

# Институт по Физика на Твърдото тяло

## Научен съвет

### Извадка от ПРОТОКОЛ № 32

От заседание проведено на 24. 03. 2005г.

Състояние на кворума:

Списъчен състав	- 15 души
Редуциран състав	- 15 души
Необходим кворум по ЗНСЗ	- 10 души
Присъстват	- 14 души

#### По точка ПЕТА

Ст.н.с.М.Митов представи Правилник за ползване на компютърните ресурси в постоянните научни звена (ПНЗ) на БАН.

Беше обърнато специално внимание на т.9, в която се казва, че за да не се затруднява ползването на тези ресурси от другите потребители се забранява достъпът до:

- а) сайтове за музика;
  - б) сайтове за филми;
  - в) еротични сайтове от всякакъв вид
- Потребителят на електронна поща е длъжен:

. Да не изпраща e-mail бомби – писма, адресирани до хиляди индивидуални получатели. За тази цел би трябвало да се използват официално обявените пощенски списъци.

. Да не изпраща e-mail SPAM нежелани от получателите писма, най-често с рекламно съдържание.

. Да не изпраща верижни писма, подканящи получателите да ги препращат на множество други получатели.

. Да не изпраща писма с фалшифицирани адреси и /или съдържание.


. Да не изпраща писма с обидно и/или оскърбително съдържание.

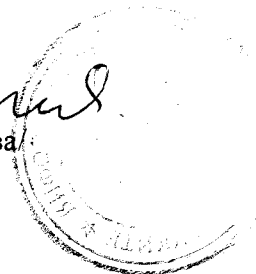
Компютърните ресурси на ПНЗ на БАН трябва да се използват в духа на допълнителните правила за ползване, определени от отговорниците на съответните услуги, списъкът на които се намира на адрес:

<http://www.XYZ.bas.bg/network/rules/>

Правилникът е приет от Ръководството на БАН на заседание от 01.03.05 – Протокол №9 т.8.

Вярно с оригинала.

Секретар на НС:   
/ст.н.с.С.Александрова/



№ 10-00-10  
222  
Получено на 09.03.05г.



# БЪЛГАРСКА АКАДЕМИЯ НА НАУКИТЕ

1040-София, ул. "15 ноември" № 1 ☎ 981-66-22 телекс 22424 факс 981-66-29

Главен научен секретар

г-н г-жа М. Митов  
за доклад на НС.

91-00-10  
08 03-2005

ДО

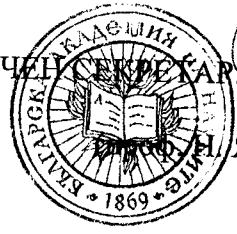
ДИРЕКТОРА  
НА .....

На заседанието си от 01.03.2005 г., Протокол № 9, т.8 във връзка с ограничаване на неправомерното използване на компютърните и комуникационни ресурси на БАН, Ръководството реши:

Считано от 10.03.2005 г. всички звена на БАН са длъжни да спазват приложения Правилник за ползване на компютърните ресурси. Отговорни за изпълнението на Заповедта са директорите.

**Приложение:** Правилник за ползване на компютърните ресурси на БАН.

ГЛ. НАУЧЕН СЕКРЕТАР



(Н. ЯКИМОВ)

# Правилник за ползване на компютърните ресурси в постоянните научни звена (ПНЗ) на БАН

Употребата на компютрите и мрежите в ПНЗ на БАН, както и свързаните с тях услуги като електронна поща (e-mail), се управляват от „Правилника за ползване на компютърните ресурси“ (ППКР). Документът ППКР описва принципите и правилата, които се прилагат при ползването на компютърните ресурси в ПНЗ на БАН.

Освен него, за отделните услуги е предвидено да могат да се формулират „Допълнителни правила за ползване“ (ДПП). Тези правила са специфични за всяка от тези услуги и са необходими за поддържането им на ниво, приемливо за потребителите. Допълнителните правила се формулират от отговорниците на съответните услуги или ресурси и се одобряват от Ръководителя на ОтделКомпМрежа към ПНЗ на БАН.

Основният документ ППКР, както и отделните ДПП, могат да бъдат прочетени при проследяване на връзките към други страници, намиращи се в следната таблица:

## Правила за ползване на компютърните ресурси

Заглавие		Дата на модификация
Правилник	(ППКР)	дд.мм.2005 г.
Общи правила за всички услуги	(ДПП1)	дд.мм.2005 г.
Е-mail услуги	(ДПП2)	дд.мм.2005 г.
Използване на мрежата и Интернет	(ДПП3)	дд.мм.2005 г.
Файлови услуги	(ДПП4)	дд.мм.2005 г.

