Логические (информационные) аспекты эксплуатации. Несанкционированное ПО. Паразитная нагрузка.

Логические (информационные) аспекты работы ЛВС

- **Недопустимо** использование **несанкционированного ПО** (в том числе сетевого);
- Пользователи **не должны использовать** ЛВС для передачи другим компьютерам или оборудованию сети **бессмысленной или бесполезной информации**, **создающей паразитную нагрузку** на эти компьютеры или оборудование, в объемах, превышающих минимально необходимые для проверки работоспособности сети и доступности отдельных ее элементов

Ограничения на информационный шум (спам)

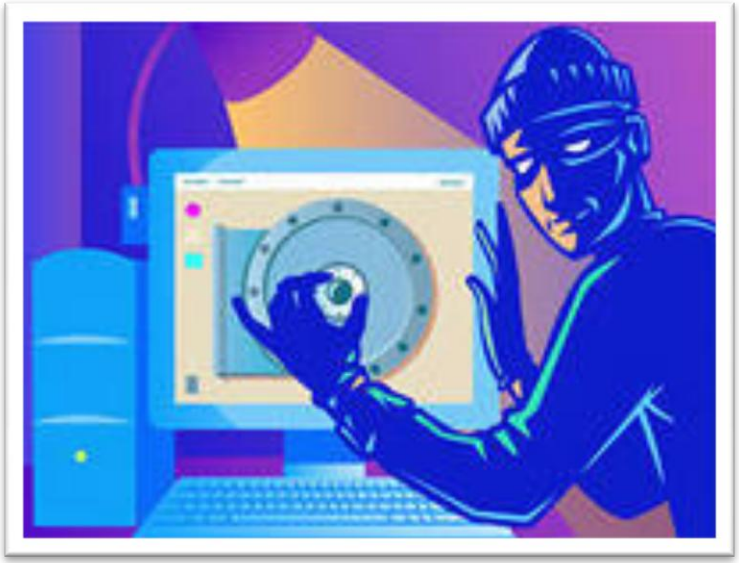
Являются **недопустимыми**:

- Массовая рассылка не согласованных предварительно электронных писем (mass mailing).
- Несогласованная отправка электронных писем объемом более одной страницы или содержащих вложенные файлы
- Несогласованная рассылка электронных писем рекламного, коммерческого или агитационного характера, а также писем, содержащих грубые и оскорбительные выражения и предложения

- Размещение в любой конференции Usenet или другой конференции, форуме или электронном списке рассылки статей, которые не соответствуют тематике данной конференции или списка рассылки (off-topic).
- Использование собственных или предоставленных информационных ресурсов (почтовых ящиков, адресов электронной почты, страниц WWW и т.д.) в качестве контактных координат при совершении любого из вышеописанных действий, вне зависимости от того, из какой точки Сети были совершены эти действия.

Запрет несанкционированного доступа и сетевых атак

- **Не допускается** осуществление попыток **несанкционированного доступа** к ресурсам Сети, проведение или участие в сетевых атаках и сетевом взломе



Запрещены

- Действия, направленные **на нарушение нормального функционирования элементов Сети**, не принадлежащих пользователю.
- Действия, направленные **на получение несанкционированного доступа**, в том числе привилегированного, к ресурсу Сети, последующее использование такого доступа, а также уничтожение или модификация программного обеспечения или данных, не принадлежащих пользователю.

Соблюдение правил, установленных владельцами ресурсов

- Владелец любого информационного или технического ресурса Сети **может установить для этого ресурса собственные правила его использования**.
- Правила использования ресурсов либо ссылка на них **публикуются владельцами или администраторами этих ресурсов в точке подключения к таким ресурсам** и являются **обязательными к исполнению** всеми пользователями этих ресурсов.

Недопустимость фальсификации

- Значительная часть ресурсов Сети не требует идентификации пользователя и допускает анонимное использование.

Пользователю запрещается:

- **Использование идентификационных данных** (имен, адресов, телефонов и т.п.) третьих лиц, кроме случаев, когда эти лица уполномочили пользователя на такое использование.
- **Фальсификация своего IP-адреса**, а также адресов, используемых в других сетевых протоколах, при передаче данных в Сеть
- **Использование несуществующих обратных адресов** при отправке электронных писем

Настройка собственных ресурсов

При работе в сети Интернет пользователь становится ее полноправным участником, что создает потенциальную возможность для использования сетевых ресурсов, принадлежащих пользователю, третьими лицами.

- Пользователь **должен принять надлежащие меры по такой настройке своих ресурсов, которая препятствовала бы недобросовестному использованию этих ресурсов третьими лицами**

Примерами потенциально проблемной настройки сетевых ресурсов являются:

- открытый ретранслятор электронной почты (SMTP-relay);
- общедоступные для неавторизованной публикации серверы новостей (конференций, групп);
- средства, позволяющие третьим лицам неавторизованно скрыть источник соединения (открытые прокси-серверы и т.п.);
- общедоступные широковещательные адреса локальных сетей;
- электронные списки рассылки с недостаточной авторизацией подписки или без возможности ее отмены.

Паразитный трафик

Паразитный трафик - это входящий трафик, получение которого не было явно инициировано самим пользователем или установленным на компьютере программным обеспечением (трафик, генерируемый сканерами сетей, трассировщиками, анализаторами)

Отделить этот паразитный трафик от всего остального, равно как избавится от него совсем, **невозможно**.

Это мировая практика - **паразитный трафик есть во всем мире** и эффективные методы по его полному устранению пока еще не изобрел никто. Как правило, такой трафик **незначителен**, но если компьютер постоянно в сети, то за месяц теоретически может набежать несколько десятков Мб.

Как минимизировать паразитный трафик?

1. **Установка критических обновлений для ОС Windows.**

2. **Отключение некоторых служб Windows**
   1. **Windows Error Reporting Service/Служба отчетов об ошибках**
   2. **Microsoft; Windows Time/Служба времени Windows**

3. **Межсетевые экраны (брандмауэры)**

4. **Антивирусные программы**