Правила работы в компьютерной сети филиала УГНТУ в г. Октябрьском

На территориальных площадках филиала:
* главный корпус, ул. Девонская
* второй учебный корпус, ул. Социалистическая
* общежитие

I. Общие положения

Отдел информационный технологий филиала УГНТУ в г. Октябрьском является структурным подразделением вуза. Отдел создан для проведения работ в области телекоммуникационных технологий в сфере образования и вузовской науки и обеспечения взаимодействия с глобальными информационными ресурсами сети Интернет в интересах широкого круга пользователей.

Согласно положению о отделе его основными задачами являются:

- развитие и внедрение новых телекоммуникационных технологий в учреждениях вузовской науки, высшей и средней специальной школы;
- обеспечение информационного обмена на основе интегрированной в отечественную и мировую системы телекоммуникационной сети;
- предоставление телекоммуникационных услуг подразделениям филиала.

Отдел информационный технологий филиала УГНТУ в г. Октябрьском в рамках своей компетенции при выполнении возложенных задач обязан:

- выполнять мониторинг телекоммуникационной сети и обеспечивать ее устойчивую работу, за исключением перерывов для проведения необходимых регламентных работ;
- проводить мероприятия по развитию сети.

Руководители подразделений согласовывают работы по планированию, разработке и вводу в эксплуатацию телекоммуникаций и локальных компьютерных сетей в филиале УГНТУ в г. Октябрьском с руководством Отдела информационный технологий филиала УГНТУ в г. Октябрьском Список контактных лиц Центра см.: http://www.of.ugntu.ru/new2/ ,

контактный e-mail: www.openpass@mail.ru

Т.к. сотрудники Отдела информационный технологий филиала несут ответственность за функционирование сети филиала в целом и определенную ответственность за деятельность сотрудников подразделений университета в локальной сети и в Интернете, то они в свою очередь требуют и соответствующей ответственности руководства подразделений университета за деятельность их пользователей в сети, т.е. осуществляется иерархический принцип ответственности - в конечном счете за деятельность своих пользователей в сети отвечает административное руководство подключенных к сети подразделений, а не только сетевые системные администраторы.

Проведение в жизнь **политики использования сетевых ресурсов** (**"network usage policy"**, далее по тексту - **сетевой политики**) также осуществляется иерархически. В частности, существует сетевая политика УГНТУ в целом, и в ее рамках ответственность/права возлагаются на/делегируются подразделениям.

Администраторам подразделений рекомендуется в рамках своей компетенции разрабатывать и применять свои правила работы, не входящие в противоречие с общеуниверситетскими. Решение всевозможных проблем, связанных с деятельностью конечных пользователей, прежде всего должна осуществлять администрация конкретного подразделения, подключенного к компьютерной сети филиала.

Политика использования сетевых ресурсов состоит из двух частей: общих принципов и конкретных правил работы, которые эквивалентны специфической сетевой политике. Общие принципы определяют подход к вопросам надежности и безопасности работы в сети, правила же определяют что разрешено, а что запрещено. Правила могут дополняться конкретными процедурами и различными руководствами.

В действиях любого сетевого администратора, направленных на реализацию сетевой политики, выделяются следующие основные задачи:

- мониторинг работы своего сетевого сегмента и создание отчетов об использовании ресурсов сети,
- осуществление управления доступом, исходя из конкретных целей работы своего подразделения,
- поддержание на должном уровне функционирования своего компьютерно-сетевого оборудования и программного обеспечения.

В условиях высшего учебного заведения можно выделить следующие основные угрозы нормальному функционированию компьютерной сети вуза:

- угроза нарушения учебного и научно-исследовательского процесса,
- угроза электронному документообороту (электронная почта, функционирование учебных, бухгалтерских информационных систем, образовательно-информационных серверов),
- угроза нормальной сетевой связности с внешним миром.

Следует подчеркнуть, что особенно внимательно Отдел информационный технологий филиала относится к попыткам несанкционированного доступа к ключевым компонентам университетской сети - коммутаторам и маршрутизаторам опорной сети (backbone), к основным центральным серверам - dns, mail, proxy, www и т.д. - и к серверам конкретных университетских подразделений.

Необходимо также отметить, что обслуживание пользователей осуществляется только при условии соблюдения ими установленных данным документом правил работы в сети филиала.

