

Учреждение Российской академии наук
Специальная астрофизическая обсерватория

«УТВЕРЖДАЮ»
Директор САО РАН,

член-корр. РАН Ю.Ю.Балега

«_____» _____ 2009г.

Информационно-вычислительная сеть САО (SAONet)

Положение о компьютерной сети

Принято на заседании Ученого совета САО РАН
3 апреля 2009 г. (протокол № 271)

п. Нижний Архыз

2009 год

Информационно-вычислительная сеть САО РАН (далее ИВС САО) является организационно-техническим комплексом, обеспечивающим и поддерживающим функционирование научной, образовательной и административной информационных систем САО РАН (далее Обсерватория). Сеть выполняет функции объединения подразделений Обсерватории в единую информационно-коммуникационную систему, способствует формированию единого научного пространства Обсерватории и его интеграции в мировое информационное пространство.

Данным Положением описываются права и обязанности администраторов различных сетевых сегментов, индивидуальных абонентов и коллективных пользователей сети. Правила основаны на существующей нормативно-законодательной базе Российской Федерации и могут изменяться в соответствии с изменением этой базы.

Положение разрабатывается Отделом информатики совместно с комиссией Ученого совета, принимается на заседании Ученого совета и утверждается директором Обсерватории.

1. Термины и определения

ИВС САО (SAONet) – территориально распределенная компьютерная сеть Обсерватории с постоянно или временно физически подключенными к сети (в том числе через телефонные каналы) компьютерами, с постоянными или временными адресами. SAONet обеспечивает работу комплексов БТА, РАТАН-600, научных, научно-технических, административно-хозяйственных подразделений и всей обсерватории в целом. SAONet состоит из локальных сетей (сетевых сегментов) и сетей рабочих групп (подразделений).

Сегмент SAONet – выделенная физически (территориально – BTANet, RATANNet, LABNnet...) или функционально (ADMNnet, WiFiNet) часть сети с единым адресным пространством.

Сеть подразделения – локальная сеть подразделения, имеющая выделенное подмножество адресов и подключенная к SAONet непосредственно или через сервер подразделения.

Сетевые элементы -

- Внутренние коммуникации - физическая среда ИВС САО, состоящая из кабельных магистралей, коммуникационного и коммутационного оборудования.
- Внешние коммуникации - каналы связи, используемые для коммуникации сети Обсерватории с другими организациями и сообществом Интернет.
- Сетевые серверы - компьютеры, предоставляющие информационно-вычислительные услуги общего пользования, включая ввод-вывод информации. Подразделения Обсерватории могут иметь аналогичные серверы, предназначенные для решения специфических задач подразделения.
- Оборудование общего пользования – все многопользовательские компьютерные средства и системы, включая компьютерные системы наблюдательных комплексов Обсерватории, допускающие доступ заранее не определенных пользователей для решения и на время выполнения научно-производственных задач.
- Компьютеры пользователей - все компьютеры и рабочие станции, использующие ресурсы сети Обсерватории.

Сетевой узел – площадка с распределением серверов, маршрутизаторов и/или прочего оборудования, обеспечивающего работу сети.

Сетевые сервисы – специальные программы и программные комплексы, реализующие предоставляемые сетью информационно-вычислительные услуги (DNS, mail, news, www, ftp и другие).

Пользователи сети – физические лица, зарегистрированные в сетевой службе ИВС САО.

Абоненты сети – имеющие статус юридического лица сторонние организации, так или иначе использующие сетевые ресурсы ИВС САО.

Ответственный пользователь – сотрудник, отвечающий за работу в сети отдельного сетевого элемента и всех пользователей, имеющих доступ к этому элементу.

Коллективный пользователь - сотрудник Обсерватории или сторонней организации, отвечающий за работу в SAONet группы школьников, студентов или сотрудников сторонних организаций.

Администратор подразделения – сотрудник Обсерватории, отвечающий за работу сети подразделения и ее взаимодействие с SAONet.

Администратор сети – сотрудник отдела информатики Обсерватории, отвечающий за работу сети, сетевого сегмента или сетевого сервиса (e-mail, ftp, www и т.п.).

