федеральное государственное бюджетное учреждение
«НОВОСИБИРСКИЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ ПАТОЛОГИИ КРОВООБРАЩЕНИЯ
имени академика Е.Н. Мешалкина»
Министерства здравоохранения Российской Федерации

П Р И К А З

«15»ЯНВ 2014 г. № 5 - ра

г. Новосибирск

«Об утверждении регламентов»

В целях обеспечения бесперебойной работы информационных ресурсов института

ПРИКАЗЫВАЮ:

1. Утвердить Положение о сети передачи данных ФГБУ «ННИИПК им. акад. Е.Н. Мешалкина Минздрава России, Положение об использовании Интернет в ФГБУ ННИИПК им. акад. Е.Н. Мешалкина Минздрава России. Ввести их в действие с момента подписания настоящего приказа.

2. Исполняющему обязанности заведующего канцелярией Туговой С.Ю. ознакомить с настоящим приказом руководителей структурных подразделений института, указанных в приложении 1 настоящему приказу, лично под роспись с предоставлением копии настоящего приказа в срок не позднее 17.01.2014.

3. Начальнику отдела вычислительной техники, программных средств и информационных систем Никитину М.А. разместить Положение о сети передачи данных ФГБУ «ННИИПК им. акад. Е.Н. Мешалкина Минздрава России, Положение об использовании Интернет в ФГБУ ННИИПК им. акад. Е.Н. Мешалкина Минздрава России на сетевом ресурсе, доступном для всех сотрудников института в срок до 17.01.2014.

4. Руководителям структурных подразделений ознакомить работников данных подразделений с Положением о сети передачи данных ФГБУ «ННИИПК им. акад. Е.Н. Мешалкина Минздрава России, Положением об использовании Интернет в ФГБУ ННИИПК им. акад. Е.Н. Мешалкина Минздрава России не позднее 31.01.2014.

5. Контроль за исполнением приказа возложить на заместителя директора по организационно-клинической работе Бойцову И.В.

Директор Института А.М. Караськов

исп. Сурков В.В. т. 55-11.

Федеральное государственное бюджетное учреждение
«Новосибирский научно-исследовательский институт
патологии кровообращения имени академика Е.Н. Мешалкина»
Министерства здравоохранения Российской Федерации

"УТВЕРЖДЕНО"
Приказом № 5 от 15 ЯНВ 2014 г.
Директор ФГБУ «ННИИПК им. акад.
Е.Н. Мешалкина» Минздрава России
_____ Караськов А.М.

Положение
об использовании Интернет в
ФГБУ «ННИИПК им. акад. Е.Н. Мешалкина»
Минздрава России

Новосибирск 2014 г.

Оглавление

1. Перечень сокращений и условных обозначений 3
2. Общие положения 3
3. Организация доступа к информационным ресурсам Интернет 4
4. Ограничения при работе в сети Интернет 4
5. Контроль целевого использования доступа к ресурсам сети Интернет 5
6. Закрытие доступа к сети Интернет 5
7. Ответственность 5
Приложение №1. Перечень заблокированных интернет ресурсов 7
Приложение №2. Список запрещённого контента/типов файла 8

1. Перечень сокращений и условных обозначений

Институт, ННИИПК — федеральное государственное бюджетное учреждение «Научно исследовательский институт патологии кровообращения им. акад. Е.Н. Мешалкина» Минздрава России;
СПД — сеть передачи данных, совокупность оборудования и физических сред передачи данных, находящихся в зоне ответственности ННИИПК;
ServiceDesk — система обработки заявок пользователей на обслуживание информационной инфраструктуры Института;
Администратор СПД — сотрудник отдела вычислительной техники, программных средств и информационных систем ННИИПК, ответственный за обеспечение работоспособности сети передачи данных, подключение к глобальной сети Интернет и защиту информационных ресурсов СПД;
Информационные ресурсы (ИР) — отдельные документы и отдельные массивы документов, базы данных, другие виды информационного обеспечения в информационных системах с использованием персонального компьютера (ПК);
ОВТПСиИС — отдел вычислительной техники, программных средств и информационных систем;
Пользователь — сотрудник ННИИПК, выполняющий свои должностные обязанности с использованием ПК, подключённого к СПД. Требования настоящего положения к пользователю в равной мере распространяются на обучающихся в ННИИПК, использующих ПК, подключенный к СПД;
Логин(login) — имя (идентификатор) учётной записи пользователя в компьютерной системе;
Трафик — объем информации, полученной пользователем из глобальной компьютерной сети Интернет.