Содержание данного документа должно быть доведено до сведения всех сотрудников подразделений, студентов и аспирантов, которые являются пользователями сетей в этих подразделениях - данная обязанность возлагается на администрацию конкретных подразделений филиала университета и локальных системных администраторов.

II. Цели разработки и внедрения сетевой политики

Данный документ нацелен прежде всего на создание условий для совместного использования всеми пользователями сетевых ресурсов филиала и фиксирует определенные требования, в рамках которых должны осуществлять свою деятельность администраторы и пользователи сетей подразделений.

Необходимо отметить, что в настоящее время резко возросла значимость сети для работы и учебы. Соответственно, простои, связанные с проблемами в сетевых коммуникациях, влекут за собой большие проблемы и потери как рабочего времени, так и прямые потери в учебной, научной и организационно-финансовой области, а по мере увеличения зависимости нормального функционирования вуза от локальных/глобальных сетей потери от инцидентов с нарушением функционирования сети и сетевой безопасностью становится практически невозможно прямо оценить только финансовыми мерками.

Одна из целей данного документа - дать документальную основу действиям и политике Отдела информационный технологий филиала, чтобы они однозначно воспринимались как действия, направленные на реализацию определенной сетевой политики при работе в сети университета, выработанной и согласованной с руководством Университета ИТМО.

III. Правила работы в сети филиала УГНТУ в г. Октябрьском

Обычно при разработке сетевой политики приходится балансировать между ограничением функциональности ради увеличения безопасности и надежности работы и соглашением на определенные компромиссы в отношении легкости использования ресурсов сети. Причем, все это необходимо осуществлять с учетом необходимости вложения ресурсов - рабочего времени для внедрения и поддержания сетевой политики и финансовых средств, необходимых для приобретения, разработки и сопровождения соответствующего оборудования и программного обеспечения.

Детально однозначно расписать по пунктам, что пользователи вуза должны и могут делать в компьютерной сети, конечно, невозможно, тем более в рамках учебы и работы в филиале университета, - слишком широк профиль деятельности пользователей в сети вуза. Цель данного документа - привести общие рекомендации, а также некоторые указания о том, что явно запрещено или нежелательно делать в нашей сети. Вполне естественно, что ряд общеизвестных и общепринятых правил работы в компьютерных сетях в целом не требует явного повторения и отражения в данном документе (см. Приложения).

Далее приведен текущий список требований к работе в сети филиала. **Данный список является рабочим документом**, т.е. это не просто предмет дальнейших уточнений, а предмет постоянной работы и изменений.

1. **Запрещается проводить несанкционированное сканирование чужих систем** (в т.ч. на предмет поиска уязвимостей) и, тем более, осуществлять попытки несанкционированного проникновения в чужие системы и атаки типа "отказ в обслуживании" (DoS - denial of service). Деятельность по санкционированному проведению сканирований и тестовых атак на системы, с администраторами которых есть договоренность (в учебных целях или в целях обговоренной проверки защиты систем), если она проходит по backbone сети филиала или выходит в Интернет, а не сугубо локальна, в обязательном порядке должна согласовываться с Отделом информационный технологий филиала.
2. **Запрещается производить попытки присвоения себе чужих сетевых атрибутов** (в частности ip-адресов, MAC-адресов сетевых карт), не выделенных явно сетевыми администраторами, генерировать сетевой трафик с поддельными ip- и MAC-адресами, рассылать электронную почту с поддельными исходными адресами, и в целом маскироваться под авторизованных

пользователей для кражи или уничтожения информации, попыток несанкционированного доступа к информации, введения пользователей в заблуждение.

3. **Запрещается предоставлять на своих компьютерах бюджеты посторонним пользователям**, если их деятельность связана с использованием этих машин как промежуточных при проведении с них дальнейших сканирований, атак или взломов компьютерных систем, а также с использованием этих машин как посредников для несанкционированного использования ресурсов филиала посторонними внешними пользователями (например, пересылка "навылет" через внутренние почтовые сервера посторонней почты - mail relaying, организация открытых для внешнего мира proxy/socks/redirect-серверов общего доступа для использования через них сетевых ресурсов филиала, создание серверов с возможностью для анонимных пользователей закачивания на них произвольных файлов с целью организации так называемых "warez"-серверов).
4. **Настоятельная рекомендация к системным администраторам подразделений - устанавливать на свои системы текущие обновления, сервисные пакеты и патчи, а также по возможности обновлять версии программного обеспечения**, связанного с работой в сети, особенно на серверах www/ftp/mail/dns/ssh и др. Всевозможные уязвимости в компьютерных системах обнаруживаются очень часто, и иногда промедление в обновлении Вашей системы может обернуться полной потерей Вашей информации благодаря неизвестному взломщику или, что еще хуже - потерей контроля за собственной системой, когда ее ресурсы будут работать уже не на вас, а на безымянного "крэкера".