Сетевая служба – системно-административная группа отдела информатики Обсерватории, обеспечивающая работоспособность сети в целом, а также функционирование оборудования общего пользования, регистрацию и консультации его пользователей.

Регистрация в сети – процедура присвоения адресов и имен компьютерам и серверам подразделений, сетевым элементам и доступным сервисам, а также персональных идентификационных имен пользователям SAONet, выдача сертификатов.

Открытый Интернет-доступ – подключение компьютера непосредственно к Интернет-провайдеру с контролем доступа только системой самого компьютера.

Внешний доступ к сетевому элементу - обеспечение непосредственного доступа к сетевому элементу из сетей внешних провайдеров по фиксированному сетевому имени и IP-адресу элемента.

Защищенный Интернет-доступ – обеспечение безопасной работы в Интернете через систему информационной защиты.

2. Общие положения

2.1. SAONet является некоммерческой научно-образовательной сетью, финансируемой из бюджета Обсерватории и целевых дотаций РАН, Министерства науки и образования РФ, а также прочих источников, накладывающих обязательства по некоммерческому использованию сети.

2.2 Основное назначение SAONet состоит в обеспечении бесперебойного информационного обмена между сетевыми элементами Обсерватории, доступа к стандартным сетевым сервисам (DNS, электронная почта и др.) и доступа к ресурсам сети Интернет. SAONet предоставляет услуги как индивидуальным абонентам, так и коллективным пользователям (лабораториям, отделам, административно-управленческим и другим подразделениям Обсерватории). Доступ ко всем ресурсам SAONet для пользователей ИВС САО осуществляется на некоммерческой основе.

2.3. Все сетевые элементы и сервисы SAONet предоставляются пользователям для выполнения научно-производственных работ в направлениях, соответствующих определенным Уставом целям и задачам деятельности Обсерватории. Сетевые элементы пользователей ИВС САО подразделяются на три группы :

- элементы, имеющие фиксированный IP-адрес с возможностью как прямого Интернет-доступа, так и внешнего доступа к сетевому элементу
- элементы, имеющие фиксированный IP-адрес с возможностью опосредованного Интернет-доступа
- элементы, имеющие временный динамический IP-адрес через систему DHCP серверов с возможностью опосредованного Интернет-доступа

Коммерческое или другое нецелевое использование сети, сетевых элементов и сервисов не допускается.

2.4. Ответственность за работоспособность SAONet в целом, ее сопровождение, развитие и модернизацию несет Отдел информатики Обсерватории (ОИ). Отдел выполняет регистрацию пользователей, компьютеров и сетей подразделений, подключение компьютеров пользователей и сетей подразделений к SAONet, осуществляет или организует установку, наладку, эксплуатацию, ремонт и сопровождение программно-аппаратных средств общего пользования Обсерватории и оказывает консультационную помощь пользователям по сетевым вопросам.

2.5. Ответственность за работу в сети индивидуальных компьютеров, компьютеров и сетей подразделений несут подразделения Обсерватории, в которых они находятся. Для каждой зарегистрированной в SAONet сети подразделения, сервера или компьютера определяется администратор или ответственный пользователь.

2.6. Подключение абонентов к SAONet производится в соответствии с соответствующими двухсторонними договорами между Обсерватории и организациями – абонентами.

2.7. Отдел информатики готовит и обновляет информацию о структуре ИВС CAO (полная информация о магистральном уровне ИВС CAO, полный перечень сетевого оборудования и сетевых элементов, постоянно подключенных к ИВС CAO РАН, с указанием имени сетевого элемента, его IP-адреса, места расположения, ФИО ответственного за компьютер). Информация должна быть доступна Вычислительному совету CAO РАН.

3. Вычислительный совет (ВС)

3.1. Для проведения согласованной информационно-вычислительной политики Обсерватории создается совещательный орган – Вычислительный совет. В компетенцию ВС входит обсуждение и выработка рекомендаций по вопросам, связанным с эксплуатацией и развитием ИВС CAO. ВС готовит предложения по приоритетному использованию ресурсов ИВС CAO. ВС рассматривает и готовит предложения по спорным вопросам использования ресурсов ИВС CAO.