2. Общие положения

2.1. Настоящий документ определяет порядок доступа пользователей СПД ННИИПК к информационным ресурсам сети Интернет. В документе установлен порядок взаимодействия подразделений, получающих доступ к сети Интернет с отделом вычислительной техники, программных средств и информационных систем, обеспечивающим данный доступ, определяющим и контролирующим меры по обеспечению информационной безопасности при использовании сотрудниками информационных ресурсов сети Интернет. Регламентируются меры по защите информационных ресурсов ННИИПК и организационные аспекты доступа подразделений к сети Интернет.

2.2. В соответствии с данным документом подразделениям предоставляются следующие виды сервисов Интернет:

- HTTP – доступ к ресурсам сети Интернет для просмотра информации с помощью WEB – браузера, устанавливаемого на компьютере;
- FTP - доступ к ресурсам сети Интернет для копирования на компьютер файлов, предоставленных на FTP - серверах Интернет;
- электронная почта сети Интернет.

Перечисленные сервисы обеспечивают:

- оперативное получение информационно–справочных данных, требуемых для производственной деятельности, в случаях, когда указанная информация недоступна из имеющихся информационных ресурсов ННИИПК;
- информационно-технологическую поддержку пользователей программно-аппаратных медицинских комплексов;
- получение обновлённых версий программного обеспечения с серверов производителей;
- получение обновлений антивирусных баз;

- электронный документооборот с государственными организациями;
- ведение переписки с помощью электронной почты с партнёрами, пациентами и т.п.;

2.3. В случае необходимости использование других сервисов должно быть обосновано конкретными функциональными задачами запрашивающего подразделения и согласовано ОВТПСиИС.

3. Организация доступа к информационным ресурсам Интернет

3.1. Подключение пользователей к сети Интернет производится по заявке на подключение к ресурсам СПД ННИИПК в системе ServiceDesk в соответствие с «Положением о сети передачи данных ФГБУ «ННИИПК им. акад. Е. Н. Мешалкина» Минздрава России от 15.01.2014г. и осуществляется непосредственно с рабочих станций сотрудников.

3.2. Программно-аппаратный комплекс СПД обеспечивает ведение журналов аудита доступа пользователей в сеть Интернет, которые регистрируют информацию о работе сотрудников ННИИПК в сети Интернет за период не менее трёх календарных месяцев. Настройки оборудования СПД обеспечивают возможность фильтрации и блокировки доступа пользователей к сайтам и активному содержимому страниц, опубликованным в сети Интернет и носящим заведомо непроизводственный характер.

3.3. На серверах электронной почты ННИИПК в сети Интернет допускается ведение только почтовых ящиков, закреплённых за конкретными сотрудниками. Почтовые ящики, использование которых носит технологический характер, закрепляются персонально за сотрудниками, выполняющими данные технологические функции.

