКСОН.

Рекомендации рассчитаны на администратора сети, или другого сотрудника, отвечающего за поддержку и эксплуатацию корпоративной сети учреждения и содержат общие правила построения и поддержки безопасной корпоративной сети.

# Введение

В настоящее время рабочие станции пользователей в сети организации обладают значительно более высокой вычислительной производительностью, чем сетевые устройства и подключены к сети высокоскоростными интерфейсами, 100 или 1000 Мбит/с. Вредоносная сетевая активность с отдельного пользовательского компьютера вполне способна перегрузить CPUцентрального маршрутизатора, или переполнить полосу пропускания внешнего канала, и таким образом привести корпоративную сеть в нерабочее состояние. Рабочие станции, серверы, и сетевое оборудование, при наличии незакрытых уязвимостей или неправильных настроек сетевых служб становятся участниками распределённых атак, или массовых рассылок, а также используются как промежуточные агенты для распространения вредоносного ПО и поиска уязвимостей внутри корпоративной сети. Пострадавшие от распределённой атаки или рассылки хостинг-провайдеры или операторы связи зачастую вносят в блэклисты и начинают фильтровать не только адреса, непосредственно принимавшие участие в атаке, а крупные блоки адресов, включающие адреса соседних организаций. Таким образом, вредоносная активность, исходящая из корпоративной сети одной организации может затруднять работу в сети других организаций-участников сети РОКСОН.

При этом сканирование доступных в сети Интернет адресов на предмет поиска уязвимостей и ошибок в настройках происходит в автоматическом режиме круглосуточно. Администратор корпоративной сети должен учитывать требования обеспечения сетевой безопасности при планировании, построении и поддержке корпоративной сети.

# Термины и определения

|  |  |
| --- | --- |
| Корпоративная сеть | Коммуникационная система, принадлежащая и/или управляемая единой организацией в соответствии с правилами этой организации. |
| Администраторкорпоративной сети | Лицо или группа лиц, ответственных за обслуживание технических и программных средств корпоративной сети, её развитие и надежное функционирование |
| Пользователь корпоративной сети | Работник организации, которому предоставлено право пользования корпоративной сетью |
| Узел сети | Устройство, соединённое с другими устройствами как часть компьютерной сети |
| Сегмент сети | Логически или физически обособленная часть сети |
| Коммутатор | Устройство, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного или нескольких сегментов сети |
| Маршрутизатор | Устройство, которое пересылает пакеты между различными сегментами сети на основе правил и таблиц маршрутизации |
| Граничный маршрутизатор | Маршрутизатор, предоставляющий доступ корпоративной сети к сети оператора связи и глобальной сети Интернет |
| Сетевая служба | Специализированное ПО, обеспечивающее взаимодействие компьютеров в сети и обмен информацией между ними |
| Сервер | Выделенный компьютер в сети, выполняющий задачи предоставления сетевых служб участникам корпоративной или глобальной компьютерной сети. |

# Рекомендации по конфигурации коммутируемой сети

## Используйте управляемые коммутаторы для построения сети, в особенности, если речь заходит об узловых точках (серверная, переход из здания в здание, с этажа на этаж).

## Старайтесь сегментировать сеть по расположению (определяйте отдельные сегменты для разных корпусов), назначению (разные отделы),характеристикам подключения (у кого-то трафик заметно отличается по объёму, или другим параметрам).

## В случае использования динамической адресации в сети устанавливайте на коммутаторах настройки, препятствующие работе паразитных DHCP-серверов, dhcp-snooping и пр.

## По-возможности, не позволяйте пользователям устанавливать сетевое оборудование (коммутаторы, wi-fiмаршруизаторы и т.п.) самостоятельно.

# ﻿Рекомендации по настройкам граничного маршрутизатора

## Используйте частные (private) IP адреса для участников сети. Внешние (public)адреса рекомендуется устанавливать только на серверах с общедоступными ресурсами.