3.2. Количественный состав ВС определяется Ученым советом. В Состав ВС входят:

- зав. инженерно-техническим сектором ОИ;
- руководитель группы системных администраторов ОИ;
- представители научных и научно-технических подразделений Обсерватории, делегированные в ВС Учёным советом.

3.3. Состав ВС утверждается приказом директора.

4. Администраторы подразделений

4.1. В подразделениях Обсерватории, организовавших локальную сеть, должны назначаться администраторы. В их обязанности входит:

- обеспечение работоспособности сетевых элементов подразделения, включая как сервера подразделения, так и сетевое оборудование внутреннего пользования;
- регистрация пользователей для работы с сетевыми элементами и сервисами подразделения;
- соблюдение положения о ИВС CAO;
- обеспечение антивирусной защиты сетевых элементов подразделения;
- обеспечение информационной безопасности сетевых элементов подразделения.

4.2. Администратор подразделения имеет право:

- участвовать в работе Вычислительного совета;
- вносить предложения по вопросам эксплуатации и развития ИВС CAO;

- обращаться за содействием по вопросам эксплуатации сети подразделения в Отдел информатики.

5. Порядок регистрации и работы пользователей

5.1. Пользователем ИВС САО может быть любой сотрудник Обсерватории, сотрудник другой научной или образовательной организации, а также другое лицо, необходимость доступа которого к сети обусловлена научно-производственными или учебно-просветительскими интересами Обсерватории. Пользователь должен обладать знаниями, необходимыми для работы в сети и на оборудовании общего пользования. Регистрация пользователей осуществляется Сетевой службой по представлению руководителя соответствующего подразделения Обсерватории.

5.2. Пользователи подразделяются на следующие категории:

- постоянные пользователи – сотрудники обсерватории;
- постоянные пользователи - сотрудники других организаций;
- временные пользователи;
- коллективные пользователи.

5.3. Пользователи всех категорий оформляют электронную заявку на регистрацию в SAONet (ссылка на странице Обсерватории в разделе *Сервис > Правила для пользователей ИВС САО*). Печатают сформированную Регистрационную карту пользователя, которая хранится в сетевой службе.

5.4. Для регистрации в SAONet постоянного пользователя - сотрудника Обсерватории или временного пользователя регистрационная карта подписывается пользователем и руководителем соответствующего подразделения. Для регистрации постоянного пользователя - сотрудника другой организации дополнительно необходимо согласие зам. директора Обсерватории по компетенции. Для регистрации коллективного пользователя регистрационная карта заполняется ответственным за группу лицом и руководителем соответствующего подразделения с приложением списка группы. Заполненная регистрационная карта представляется на согласование заведующему отделом информатики.

5.5. Администратор сетевой службы либо подразделения знакомит пользователя с правилами работы в сети и на оборудовании общего пользования, после чего регистрирует пользователя, фиксирует имя (login) для работы в сети, определяет права доступа и доступные сетевые ресурсы.

5.6. Сетевая служба (NOC) создает и сопровождает базу данных пользователей и сетевых элементов, ведет оперативную статистику использования ресурсов сети.

5.7. Пользователь несет ответственность за все действия, производимые им при работе в сети Обсерватории. При определении ответственности пользователя не имеет значения, преднамеренно или непреднамеренно пользователь совершал эти действия, понимал или не понимал смысл совершаемых им действий.

5.8. Аналогично п. 5.7 ответственный пользователь (администратор подразделения) отвечает за действия, производимые членами соответствующего коллектива пользователей.

5.9. Пользователь имеет право:

- круглосуточно получать непосредственный или удаленный доступ к сети для научно-производственной деятельности;
- использовать в научно-производственных целях оборудование общего пользования;
- использовать для удаленного доступа модемный пул SAONet;
- получать информацию о текущем и планируемом состоянии сети;
- получать консультационную помощь персонала сетевой службы.

5.10. Пользователь обязан:

- сохранять свой пароль в тайне и применять все доступные средства для защиты учетной и другой сетевой информации от несанкционированного и неавторизованного доступа;
- выполнять при работе в сети указания и следовать рекомендациям сетевой службы, а также администраторов подразделений и ответственных пользователей подразделений Обсерватории;
- сообщать сетевой службе или администратору подразделения о каждой ставшей ему известной попытке несанкционированного доступа к сети или ее элементам и случаях нарушений правил работы;
- соблюдать правила работы в сети, уважать права на работу в сети других сотрудников, не допускать необоснованной загрузки сети и оборудования общего пользования в ущерб другим пользователям.
- сообщать сотрудникам сетевой службы об изменениях регистрационных данных.