4. Ограничения при работе в сети Интернет

4.1. Пользователям СПД ННИИПК запрещается:

- передавать через сеть Интернет и опубликовывать в сети служебную информацию ННИИПК, нормативные и регламентные документы ННИИПК. В случае необходимости публикации информации и внутренних нормативных документов в сети Интернет в соответствии с требованиями законодательства, подразделение-инициатор в обязательном порядке согласует данный вопрос с юридическим отделом и отделом общественных связей, передает материалы отделу общественных связей для размещения в сети Интернет. Данное требование не распространяется на размещение в сети Интернет информации и документов в порядке, предусмотренном локальными актами ННИИПК;
- использование имеющегося доступа к сети Интернет в непроизводственных целях
- подключение к публичным почтовым серверам и использование заведённых на них почтовых ящиков для получения, отправки какой-либо информации;
- публикация и обсуждение на форумах в сети Интернет вопросов, касающиеся служебной деятельности, без разрешения руководства ННИИПК;
- подключение к публичным FTP серверам и использование заведённых на них ресурсов для передачи в сеть Интернет любой информации, кроме FTP серверов организаций, с которыми заключены договора, предполагающие подобный документооборот.

4.2. Передача служебной информации, содержащей персональные данные, через Интернет в сторонние организации допускается только в защищённом виде в соответствии с отдельными регламентами, подготовленными ОВТПСиИС совместно с подразделением, осуществляющими такую передачу. При этом криптографическая защита отправляемых данных должна выполняться с использованием сертифицированных криптографических средств.

4.3. По запросам руководителей подразделений администраторами СПД может быть подготовлен отчет, содержащий перечень сайтов, посещаемых сотрудниками подразделения.

4.4. Администратор СПД без предварительного согласования имеет право произвести временную блокировку любой, не технологической учётной записи, в случае если её активность в сети Интернет нарушает проведение технологических работ в СПД.

4.5. Необходимость ограничения на объёмы получаемой из сети Интернет информации (в пределах предоставленных подразделению сервисов и времени доступа) определяется администраторами СПД.

4.6. Администраторы СПД, исходя из загрузки оборудования СПД и линии связи, может изменять время доступа подразделений к сети Интернет, предварительно направив широковещательное сообщение пользователям СПД.

4.7. В целях снижения непроизводительной загрузки оборудования и линий связи, обеспечения антивирусной безопасности СПД, обеспечения исполнительской дисциплины система контроля Интернет-доступа ННИИПК предусматривает следующие автоматические ограничения:

- Блокировка доступа на определённые сайты (Приложение №1).
- Блокировка запрещённого контента/типов файла (Приложение№2).

4.8. Список блокируемых интернет ресурсов контента/типов файла утверждается директором ННИИПК по представлению начальника ОВТПСиИС, исходя из политики безопасности СПД, статистики использования каналов связи и Интернет контента.

Актуальная версия Приложений №1, 2 доступна к просмотру на корпоративном портале.

5. Контроль целевого использования доступа к ресурсам сети Интернет

5.1. Администраторами СПД проводится анализ информационного трафика ("контент-анализ") с целью выявления фактов передачи конфиденциальной информации и доступа к ресурсам непроизводственного характера. Полученные отчеты докладываются директору ННИИПК.

5.2. В случае выявления фактов использования доступа в сеть Интернет в непроизводственных целях администраторы СПД могут инициировать блокировку доступа соответствующего сотрудника к информационным ресурсам Интернет.

6. Закрытие доступа к сети Интернет

6.1. Закрытие или ограничение доступа к сети Интернет для сотрудников осуществляется на основании заявки в Service Desk от руководителя подразделения.

6.2. В заявке на закрытие или ограничение прав доступа к сети Интернет указываются:

- наименование сервиса (HTTP, FTP, Электронная почта), к которому необходимо закрыть (ограничить) доступ;
- основание для закрытия (ограничения) доступа;
- дата, с которой должен быть закрыт (ограничен) доступ.

6.2. Необходимость ограничения объёмов получаемой из сети Интернет информации (в пределах предоставленных подразделению сервисов и времени доступа) определяется администраторами СПД.

7. Ответственность

7.1. Администраторы СПД несут ответственность за работоспособность комплекса программно-аппаратных средств, обеспечивающего доступ к сети Интернет и обеспечивают контроль за выполнением требований настоящего положения.

7.2. Пользователи несут ответственность за использование доступа к ресурсам Интернет в непроизводственных целях, передачу конфиденциальной информации либо информации, содержащей персональные данные через сеть Интернет.