**Забележка:** Като изходна база, за тази нормативна уредба, са използвани съответните документи на "CERN – Organisation Européenne pour la Recherche Nucléaire / Laboratoire Européenne pour la Physique des Particules – Genève, Suisse" и на Института за ядрени изследвания и ядрена енергетика (ИЯИЯЕ) – БАН.



## Правилник за ползване на компютърните ресурси

Постановките в този документ са приети на Научен съвет на ПНЗ на БАН, на дд.мм.2005 год.

Този документ се отнася както до служителите на ПНЗ на БАН, така и до външните потребители на компютърни ресурси, функциониращи в ПНЗ на БАН.

С цел да се постигне по-прегледно изложение, този документ е записан при употреба само на мъжки род. Този подход не ограничава приложението му, а мъжкият род следва да се разбира като отнасящ се и за двата пола. Поради това постановките в този документ се прилагат както за мъже, така и за жени, освен ако обратното не е изрично указано.

### Ползване на компютърните ресурси в ПНЗ на БАН

#### I. Въведение

1. Този документ определя правилата за използване на компютърните ресурси чрез компютърната мрежа на ПНЗ на БАН.
2. За целите на този документ, терминът „компютърни ресурси“ включва:
  - а) всички персонални компютри (PC), работни станции (work-station) и периферни системи, например принтери, които са свързани (директно или индиректно), към мрежата на ПНЗ на БАН, включително и комуникационната мрежа;
  - б) всички други компютри и местни или отдалечени мрежи, които са частично или изцяло финансирани от ПНЗ на БАН;
  - в) всички обслужващи процеси (services), програмни библиотеки, приложения или друг софтуер, документация или услуги по поддръжка, изпълняващи се на (или отнасящи се до) компютрите и мрежите, посочени по-горе, както и електронната поща и всички Интернет услуги, поддържани от компютърни ресурси на ПНЗ на БАН.
3. За целите на този документ, терминът „потребител“ (user) означава всяко лице, което използва (употребява) компютърни ресурси на ПНЗ на БАН.
4. ОтделКомпМрежа има правото и задължението да планира, проектира, изгражда, поддържа и контролира комуникационните и компютърните мрежи на ПНЗ на БАН, в частност, да инсталира, настройва и поддържа функционирането на общоинститутските компютърни услуги.
5. За целите на този документ, терминът „отговорник“ (administrator) означава лице, което ръководи (управлява) функционирането на компютърни ресурси на ПНЗ на БАН:
  - а) отговорник по компютърна сигурност в ПНЗ на БАН е Ръководителят на ОтделКомпМрежа;
  - б) отговорниците на съответните услуги в ПНЗ на БАН се определят от Ръководителя на ОтделКомпМрежа;
  - в) отговорниците на други специфични компютърни ресурси в ПНЗ на БАН се определят от Ръководителя на ОтделКомпМрежа, при включването на съответния ресурс в компютърната/комуникационната мрежа на ПНЗ на БАН.
6. Нарушаването на постановките в този документ, в частност, неправилната или злонамерена употреба на компютърни ресурси на ПНЗ на БАН, може да накърни компютърната сигурност в ПНЗ на БАН, да причини материални щети на ПНЗ на БАН, както и да предизвика сериозни проблеми на потребителите на тези ресурси, причинявайки им неимуществени или имуществени вреди.