   (Сеть - это важный ресурс, который изменил стиль деятельности многих людей и организаций. Тем не менее, сети вообще и Интернет, в частности, страдают от серьезных и широко распространенных проблем с безопасностью. Много организаций было атаковано или зондировано злоумышленниками, в результате чего они понесли большие финансовые потери и утратили свой престиж. В некоторых случаях организации бывают вынуждены временно отключиться от сети и потратить значительные средства на устранение проблем с конфигурациями своих хостов и сетей. Системные администраторы, которые неосведомлены или игнорируют эти проблемы, подвергают свои системы риску сетевой атаки злоумышленниками. Следует учитывать, что даже те системы, которые внедрили у себя текущие на данный конкретный момент меры по обеспечению безопасности, подвергаются тем же опасностям из-за появления новых уязвимых мест в сетевых программах и настойчивости некоторых злоумышленников.)

   Следует подчеркнуть, что один "заброшенный" хост или ресурс, администратор которого не уделяет достаточно внимания обеспечению его безопасности, привлекает к себе потенциальных взломщиков, которые затем могут (и делают это!) производить аналогичные попытки проникновения и по отношению к "соседним" по сети хостам, которые зачастую в условиях учебного заведения могут принадлежать совсем к другому подразделению и важность которых несоизмерима по отношению к первоначальной "приманке" (к примеру, попытки взлома могут перейти от "забытого" тестового студенческого учебного сервера к компьютерам ректората/деканатов/бухгалтерии и т.п.).

5. **Общая политика действий сетевых администраторов при возникновении заметных проблем и "заторов" в сети** (сбои, атаки, сканирования, рассылка вирусов или спама, проведение массированных скачиваний в рабочее время информации постороннего для университета характера - игры, музыкальные и видеофайлы, а также в целом трафика весьма существенных объемов) **- производить временные блокировки такого типа трафика, вплоть до временного отключения от сети такого пользователя или подразделения**, до совместного обсуждения и решения вопроса между "проштрафившимися" пользователями и системными администраторами.
6. **При возникновении у конкретных подразделений проблем в работе с сетью филиала, требующих выяснения внутренних причин, поиска конкретных внутренних нарушителей и проведения внутренних "расследований", эти обязанности осуществляются системными администраторами этих подразделений. Сотрудники Отдела информационный технологий филиала готовы при этом оказывать посильную помощь и консультации.** Однако, с учетом того, что наши услуги по предоставлению доступа к сети предоставляются в основном лицам, имеющим непосредственное отношение к системе высшего образования, причем в компьютерно-сетевой области, большая часть вопросов, видимо, может быть решена в консультациях с преподавателями компьютерных кафедр филиала (пожалуйста, поберегите наше рабочее время и наши нервы). Кроме того, мы рекомендуем воспользоваться соответствующей литературой и поиском ответов на Ваши вопросы в Интернете.
7. **Отдел информационный технологий филиала может производить временную блокировку проблемного трафика - с оповещением системных администраторов подразделения (а в случаях, не терпящих отлагательства по причинам возможного причинения ущерба сети филиала, и без оповещения непосредственно в момент проведения работ) - до устранения самого проблемного трафика и причин, его вызвавших, для того, чтобы остальные пользователи сети университета могли продолжать в это время нормально работать с сетевыми ресурсами.** Подобные блокировки снимаются только после предоставления отчета о результатах расследования и предпринятых действиях.
8. Настоятельное пожелание/требование - по возможности не генерировать особенно большие потоки трафика в рабочее время, стараться переносить это на ночное время, когда загрузка внешнего канала заметно меньше, и когда нет большого количества пользователей, работающих с сетью в интерактивном режиме (рабочим считается время 9:00-21:00 с понедельника до субботы включительно). Разумно также прежде всего попытаться воспользоваться внутренними университетскими информационными сетевыми ресурсами - информационными www/ftp-серверами учебных кафедр и университета в целом.