7.3. Руководители подразделений ННИИПК, имеющих доступ к информационным ресурсам Интернет, несут ответственность за соблюдение требований настоящего положения в подчиненных подразделениях.

7.4. Лица, виновные в нарушении настоящих правил, явившемся причиной уничтожения, блокирования или модификации данных ННИИПК, материального ущерба, несут ответственность в соответствии с действующим законодательством.

7.5. Контроль выполнения данного положения возлагается на руководителей подразделений ННИИПК и администраторов СПД ННИИПК.

СОГЛАСОВАНО:

Начальник ОВТПСиИС Никитин М.А.

Начальник юридического отдела Шмыкова А.В.

Разработал:
инженер по информационной
безопасности ОВТПСиИС
Сурков В.В.
Т.55-11.

Приложение №1. Перечень заблокированных интернет ресурсов

100druzei.com
2ip.ru
7ruk.ru
alkashi.org
anonymitychecker.com
anonymizer.ru
antioffice.ru
atlaskit.com
autokadabra.ru
babyblog.ru
beon.ru
blog.ru
blogistan.ru
blogmania.ru
blogonline.ru
blogosphera.ru
blogs.klerk.ru
blogs.mail.ru
blogs.tks.ru
blogus.ru
buhashka.ru
catchup.ru
cd.ru
centurian.org
d3.ru
diary.ru
dirty.ru
dogster.ru
dostupest.ru
dostyp.ru
drom.ru
drugme.ru
dumalka.ru
emoworld.su
facebook.com
fakultet.ru
fion.ru
fishingmap.ru
freeproxy.ru
gamemag.ru
gde-vse.ru
ikra.tv
ilovecinema.ru
inhobby.ru
itblogs.ru
lifestylerepublic.ru
limpa.ru
live.cnews.ru
live.hh.ru
liveindex.ru
liveinternet.ru
livelib.ru
lj.rossia.org
love-ok.ru
mazoo.net
megaperson.ru
mindmix.ru
mirtesen.ru
mmm-tasty.ru
moikrug.ru
moskva.com
my.mail.ru
my-lib.ru
mylivepage.ru
myspace.com
npj.ru
odnoklassniki.ru
oleee.ru
opencoffee.ru
otdihali.ru
planeta.rambler.ru
plus.google.com
posekretu.info
presscom.org
privet.ru
publicproxyservers.com
rb.ru
revision.ru
rusedu.net
ruspace.ru
savemysoul.ru
seeeto.com
sibmama.ru
smspr.ru
sobiraloff.ru
sosedi-online.ru
spaces.ru
spurtup.com
toodoo.ru
tumblr.com
tutvsesvoi.ru
twitter.com
venividi.ru
videogai.ru
vk.com
vnezapno.ru
vsedruzya.ru
webkrug.ru
www.vkontakte.ru
x-libris.net
xroxy.com
yatalent.com
youmama.ru
zabarankoi.ru