## Используйте средства защиты от подмены IP адресов, доступные для вашего оборудования, такие как IP spoofingprotectionиUnicastReversePathForwarding.

## Ограничивайте доступ по неиспользуемым протоколам и портам пакетным фильтром или ACL.

## Порты, часто используемые для проведения известных DOS-атак и такие как 53 (dns), 161 (snmp), должны быть закрыты для прямогодоступа во внешний мир из локальной сети.

## Не разрешайте прямые подключения из локальной сети к службе доставки почты на сторонних почтовых серверах. (доступ из локальной сети на порт 25 (smtp)).

# Рекомендации по управлению серверными ресурсами в сети

1. Используемые на серверах под управлением администратора корпоративной сети службы старайтесь настраивать по принципу "всё, что не разрешеноспециально - запрещено", напр. почтовый сервер принимает сообщения на отправку только из локальной сети, на доставку -только по списку зарегистрированных на сервере пользователей. DNS-сервер отвечает на запросы только для локальных пользователей,либо на запросы к DNS зонам, размещённым на сервере и т.п. Входящие подключения по всем протоколам и портам, кроме необходимых для работы сетевых служб на сервере должны быть запрещены.
2. Не оставляйте в настройках сетевых служб пароли доступа «по-умолчанию», и другие средства упрощённого доступа к сетевой службе, установленные на этапе настройки или отладки.
3. Отслеживайте и своевременно устраняйте найденные проблемы в безопасности ПО. Мониторьте аномальную активность сетевых служб.Подпишитесь на рассылкиот производителей или сообщества с оповещениями опроблемах безопасности для используемого на сервере ПО.
4. Для серверов под управлением сотрудников организации (вычислительные ресурсы, серверы научных проектов и т.п.), настройте ограничения доступа только к необходимым сетевым службам.
5. Отслеживайте выход обновлений и исправленийдля серверного ПО, уведомляйте администратора сервера.
6. В некоторых случаях возникает необходимость использованияпублично доступного сервера с высокой вероятностью наличия или появления на нём проблем безопасности. Например, аппаратный сервер виденаблюдения, снятый с производства и не обновляемый производителем, или сервер под управлением ОС MS Windows. Назначайте таким серверам частные IP адреса, а доступность из внешнего мира организуйте правиламитрансляции, проброса портов, reverseproxyит.п.

# Рекомендации по мониторингу ресурсов сети

1. Установите в сети сервер мониторинга, собирайте данные по доступности оборудования и служб в сети. Задействуйте какой-либо из хорошо известных и широко используемых программных продуктов, например nagios(<https://www.nagios.org/>), zabbix(<https://www.zabbix.com/>).
2. Мониторьте загрузку сети, пиковые значения, аномальную активность. Интерес представляет не только общая загрузка полосы пропускания (bps), но и значения количества передаваемых сетевых пакетов (pps), широковещательных пактов (broadcastpps), количество ошибок на интерфейсах сетевых устройств (eps).Примеры ПО: cacti (<https://www.cacti.net/>), zabbix(<https://www.zabbix.com>)
3. Отслеживайте время обновления ресурсов, требующих периодическойоплаты/регистрации - доменные имена, сертификаты доменных имён, сертификаты безопасности.

# Список литературы

1. IETF, Руководство по информационной безопасности предприятия (SiteSecurityHandbook, RFC 1244), http://unix1.jinr.ru/faq\_guide/sec/jet/secplant/annex-14.html
2. Cisco, Политика сетевой безопасности: Рекомендации и Описание технологических решенийhttps://www.cisco.com/c/ru\_ru/support/docs/availability/high-availability/13601-secpol.html
3. Microsoft, Рекомендации Azure по обеспечению сетевой безопасности <https://docs.microsoft.com/ru-ru/azure/security/fundamentals/network-best-practices>