5.11. Пользователю **запрещается**:

- нецелевое использование компьютеров, периферийных устройств и других сетевых элементов;
- передача имеющегося на компьютерах и в сети лицензионного математического обеспечения другим лицам или организациям;
- передача другим лицам и организациям созданных в Обсерватории программных систем, баз данных и открытие доступа к данным, полученным в Обсерватории, без согласования с авторами и администрацией Обсерватории;
- размещение на компьютерах лицензионного математического обеспечения без наличия соответствующей лицензии;
- предоставление доступа к данным и программам лицам, не имеющим на это право;
- доступ в любой форме к конфиденциальной учетной информации других пользователей;
- незапланированная и/или необоснованная загрузка сети в ущерб другим пользователям;
- рассылка анонимных писем и писем с модифицированными адресами, затрудняющими идентификацию автора, а также массовая безличная рассылка;
- транслирование в SAONet пакетов сторонних сетей (провайдеров);
- использование средств радиодоступа в SAONet без согласования с Отделом информатики.

5.12. Перерегистрация пользователей производится по мере необходимости по приказу директора Обсерватории. Учетная информация пользователей, не прошедших перерегистрацию, их каталоги и файлы аннулируются.

6. Порядок регистрации, подключения и работы сетевых элементов

6.1. Все пользователи (рабочие группы, подразделения), имеющие в своем распоряжении сетевые элементы, отвечающие стандартам сетевого оборудования, имеют право на включение этих элементов в сеть.

6.2. Все подключения, отключения, переключения и перенастройки сетевых элементов и оборудования общего пользования производятся только сотрудниками отдела информатики или, в особых случаях, другими лицами с обязательным уведомлением сетевой службы.

6.3. Каждый сетевой элемент, подключенный к сети Обсерватории, должен быть зарегистрирован в сетевой службе с указанием лица, ответственного за данный сетевой

элемент. Незарегистрированные должным образом устройства подлежат отключению от ИВС САО.

6.4. Регистрация и подключение сетевого элемента осуществляется на основании обращения его ответственного пользователя либо администратора подразделения, либо руководителя соответствующего подразделения.

6.5. Для регистрации и подключения сетевого элемента пользователь (ответственный пользователь, администратор рабочей группы) заполняет электронную форму, печатает сформированную заявку на регистрацию сетевого элемента, подписывает у руководителя соответствующего подразделения, и представляют в отдел информатики.

6.6. Подключение сетевого элемента выполняется Отделом информатики после оформления заявки в соответствии с производственными планами ОИ.

6.7. После выполнения процедуры подключения сетевая служба проводит регистрацию сетевого элемента и инструктаж ответственного лица.

6.8. Открытый Интернет-доступ и *Внешний доступ к сетевому элементу* предоставляются по запросу руководителя подразделения, согласованному с зам. дир. по науке.

6.9. Все сетевые элементы, включенные в сеть Обсерватории, могут использоваться только в научно-производственных целях, соответствующих направлениям научной деятельности Обсерватории, кроме особо оговариваемых случаев.

6.10. Запрещается использовать любой элемент сети Обсерватории, включая персональные компьютеры и рабочие станции, для организации несанкционированного доступа к ресурсам сети Обсерватории, а также к ресурсам других сетей и Интернет.

6.11. Запрещается использовать любой элемент сети Обсерватории для хранения и распространения лицензионной информации, лицензионного программного обеспечения, а также материалов, защищенных авторскими правами, без соответствующего разрешения.

6.12. Доступ, непосредственный или удаленный, к оборудованию общего пользования разрешается только зарегистрированным пользователям. Пользователь обязан выполнять требования инструкций и бережно относиться к оборудованию общего пользования.

6.13. Пользователям оборудования общего пользования **запрещается**:

- самовольно останавливать, перезагружать, выключать и включать любое компьютерное и сетевое оборудование общего пользования;
- производить переключение внешних соединений такого оборудования;
- менять конфигурацию внешних устройств и аппаратных средств оборудования общего пользования;
- использовать не соответствующие техническим нормам машинные носители при работе с оборудованием общего пользования.