Приложение №2. Список запрещённого контента/типов файла

Тип файла	Описание
.0xe	Переименованный файл с вирусом F-Secure
.acr	Скрипт ACRobot
.actm	Макрос AutoCAD
.ahk	Сценарий AutoHotkey
.air	Установочный пакет Adobe AIR
.apk	Пакет приложения Android
.app	Приложение Mac OS X
.app	Приложение FoxPro
.app	Приложение Symbian OS
.asb	Макрос Visual Basic (Alphacam)
.awk	Скрипт AWK
.bat	Пакетный файл MS-DOS
.bin	Исполняемый файл Unix
.cgi	Web-страница, скрипт CGI
.cmd	Пакетный файл Windows
.cof	Исполняемый файл MPLAB COFF
.com	Приложение MS-DOS
.csh	Скрипт C Shell
.cyw	Файл Rbot.CYW Worm
.dek	Пакетный файл Eavesdropper
.dld	Скомпилированная программа EdLog
.dmc	Сценарий Medical Manager
.ds	Источник данных TWAIN
.dxl	Сценарий Rational DOORS
.ebm	Основной макрос EXTRA!
.ecf	Файл компонента SageCRM
.elf	Исполняемый файл Playstation
.elf	Исполняемый файл игры Nintendo Wii
.es	Файл сценария SageCRM
.esh	Расширенный пакетный файл DOS
.ex_	Сжатый исполняемый файл
.ex_	Переименованный исполняемый файл Windows
.ex4	Скомпилированная программа MetaTrader
.exe	Приложение Windows
.exe	Приложение PortableApps.com
.exopc	Приложение ExoPC
.ezs	Протокол пакетного сценария EZ-R
.ezt	Вредоносный червь EZT
.fas	Скомпилированный исходный код Virtual LISP
.fky	Макрос Visual FoxPro
.fpi	Сценарий FPS Creator
.frs	Сценарий Flash Renamer
.fxp	Компилированный код FoxPro
.gadget	Гаджет Windows
.gpe	Видеоигра GP2X
.gpu	Программа (утилита) GP2X
.hms	Скрипт HostMonitor
.hta	Исполняемый HTML-документ
.icd	Защищенная программа SafeDisc

Тип файла	Описание
.iim	Макрос iMacro
.inx	Скомпилированный скрипт
.ipa	Приложение iPhone или iPod Touch
.ipf	Скрипт установки System Management Server
.isu	Сценарий удаления программы (InstallShield)
.jar	Архив Java
.js	Исполняемый скрипт JScript
.jse	Закодированный скрипт JScript
.jsx	Исходный код ExtendScript
.kix	Сценарий KiXtart
.lo	Компилированный исходный код Interleaf
.ls	Сценарий LScript (LightWave)
.m3g	Приложение Mobile 3D Graphics
.mcr	Сценарий 3ds Max
.mel	Сценарий Maya Embedded Language
.mem	Файл макроса
.mio	Приложение MioEngine
.mpx	Компилированная программа-меню FoxPro
.mrc	Сценарий mIRC
.ms	Скрипт 3ds Max
.mst	Сценарий модификации Windows SDK
.mxe	Макрос Macro Express
.obs	Сценарий ObjectScript
.otm	Макрос Microsoft Outlook
.paf	Файл-установщик портативных приложений
.paf.exe	Программа PortableApps.com
.pex	Исполняемый файл ProBoard
.phar	Архив PHP
.pif	Информация о приложении Windows
.plsc	Скрипт Messenger Plus! Live
.plx	Исполняемый файл Perl
.prc	Файл ресурсов Palm
.prg	Файл программы
.prg	Исполняемая программа FoxPro
.ps1	Скрипт Windows PowerShell
.pvd	Скрипт Instalit
.pwc	Установочный пакет PictureTaker
.pyc	Компилированный файл Python
.pyo	Оптимизированный код Python
.qit	Вирус QIT (backdoor.QIT)
.rbx	Скомпилированный скрипт Rembo-C
.rgs	Сценарий операций с реестром Windows
.rox	Исполняемый файл отчета Actuate
.rpj	Файл пакетного процесса Real Pac
.rxe	Исполняемая программа Lego Mindstorms NXT