# Приложение 1. Пример сегментации локальной сети

маршрутизатор



управляемый коммутатор 1

управляемый  
коммутатор 2

управляемый коммутатор 3



Управляющий сегмент

(для настройки

телекоммуникационного оборудования) vlan1

Бухгалтерский сегмент vlan2

Пользовательский сегмент vlan3

# Приложение 2. Пример использования неправильно настроенныхdns-сервероввDDOSатаках



Злоумышленник

Боты

DNS-серверы

Жертва



Отправка сигнала   
о начале атаки

Отправка пакетов  
с поддельнымIP-адресом источника (адрес жертвы)

Каждый сервер отвечает на запросы на поддельный IP-адрес поражая жертву

# Приложение 3. Препятствие работе паразитных dhcp-серверов, dhcp-snooping



Авторизованный  
DHCP-сервер

Коммутатор с

DHCP snooping



Не авторизованный  
DHCP-сервер

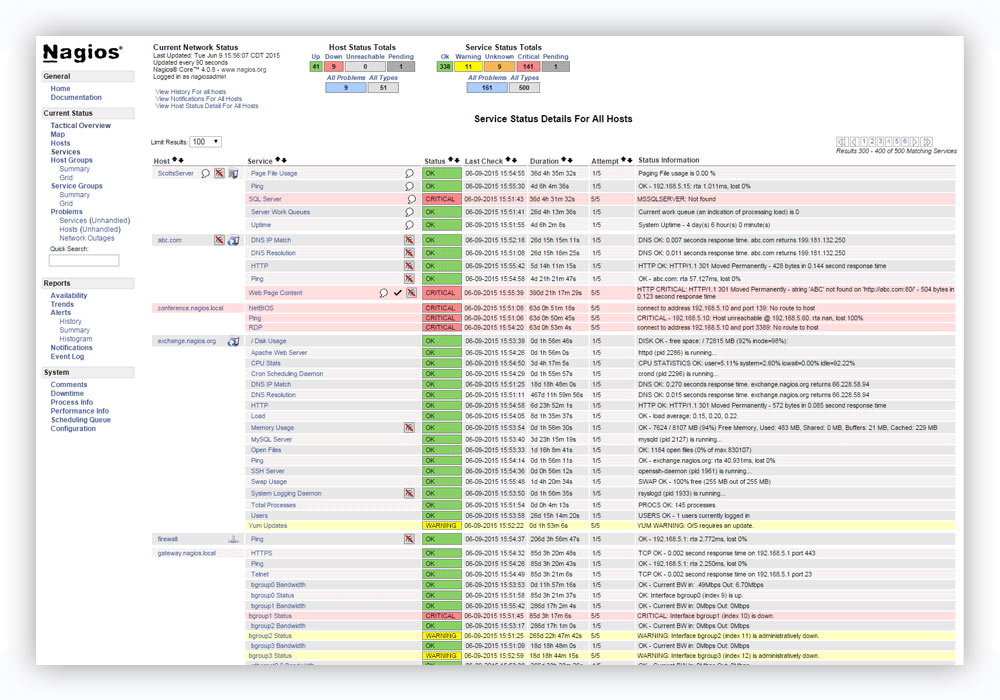
Untrusted port

Untrusted port

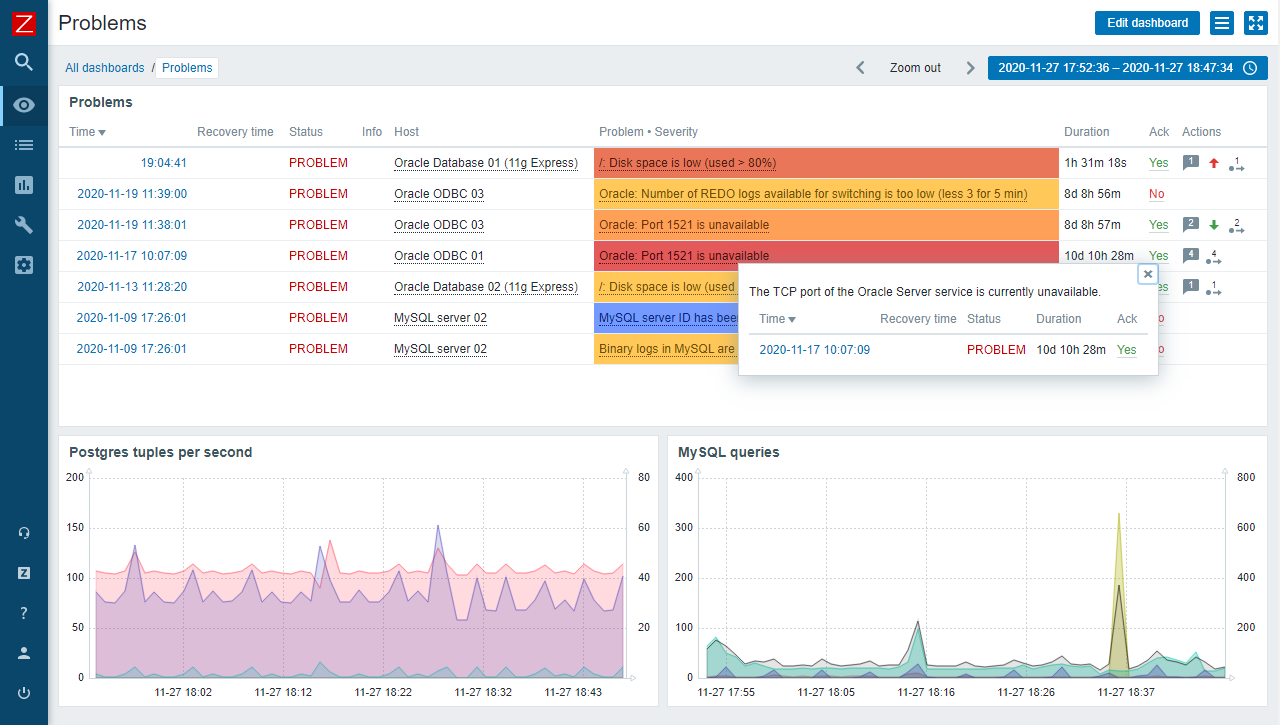
Trusted port

DHCP ответы на Untrusted порты блокируются

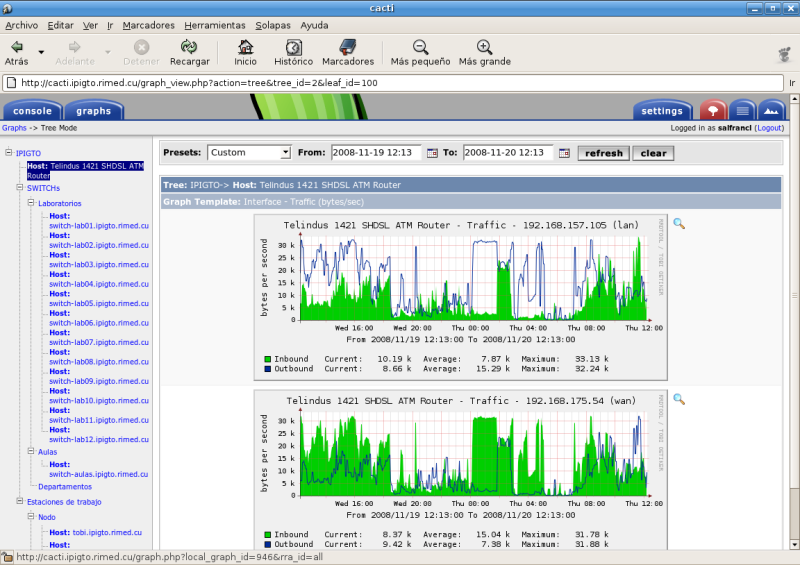
# Приложение 4. Примеры ПО мониторинга.