6.14. Отключение электропитания любого оборудования общего пользования допускается только в экстренных ситуациях (возгорание оборудования, затопление оборудования водой и т.п.) с немедленным уведомлением сетевой службы.

6.15. Перерегистрация сетевых элементов производится по мере необходимости по приказу директора Обсерватории. Сетевые элементы, не прошедшие перерегистрацию, отключаются от сети.

7. Порядок регистрации и работы сетевых сервисов

7.1. Каждый сетевой сервис должен:

- не мешать правильной работе сети и центральных сервисов и не противоречить центральным сетевым сервисам;
- иметь соответствующие описания и инструкции (не описанный сервис не должен иметь доступ из-за пределов сети);

- обладать достаточным уровнем защищенности и пройти контроль на сетевую безопасность.

7.2. Каждый сетевой сервис, реализованный в SAONet, должен быть зарегистрирован в сетевой службе на определенное ответственное лицо. Незарегистрированные должным образом сервисы подлежат блокировке без дополнительного предупреждения.

7.3. Для регистрации сервиса ответственное лицо и руководитель соответствующего подразделения заполняют электронную форму, печатают, подписывают и представляют в отдел информатики.

7.4. Сетевая служба регистрирует сервис после выполнения процедур согласования и тестирования.

7.5. Сотрудники сетевой службы имеют право блокировать внешний доступ к отдельным сервисам в случае, если их функционирование угрожает безопасности сети как целого либо нарушает законодательство РФ. При блокировке сервиса сетевая служба обязана предоставить его владельцу обоснование своего решения и предложения по решению выявленных проблем.

8. Обеспечение безопасности

8.1. Под обеспечением безопасности сети подразумевается защита сети и ее элементов от несанкционированного доступа, нарушений нормальной работы, повреждений и других умышленных и неумышленных действий, создающих помехи функционированию SAONet.

8.2. Контроль обеспечения безопасности сети осуществляет сетевая служба, которая имеет право:

- собирать необходимую информацию о работе сети в целях поддержания безопасности и накопления статистики;
- получать информацию, касающуюся сети и сетевых ресурсов Обсерватории от пользователей, ответственных пользователей и администраторов подразделений, а также от имеющих подключение к сети сторонних организаций;
- проверять сетевые элементы и сервисы на уровень их защищенности;
- отключать с уведомлением ответственного лица от сети элементы и блокировать сервисы, не обладающие достаточным уровнем защищенности.

8.3. Сетевая служба **обязана**:

- планировать и осуществлять мероприятия по повышению уровня защищенности сети, сетевых элементов и сервисов;
- проводить по вопросам безопасности консультационно-разъяснительную работу;
- оперативно реагировать на случаи нарушения безопасности сети.

8.4. Для обеспечения безопасности SAONet все пользователи **обязаны**:

- выбирать сложные пароли в соответствии с рекомендациями сетевой службы;
- обеспечивать недоступность своей учетной информации (login/password) другим лицам;
- заранее согласовывать с сетевой службой процедуру и средства удаленного доступа при необходимости временной или постоянной удаленной работы;
- обоснованно применять процедуры тестирования сетей и минимизировать применение таких процедур;
- реагировать на вызов системного администратора, даже если для этого необходимо аварийно прервать текущую работу (пересылка файла, сеанс редактирования и т.п.);
- выполнять рекомендации по безопасной работе в сети (Приложение 1).

- корректно выходить из системы по завершении работы.

8.5. Администраторы подразделений (ответственные пользователи) **обязаны** обеспечивать выполнения требований безопасности в своих группах.

8.6. Обеспечение информационной безопасности (защита от несанкционированного доступа) возлагается на лиц, ответственных за соответствующие информационные сервисы (архивы, базы данных и т.п.).

8.7. При нарушении или возникновении угрозы нарушения безопасности функционирования сети, элементов сети и сервисов сетевая служба имеет право без предварительного уведомления:

- блокировать учетную информацию любого пользователя;
- отключить от сети любой элемент;
- блокировать любой сетевой сервис.