Тип файла	Описание
.sbs	Сценарий SPSS
.scar	Сценарий SCAR
.scb	Сценарий Scala
.scr	Скрипт
.script	Скрипт
.sct	Скрипт компонента
.shb	Ярлык документа Windows
.shs	Обработчик объектов-фрагментов Windows
.spr	Файл данных FoxPro
.tcp	Скомпилированное приложение (Tally)
.tlb	Библиотека OLE
.tms	Сценарий Telemate
.u3p	Приложение U3 Smart
.udf	Пользовательские функции Microsoft Excel
.upx	Упакованный исполняемый файл Ultimate Packer for eXecutables
.vb	Скрипт VBScript
.vbe	Кодированный исходный код VBScript
.vbs	Скрипт VBScript
.vbscript	Скрипт Visual Basic
.vdo	Файл с возможным вирусом Heathen
.vexe	Исполняемый файл, содержащий вирус
.vlx	Скомпилированный сценарий AutoLISP
.wcm	Макрос WordPerfect
.widget	Виджет Yahoo!
.wiz	Файл мастера Windows (Microsoft Wizard)
.wpk	Макрос WordPerfect
.ws	Исполняемый сценарий Windows
.wsf	Файл сценария Windows
.xap	Файл данных Microsoft Silverlight
.xbap	Web-приложение XAML
.xqt	Макрос SuperCalc
.xys	Сценарий XYplorer
.zl9	Копия заражённого файла приложения (карантин) ZoneAlarm

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
«Новосибирский научно-исследовательский институт
патологии кровообращения имени академика Е.Н. Мешалкина»
Министерства здравоохранения Российской Федерации

"УТВЕРЖДЕНО"
Приказом № 5 от 15 ЯНВ 2014 г.
директор ФГБУ «ННИИПК им. акад.
Е.Н. Мешалкина» Минздрава России
академик РАМН, д.м.н., профессор
_____ Караськов А. М.

Положение о сети передачи данных ФГБУ «ННИИПК им. акад. Е. Н. Мешалкина» Минздрава России

Новосибирск, 2014 г.

Содержание

Перечень сокращений и условных обозначений 2
1. Общие положения 4
2. Структура и состав СПД 4
3. Основные задачи СПД 5
4. Организационные основы функционирования СПД 5
5. Порядок присвоения имён объектам вычислительной техники в СПД 5
6. Порядок подключения рабочих станций к СПД 6
7. Обязанности должностных лиц и пользователей СПД 7
8. Обеспечение информационной безопасности СПД 8
9. Ответственность должностных лиц и пользователей СПД 9
10. Перечень внутренних нормативных документов, которые утрачивают силу с вводом в действие настоящего документа.

Приложение 1. Заявка на доступ к СПД ННИИПК.

Приложение 2. Уголовный кодекс РФ. Глава 28. Преступления в сфере компьютерной информации. 11

Перечень сокращений и условных обозначений

Институт, ННИИПК — федеральное государственное бюджетное учреждение «Научно-исследовательский институт патологии кровообращения им. акад. Е.Н. Мешалкина» Министерства здравоохранения Российской Федерации;

СПД — сеть передачи данных, совокупность оборудования и физических сред передачи данных, находящихся в зоне ответственности ННИИПК;

ServiceDesk — система обработки заявок пользователей на обслуживание информационной инфраструктуры Института;

Информационные ресурсы (ИР) — отдельные документы и отдельные массивы документов, базы данных, другие виды информационного обеспечения в информационных системах с использованием вычислительной техники;

Владелец информационного ресурса (Владелец ИР) – структурное подразделение ННИИПК, реализующее полномочия владения, пользования и распоряжения информацией в соответствии со своими функциями и задачами. Владелец ИР - устанавливает, в пределах своей компетенции, режим и правила обработки, защиты ИР, доступа к ИР, условия копирования и тиражирования ИР (в виде распоряжения на создание информационного ресурса или в виде отдельных регламентов). Владелец добавляет, изменяет, удаляет данные и отвечает за их достоверность и соответствие первичным документам. Владелец информации (информационного ресурса) определяется на этапе создания или передачи информационного ресурса соответствующим распоряжением;

Администратор СПД — сотрудник отдела вычислительной техники, программных средств и информационных систем ННИИПК, ответственный за обеспечение работоспособности сети передачи данных, подключение к глобальной сети Интернет и защиту информационных ресурсов СПД;

ОВТПСиИС — отдел вычислительной техники, программных средств и информационных систем;

Сетевое устройство – любое устройство, подключенное к СПД (персональный компьютер, планшет, ноутбук и т.д.);

Пользователь — сотрудник ННИИПК, выполняющий свои должностные обязанности с использованием любого устройства, подключённого к СПД;

Логин (login) — имя (идентификатор) учётной записи пользователя в компьютерной системе.