## II. Основни принципи

7. Разрешението да се използват компютърните ресурси на ПНЗ на БАН се дава или отнема от Директора на ПНЗ на БАН или упълномощено от него лице.
8. Компютърните ресурси на ПНЗ на БАН са предназначени за изпълнението на задачите и постигането на целите на ПНЗ на БАН. Тяхната употреба трябва да се вменява в професионалните задължения на съответния потребител, както е предвидено в структурата на ПНЗ на БАН.
9. Използването на компютърните и комуникационни ресурси на ПНЗ на БАН не трябва да влошава или прекъсва тяхното функциониране, както и да не затруднява използването на тези ресурси от другите потребители, а така също и да не причинява морални или материални щети на звеното. За тази се забранява достъпът до:
  - а) сайтове за музика;
  - б) сайтове за филми;
  - в) еротични сайтове от всякакъв вид;както и други сайтове по преценка на директора на звеното.
10. Компютърните ресурси на ПНЗ на БАН трябва да се използват в духа на:
  - а) допълнителните правила за ползване (ДПП), определени от отговорниците на съответните услуги, списъкът на които се намира на следната web-страница: <http://www.XYZ.bas.bg/network/rules/>
  - б) специалните изисквания, които някоя от тези услуги може да наложи във всеки отделен случай.
  - в) ангажиментите, поети от България в рамките на международните проекти GEANT, EGEE и SEE-GRID.
11. Въпреки че ПНЗ на БАН се наема да поддържа и защитава своите компютърни ресурси, тяхното пълноценно функциониране и поверителността на информацията, съхранена на тях, не могат да бъдат напълно гарантирани. Поради това, ПНЗ на БАН не носи отговорност за каквато и да е загуба на информация и каквото и да е нарушаване на поверителността.

## III. Потребителски достъп до акаунти и данни

12. Акаунтите (account), било то с индивидуален или със споделен достъп, могат да бъдат използвани само за целите, за които са били предоставени на потребителя.
13. Всички акаунти трябва да имат подходяща защита на достъпа до тях, като пароли или кодове.
14. Потребителят трябва да предприема необходимите предпазни мерки за защита от неоторизиран достъп до персоналните компютри и работните станции, на които работи. Потребителят трябва да защитава детайлите на личния си акаунт, особено чрез избягване на очевидни пароли, и не трябва да разгласява паролите си на трети страни, освен ако не е изрично упълномощен от своя пряк ръководител, в интерес на изпълняване на служебните задължения. При поискване, от страна на отговорника по компютърна сигурност или отговорника на съответната услуга, потребителят трябва да избере нова парола.
15. Ако на потребителя е бил даден акаунт с привилегирован достъп, във връзка със специфично професионално задължение, той е длъжен да уведоми отговорника на съответната услуга веднага, щом като неговите задължения престанат да изискват този привилегирован достъп.
16. Потребителят е длъжен да опазва поверителността на цялата информация, получена чрез достъп до компютърни ресурси на ПНЗ на БАН, за която с основание може да се очаква, че той разбира природата на нейната поверителност или деликатност.
17. Потребителят не трябва да се опитва да получи неоторизиран достъп до акаунти, които имат защита на достъпа. Той не трябва също така, освен в случаите описани

в т. 20 на този документ, да търси, да разкрива или да се възползва от каквато и да е слабост в сигурността на компютърните ресурси на ПНЗ на БАН или да употребява тези ресурси с цел да търси, да разкрива или да се възползва от каквато и да е слабост в сигурността на други, външни за ПНЗ на БАН, компютърни ресурси.

18. Потребителят е длъжен да съобщава за какъвто и да е неоторизиран достъп до персонални компютри, работни станции или акаунти, с които работи, на отговорника по компютърна сигурност на ПНЗ на БАН или на отговорника на съответната услуга.
19. Потребителят трябва да зачита авторското право и сродните му права, отнасящи се до компютърните ресурси на ПНЗ на БАН, включително софтуерните авторски права. Неспазването на това задължение може да се счита за нарушение на договорите, сключени от ПНЗ на БАН с външни доставчици на компютри, софтуер, мрежи и услуги.

#### **IV. Достъп на трети страни до акаунтите и данните на потребителя**

20. Отговорникът по компютърна сигурност на ПНЗ на БАН, отговорниците на съответните компютърни ресурси и услуги, и всички лица, изрично упълномощени от Директора на ПНЗ на БАН, могат да имат достъп до информацията, съхранявана на компютърните ресурси на ПНЗ на БАН. Този достъп е обект на следните условия:
  - а) гореспоменатите лица не трябва да обменят помежду си придобитата информация, освен ако това не е изрично необходимо за изпълняване на служебните им задължения в ПНЗ на БАН;
  - б) достъпът винаги трябва да е в съответствие с професионалните задължения на гореспоменатите лица и е допустим единствено за:
    - i) решаване на проблеми, засягащи компютърните ресурси на ПНЗ на БАН, включително обновяване или инсталиране на нови ресурси;
    - ii) детектиране на слабости в компютърната сигурност или нарушения на компютърната сигурност;
    - iii) наблюдаване на наличните ресурси за осигуряване на адекватното поведение на компютърните системи в ПНЗ на БАН;
    - iv) разследване, при поискване от страна на отговорника по компютърна сигурност на ПНЗ на БАН или на ръководителя на съответното ПНЗ на БАН, на заподозряно престъпване на правилата в ППКР от даден потребител;
    - v) изменение на достъпа до (или закриване на) акаунти, когато договорът на потребителя с ПНЗ на БАН бъде прекратен, или когато неговите действия станат несъвместими със задачите и целите на ПНЗ на БАН;
    - vi) нормалното функциониране на работната група на даден потребител, когато неговото отсъствие би препятствало сериозно работата ѝ.