8.8. Сетевая служба имеет право:

- потребовать объяснений и корректирующих действий от лиц создавших угрозу безопасности;
- ходатайствовать перед администрацией о применении санкций к лицам, ответственным за нарушение безопасности SAONet.

9. Ответственность за нарушение правил.

9.1. Пользователи ИВС САО обязаны соблюдать настоящие правила.

9.2. Пользователь несет ответственность за весь информационный обмен между его компьютером и другими компьютерами в ИВС САО и за ее пределами, а также за все нарушения правил сетевого взаимодействия, вызванные несоблюдением принципов "security" (передача посторонним лицам своего пароля и идентификатора).

9.3. В случае нарушения правил, виновный может быть временно или постоянно лишен права пользования SAONet, сетевые элементы временно или постоянно отключены от сети, а сетевые сервисы временно или постоянно заблокированы.

Приложения:

1. Рекомендации по безопасной работе в сети.
2. Обязанности системных администраторов.

Рекомендации по безопасной работе в сети

Все системы, подключенные к INTERNET, могут подвергаться атакам с целью их взлома или нарушения работы. Взлом сервера может иметь весьма тяжелые последствия, влекущие невосполнимые потери информации и большие материальные затраты.

Для предотвращения таких инцидентов рекомендуется придерживаться следующих рекомендаций:

1. Авторизация

Поскольку проверка прав доступа к сети производится только на основании пароля, то основная опасность, которая может грозить абоненту – получение этого пароля недобросовестными лицами. ***Пароль должен*** иметь длину 6-8 символов и включать большие и малые буквы, знаки пунктуации. ***Пароль не должен*** быть связан с: информацией о пользователе (имя, фамилия, название отдела, номер комнаты, телефона и т.д.); информацией о компьютере пользователя или о сервере (имена, типы компьютеров); мнемоническими комбинациями клавиатуры (типа УКЕНГ, QUERTY, SSSSSS и т.п.).

Недопустимо передавать свой login/password любому другому лицу. При необходимости даже кратковременной работы другого человека (коллеги, студента) необходимо зарегистрировать для него отдельный login.

По возможности нигде ***не применяйте сохранение паролей***. Каждый раз вводите пароли вручную.

Завершив работу, необходимо аккуратно выйти из системы - закрыть окна и корректно выйти из системы.

2. Программы, использующие сетевые функции

Следует ограничить применение операций тестирования сетей, таких, как ***ping, traceroute***, и использовать их, только если это действительно необходимо. В некоторых ситуациях системный администратор может попросить вас обосновать реальную необходимость этих действий.

Из-за многочисленных ошибок в реализации сетевых функций операционных систем семейства Windows у недобросовестных лиц существует возможность нарушить работу компьютера абонента во время его доступа в сеть.

Рекомендации:

- Никому не сообщайте выданный вам IP-адрес. Применяйте Personal firewall, или его аналоги.
- Следите за сетевыми новостями и своевременно устанавливайте обновление ОС и свежие версии программ. (Ошибки программ, позволяющие получить доступ к ресурсам компьютера, были обнаружены, например, в некоторых версиях Internet Explorer, Netscape Navigator и ICQ).

3. Совместный доступ к ресурсам

В случае предоставления ресурсов Windows в совместное пользование без закрытия паролем, во время работы в сети существует реальная угроза получения недобросовестными лицами доступа к этим ресурсам.

Рекомендуется не предоставлять свои ресурсы в совместное пользование или хотя бы устанавливать на них пароль.

4. Конфигурация сервисов на компьютере

В случае размещения на компьютере абонента сетевых сервисных функций (WWW, FTP, Sendmail), при их неправильной конфигурации возможны получения недобросовестными лицами доступа к ресурсам компьютера.

Рекомендуется, если Вы не уверены, что способны правильно настроить сетевые сервисные функции своего компьютера - не используйте их совсем или обратитесь за консультацией в административную группу.

5. Вредоносные программы


Существуют программы, заведомо приводящие к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети.

На практике вредоносными программами признаются: компьютерные вирусы, черви, троянские программы, руткиты, эксплоиты уязвимостей, spyware-программы, а также некоторые программные инструменты для взлома.