Несанкционированный доступ (НСД) - доступ к информации, нарушающий установленные правила разграничения доступа.

Авторизация — предоставление определённому лицу или группе лиц прав на выполнение определённых действий; включая процесс проверки (подтверждения) данных прав при попытке выполнения этих действий.

Аутентификация — проверка, является ли некто тем, за кого себя выдаёт. Подразумевает ввод логина и пароля, но также могут быть использованы и другие средства, такие как использование смарт-карты, отпечатков пальцев и др.

Штатное программное обеспечение - лицензионное программное обеспечение, приобретённое ННИИПК для обеспечения деятельности подразделений. Перечень штатного программного обеспечения размещается администраторами СПД на общедоступном ресурсе сети.

1. Общие положения

1.1. Положение о сети передачи данных ННИИПК является нормативной основой регулирования информационных процессов в сети передачи данных ННИИПК

1.2. СПД ННИИПК представляет собой систему объектов вычислительной техники, содержащих информационные ресурсы ННИИПК, созданную в целях обеспечения медицинской, научной, хозяйственной и других, предусмотренных Уставом Института видов деятельности ННИИПК. СПД является основой единой информационной медицинской, научно-исследовательской и научно-образовательной среды ННИИПК.

1.3. Правовой режим СПД ННИИПК определяется законодательством РФ и иными нормативно-правовыми актами, в частности:

- Гражданским кодексом Российской Федерации;
- Федеральным законом Российской Федерации (далее ФЗ РФ) «О связи» от 07.07.2003 №126-ФЗ;
- ФЗ РФ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 №149-ФЗ;
- ФЗ РФ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» от 19.12.2005 № 160-ФЗ;
- ФЗ РФ «О персональных данных» от 27.07.2006 № 152-ФЗ;
- ФЗ РФ «Об оперативно-розыскной деятельности» от 12.08.1995 №144-ФЗ;
- ФЗ РФ «О безопасности» от 28.12.2010 №390-ФЗ;
- постановлением Правительства Российской Федерации от 17.11.2007 №781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;
- приказом ФСТЭК, ФСБ, Министерства информационных технологий и связи Российской Федерации от 13.02.2008 №55/86/20 «Об утверждении порядка приведения классификации информационных систем персональных данных»;
- Гражданским кодексом РФ, а также нормативно-правовыми актами и организационно-распорядительными документами ННИИПК;

2. Структура и состав СПД

2.1. Физической средой передачи информации в СПД служит структурированная кабельная система корпусов Института, отдельно проложенные кабели и радиочастотные каналы беспроводной сети Wi-Fi. СПД ННИИПК представляет собой среду передачи данных, основанную на стандартах стека сетевых протоколов TCP/IP. Активное коммутационное оборудование СПД, серверы, а также наиболее ответственные рабочие станции питаются от сети гарантированного электроснабжения.

2.2. СПД образуют следующие базовые компоненты оборудования и программного обеспечения (программно-аппаратные ресурсы):

- Центральная группа серверов: файловые сервера, баз данных, приложений, электронной почты, архивные, удалённого доступа, антивирусной защиты и др.
- Дисковые системы хранения данных.
- Телекоммуникационная инфраструктура: оптоволоконные кабели связи, структурированные кабельные системы, сетевое активное оборудование, точки доступа к беспроводной сети Wi-Fi.
- Высокотехнологичное медицинское оборудование.
- Рабочие станции (персональные компьютеры) пользователей.

- Системы бесперебойного питания серверов и рабочих станций.
- Информационная инфраструктура: операционные системы, прикладное программное обеспечение коллективного доступа (медицинские информационные системы, информационно-справочные системы, средства аналитической обработки данных и прочие информационные системы), системы электронного документооборота, программное обеспечение рабочих станций.
- Периферийные устройства (принтеры, сканеры, МФУ и т.д.).