При служебной/научной необходимости действительно больших потоков сетевого трафика, в т.ч. и проходящего только по внутреннему бэкбону сети филиала без выхода наружу в мир, а также при создании и долговременной эксплуатации подобных сетевых туннелей (различные vpn и т.п.) существенной пропускной способности нужно заранее оповещать об

этом сотрудников Отдела информационный технологий филиала, в противном случае подобный трафик может быть заблокирован.

Особо следует подчеркнуть, что размещение на серверах и рабочих станциях пользователей в открытом общем доступе (в т.ч. и с использованием программного обеспечения для пиринговых файлообменных сетей) коммерческого и лицензионного программного обеспечения, мультимедийных и информационных материалов с нарушением соответствующих авторских прав противоречит сетевой политике филиала УГНТУ в г. Октябрьском.

9. Внешний канал университета постоянно загружен всевозможного рода информационным трафиком, имеющим прямое отношение к научной и учебной деятельности. С учетом этого, **различный внешний мультимедийный трафик типа интернет-видео, музыкальных сетевых радиостанций, а также трафик пиринговых сетей у нас имеет самый низкий приоритет** и, фактически, нежелателен.
10. **Сетевые игры через опорную сеть филиала и Интернет также не поощряются**, и при возникновении подобного мешающего работе и учебе трафика подобные сетевые коммуникации блокируются без предупреждений: вуз - место для работы и учебы, а не бесплатная игротека.
11. Поскольку услуги по обеспечению телекоммуникационного доступа предоставляются подразделениям филиала без оплаты, т.е. не существует официального обоюдного договора об уровне сервисных услуг (SLA) между нами - непосредственными поставщиками сетевых услуг - и нашими клиентами-потребителями, то представляется невозможным обеспечить явные гарантии качества услуг (в частности, выделение сетевых каналов гарантированной запрошенной пропускной способности для запрошенного типа трафика). Однако **Отдел информационный технологий филиала по мере возможности будет обеспечивать потребности подразделений с учетом решаемых ими задач**.
12. **Пользователям сети филиала запрещено распространять через сеть материалы рекламного и коммерческого характера в объемах, сравнимых по порядку величины с общим трафиком подразделений университета (к примеру - реклама, рассылаемая сотнями и тысячами экземпляров писем - типичный пример spam'a, т.е. нежелательной навязчивой рекламной почты).**

    Пользователям сети филиала запрещается распространять через сеть заведомо оскорбляющую честь и унижающую достоинство граждан информацию. Примечание: Отдел информационный технологий филиала не занимается перлюстрацией и цензурой трафика, но в случае конкретных инцидентов и при наличии жалоб пострадавших данное правило применяется в полной мере.

13. **Вопросы физического подключения к сети филиала новых подразделений и новых сетевых сегментов, в том числе и беспроводных (к примеру, wi-fi) должны решаться под обязательным руководством и при участии сотрудников Отдела информационный технологий филиала. Проведение подобных сетевых работ осуществляется силами сотрудников подключаемого подразделения своими материалами после консультации и под руководством сотрудников ОИТ.**
14. При создании новых локальных компьютерных сетей подразделений, которые затем планируется подключать к единой университетской сети, а также при создании долговременных и/или постоянных сетевых туннелей с существенной пропускной способностью необходимо предварительное обсуждение и согласование планируемой сетевой структуры с Отделом информационный технологий филиала.
15. Еще раз подчеркнем - **администрация компьютерной сети филиала резервирует за собой право с целью защиты сетевой инфраструктуры и пользователей всей сети блокировать доступ из подразделений и подсетей, из которых идут spam- и вирусные рассылки, сетевое сканирование, атаки на отказ в обслуживании, а также трафик с хостов, не администрируемых надлежащим образом** - вплоть до временного прекращения всех коммуникаций с хостами, вовлеченными в подобные инциденты (спамовые рассылки, вирусные и хакерские атаки и т.п.), даже если это повлечет за собой временную невозможность нормального доступа пользователей к сетевым ресурсам.

IV. Приложения

Очень полезно почитать документы, по которым "живут и работают" сети крупных провайдеров и/или поставщиков сетевых услуг. К примеру, документ одного из крупнейших российских сетевых "игроков" yandex.ru - "Принципы взаимодействия Яндекса с другими сетями" .