Вредоносные программы помещаются злоумышленником на открытые ресурсы (файл-серверы, открытые для записи накопители самого компьютера), носители информации или присылаются с помощью служб обмена сообщениями (например, электронной почтой) из расчета на их запуск на конкретном, входящем в определенный круг или произвольном «целевом» компьютере. В последнее время распространилось большое количество, так называемых:

- троянских программ, которые предназначена для нанесения вреда пользователю или делающая возможным несанкционированное использование компьютера другим лицом (то есть превращающая компьютер в «зомби») для выполнения всевозможных задач, включая нанесение вреда третьим лицам;
- spyware программ, обычно распространяющихся вместе другим полезным, занимающееся сбором информации на компьютере пользователя и отсылкой ее создателю;
- adware программ, программное обеспечение, при использовании которого пользователю принудительно показывается реклама.

Рекомендации:

- Не перекачивайте и не запускайте неизвестные вам программы с сомнительных сайтов.
- Если во время работы в сети Вы получаете сообщение, содержание которого непонятно, закрывайте окно сообщения только через .
- Не запускайте исполняемые вложения в электронную почту, если автор и назначение письма Вам хорошо не известны.
- При установке программ внимательно отслеживайте все компоненты, которые входят в состав программы.
- Используйте постоянно антивирусное ПО и проводите профилактические проверки. Регулярно следите за обновлениями антивирусной программы (помните: антивирусная программа, которая не обновлялась больше месяца, **бесполезна**).
- Используйте программы-защитники от троянских программ и spyware-программ.

6. Взаимодействие с сетевой службой (NOC).

При возникновении вопросов можно оперативно обратиться к соответствующему администратору (Приложение 3) с помощью системных программ связи, e-mail или по телефону.

Желательно подписаться на новости группы saoinform сервера новостей news.sao.ru, а также на другие группы, информирующие о проблемах безопасности.

При обращении системного администратора (talk, срочный mail) необходимо немедленно ответить, даже если для этого приходится аварийно прервать текущую работу (пересылка файла, сеанс редактирования). Это связано с тем, что такие обращения производятся в момент опасности, когда системному администратору необходимо срочно удостовериться личность того, кто действительно работает в системе или произвести аварийный останов.

При возможности работы с других компьютеров (поездка на конференцию, работа из другой организации, и т.д.) необходимо заранее согласовать с системным администратором средства для удаленной работы.

Дополнительно для тех, кто использует телефонный доступ:

- Телефонный доступ к серверам общего пользования предназначен исключительно для сеансной (кратковременной) работы по приему и отправке служебной электронной почты.
- Не следует сообщать посторонним лицам номера телефонов модемного пула.

Обязанности системных администраторов

1. Администрирование научно-информационной сети:

- регистрация пользователей, сетевых элементов и серверов;
- управление сетью: распределение IP-адресов, конфигурирование маршрутизаторов и т.д.;
- управление доменом: распределение почтовых адресов, сопровождение DNS и т.д.;
- обеспечение доступа в сеть, обеспечение защищенного Internet-доступа;
- локализация и устранение ошибок в работе сети;
- ответственность за функционирование сетевых узлов;
- контроль состояния сети.

2. Администрирование операционных систем:

- установка и сопровождение операционных систем на серверах и компьютерах общего пользования;
- установка и сопровождение операционных систем на компьютерах, сопровождаемых отделом информатики (библиотека, редакционная группа, и т.д.).
Примечание: администраторы не несут ответственности за ПО, установленное пользователями.

3. Администрирование электронной почты:

- обеспечение сервиса электронной почты в сети SAONet;
- обеспечение сервиса проверки электронной почты на наличие вирусов и списков несанкционированной рассылки (SPAM) при наличии соответствующего лицензионного ПО;
- участие в решении проблем функционирования электронной почты пользователей.

4. Администрирование приложений:

- установка и сопровождение MAIL-сервера, NEWS-сервера, FTP-сервера, WEB-сервера, NTP-сервера и др.;
- сопровождение серверов баз данных;
- сопровождение штатных прикладных программ на компьютерах общего пользования.

5. Консультации пользователей:

- обеспечение консультаций по email и телефону в рабочее время;
- размещение инструкций и руководств на странице Обсерватории.