#### **V. Отговорност и санкции**

21. От съответния потребител ще се търси отговорност за всяко нарушаване на настоящия правилник.
22. В такива случаи, като общо правило, отговорникът по компютърна сигурност на ПНЗ на БАН, съответният ръководител на ПНЗ на БАН или отговорник на услуга, уведомяват съответния потребител в писмена форма, кое от правилата на настоящия правилник не е било спазено.
23. В случай на поредно неспазване на правилника, след предприемането на мерките описани в т. 22 на този документ, или по всяко време, когато сериозността на нарушението оправдава това, ПНЗ на БАН може да отнеме правото на достъп до компютърните и комуникационни ресурси на ПНЗ на БАН от съответния потребител за период от 1 месец и при следващо нарушение да предприеме дисциплинарни мерки и/или да отнеме изцяло правото на достъп до компютърните и комуникационни ресурси

## Общи правила за всички услуги

### Общо правило

Потребителите на компютърни услуги, предоставяни от ПНЗ на БАН, са длъжни да спазват експлоатационните правила, които са в сила, и инструкциите на отговорниците на услуги или ресурси.

### Санкции

Отговорниците на съответните услуги имат право и са задължени да предприемат всички необходими действия, включително и установяване на определени забрани за достъп, както и отнемане на всяко право на достъп до тези услуги, в случай на несъобразяване с Допълнителните правила за ползване на услуги към Правилника за ползване на компютърните и комуникационни ресурси.

### Процедури

В общия случай, отговорниците на услуги трябва да спазват следните процедури:

- Отговорникът по компютърна сигурност на ПНЗ на БАН, съответният ръководител на ПНЗ на БАН или отговорник на услуга, уведомяват съответният нарушител в писмена форма, кое от правилата на настоящия правилник не е било спазено
- В случай на поредно неспазване на правилника, след предприемането на мерките, описани в по-горе, или по всяко време, когато сериозността на нарушението оправдава това, ПНЗ на БАН може да отнеме правото на достъп до компютърните и комуникационни ресурси на ПНЗ на БАН от съответния потребител за период от 1 месец и при следващо нарушение да предприеме дисциплинарни мерки и/или да отнеме изцяло правото на достъп до компютърните и комуникационни ресурси.



## Е-mail услуги

Когато една услуга се предоставя на множество потребители, поради факта, че тя е споделен ресурс, и за да се поддържа качеството на услугата, определени правила трябва да бъдат налагани принудително. Някои от тях могат да бъдат реализирани чрез автоматични процедури, за да се ограничат злоупотребите. Други от тях могат да бъдат приложени чрез ръчни процедури. Тези правила са в допълнение към правилата, съдържащи се в Правилника за ползване на компютърните ресурси.

### Правила

Потребителят на електронна поща (е-mail услуги) е длъжен:

- Да не изпраща е-mail бомби – писма, адресирани до хиляди индивидуални получатели. За тази цел би трябвало да се използват официално обявените пощенски списъци (mailing lists).
- Да не изпраща е-mail SPAM – нежелани от получателите писма, най-често с рекламно съдържание.
- Да не изпраща верижни писма – писма, подканящи получателите да ги пратят на множество други получатели.
- Да не изпраща писма с фалшифицирани адреси и/или съдържание.
- Да не изпраща писма с обидно и/или оскърбително съдържание.

### Неприкосновеност

Както е указано в Правилника за ползване на компютърните ресурси на ПНЗ на БАН, опитът да се получи достъп до данните на друг потребител се счита за злоупотреба с компютърните ресурси на ПНЗ на БАН. Въпреки това, потребителите на системата за електронна поща трябва да са наясно, че не могат да бъдат дадени гаранции за неприкосновеността на изпращаната поща. Сбъркани или лошо адресирани писма, биха могли да бъдат доставени на грешен получател или да бъдат прочетени от пощенски администратор на друго място по пътя, извън ПНЗ на БАН.