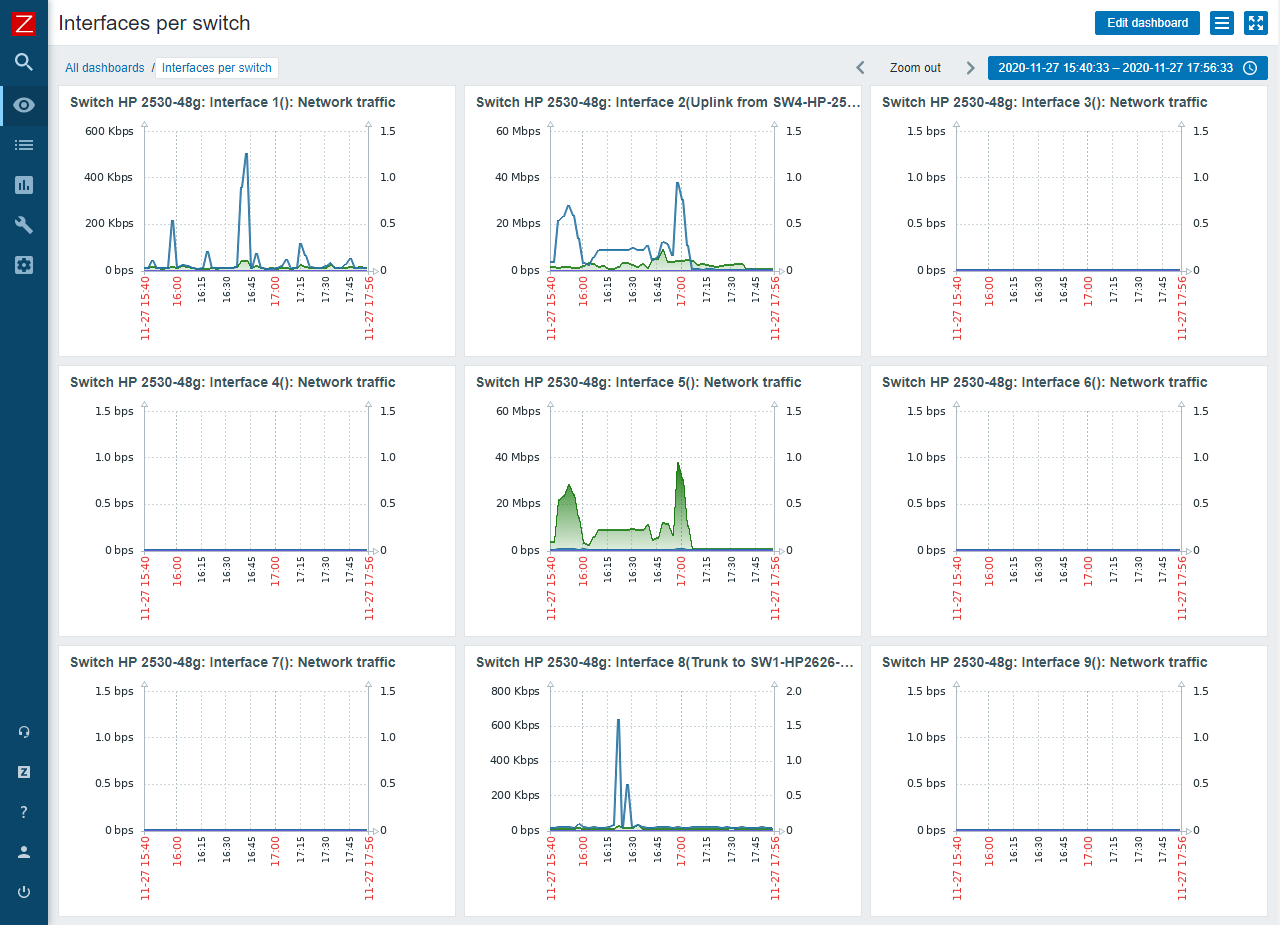
Nagios ([www.nagios.org](http://www.nagios.org))



Zabbix ([www.zabbix.com](http://www.zabbix.com))



Cacti (www.cacti.net)



Zabbix (www.zabbix.com)