ПНЗ на БАН не дава гаранция за неприкосновеността на електронната поща.

При възникване на нетривиални ситуации, които изискват намеса с цел осигуряване на функционирането на услугата, Директорът на ПНЗ на БАН предоставя на пощенските администратори правото да прихващат и проверяват е-mail съобщенията, във връзка с изпълняването на задълженията им по администриране на услугите за електронна поща.





## Използване на мрежата и Интернет

Мрежата на ПНЗ на БАН се споделя от всички служители на ПНЗ на БАН и другите звена на територията на БАН, а злоупотребата, чрез причиняване на прекалено голям трафик, се отразява на много други потребители и на качеството на услугите. По подобен начин, връзките на ПНЗ на БАН с Интернет са с ограничен капацитет и прекомерната употреба се отразява на качеството на услугите за всички потребители.

Извънредният трафик не е единственият вид нарушение – множество приложения се държат по начин, който излага на риск функционирането на други компютри или елементи от мрежовата инфраструктура. Някои приложения могат да бъдат забранени по други причини, като например, че представляват опасност за сигурността в мрежата. На първо място, могат да бъдат споменати IRC (Internet Relay Chat) сървърите, средствата Back Orifice и NetBus, а така също и P2P (peer-to-peer – като например, Napster).

### Правила

- Отговорниците на мрежовите услуги (мрежовите администратори) да откриват непровомерната употреба на локалната мрежа и на отдалечените връзки, които могат да се отразят на функционирането на услугите. Съответният потребител да бъде информиран.
- Използването на компютърните и комуникационни ресурси на ПНЗ на БАН не трябва да влошава или прекъсва тяхното функциониране, както и да не затруднява използването на тези ресурси от другите потребители, а така също и да не причинява морални или материални щети на звеното. За тази се забранява достъпът до:
  - а) сайтове за музика;
  - б) сайтове за филми;
  - в) еротични сайтове от всякакъв вид;

както и други сайтове по преценка на директора на звеното.

- Отговорникът по компютърна сигурност на ПНЗ на БАН, съответният ръководител на ПНЗ на БАН или отговорник на услуга, уведомяват съответният нарушител в писмена форма, кое от правилата на настоящия правилник не е било спазено
- В случай на поредно неспазване на правилника, след предприемането на мерките, описани в по-горе, или по всяко време, когато сериозността на нарушението оправдава това, ПНЗ на БАН може да отнеме правото на достъп до компютърните и комуникационни ресурси на ПНЗ на БАН от съответния потребител за период от 1 месец и при следващо нарушение да предприеме дисциплинарни мерки и/или да отнеме изцяло правото на достъп до компютърните и комуникационни ресурси.
- Потребителят няма право да преконфигурира каквито и да е елементи от мрежовата инфраструктура на ПНЗ на БАН. Такова право имат единствено мрежовите и системните администратори.

## Файлови услуги

Когато една услуга се предоставя на множество потребители, поради факта, че тя е споделен ресурс, и за да се поддържа качеството на услугата, определени правила трябва да бъдат налагани принудително. Някои от тях могат да бъдат реализирани чрез автоматични процедури, за да се ограничат злоупотребите. Други от тях могат да бъдат приложени чрез ръчни процедури. Тези правила са в допълнение към правилата, съдържащи се в Правилника за ползване на компютърните ресурси.

Централизираните файлови услуги предоставят инфраструктура от файлове и приложения за всички потребители на персонални компютри в ПНЗ на БАН. Като такива, те са податливи на вредно влияние, чрез въвеждане на инфектирани с вируси файлове и чрез потребяване на прекомерен трафик, от страна на неадекватно функциониращи приложения.

### Правила

- Основно изискване е локалните дискове на персоналните компютри, използващи тези услуги, както и централно управляваните файлови системи, да бъдат редовно проверявани за вируси и други известни инструменти за проникване в компютърните системи.
- Потребителят е длъжен да не възпрепятства функционирането на антивирусните програми или други приложения за поддръжка, активирани като част от тази услуга.
- Потребителят е длъжен да действа незабавно за отстраняване на вируси, червеи, троянски коне, задни вратички и други програми или приложения, детектирани от антивирусните или други програми, както и в случаите, когато бъде инструктиран да направи това от мрежовите или системните администратори.