2.3. Логическая структура СПД построена на базе Active Directory компании Microsoft. Авторизация доступа к сетевым ресурсам осуществляется на основе средств Active Directory, при авторизации с помощью других средств используется профилирование прав доступа с привязкой к членству в Active Directory. СПД ННИИПК поддерживает стандартный для IP-сетей информационный сервис:

- доступ к информационным ресурсам в сети Интернет в режиме «online» на базе протоколов HTTP, FTP и др.;
- обмен сообщениями электронной почты (E-mail) через сеть Интернет и внутри СПД ННИИПК.

3. Основные задачи СПД

3.1. СПД ННИИПК предназначена для решения следующих задач:

- обеспечение надежного и эффективного доступа сотрудников к информационным ресурсам ННИИПК;
- обеспечение информационного взаимодействия структурных подразделений, сотрудников и обучающихся в ННИИПК;
- техническое обеспечение работы высокотехнологичного медицинского оборудования;
- создание условий для внедрения новых медицинских, информационных технологий и научных инноваций на основе современных информационных технологий для обеспечения основных направлений деятельности ННИИПК;
- обеспечение эффективности сбора, обработки, хранения, распространения, поиска, передачи и защиты информации;
- обеспечение надежного и эффективного доступа к глобальной сети Интернет;
- поддержка взаимодействия с информационными системами региональных и федеральных органов РФ, включая системы гос. закупок, налоговых органов, казначейства и др.

4. Организационные основы функционирования СПД

4.1. Техническое и организационное управление СПД ННИИПК осуществляет отдел вычислительной техники, программных средств и информационных систем (ОВТПСиИС).

4.2. Порядок управления и администрирования СПД определяется начальником ОВТПСиИС.

4.3. Оперативное управление СПД осуществляют администраторы СПД, которые назначаются приказом по ННИИПК из числа сотрудников ОВТПСиИС.

5. Порядок присвоения имён объектам вычислительной техники в СПД

5.1. Все объекты вычислительной техники в составе СПД должны иметь унифицированное название. Это необходимо для удобства подключения,

переименования, учета и взаимодействия пользователей и специалистов техподдержки ОВТПСиИС.

5.2. Наименование рабочих станций производится по следующему шаблону:

mx****, где:

m - признак мобильности рабочей станции. Используется для ноутбуков, планшетов или иных переносных устройств.

x - кодовое обозначение операционной системы рабочей станции:

a - MS Windows XP

b - MS Windows 7

c - MS Windows 8.1

******** - сквозная четырёхзначная нумерация.

ПРИМЕРЫ: a0001, b0376, mb4956.

Для сохранения преемственности при переименовании, по возможности, сохраняется числовая часть прежнего имени. Сроки перехода на новую систему нумерации устанавливаются руководителем ОВТПСиИС.

5.3. Имена объектам вычислительной техники присваиваются только сотрудниками ОВТПСиИС.

5.4. Сотрудниками ОВТПСиИС ведётся база данных, однозначно определяющая соответствие номера рабочей станции текущему размещению, включая подразделение и помещение Института, где размещена рабочая станция.

5.5. Структура наименования коммутационных узлов, серверов и прочих активных сетевых устройств определяется по аналогичной схеме и устанавливается руководителем ОВТПСиИС. Администраторами серверов из числа сотрудников ОВТПСиИС ведутся паспорта серверов (аппаратные характеристики, установленное программное обеспечение, описание назначения сервера).

6. Порядок подключения рабочих станций к СПД

6.1. Подключение рабочих станций сотрудников производится специалистами ОВТПСиИС на основании заявки на доступ в СПД ННИИПК, созданной руководителем подразделения пользователя в системе ServiceDesk. В заявке указывается подразделение, должность и ФИО сотрудника в именительном падеже, помещение для размещения рабочей станции, необходимость установки принтера для распечатывания информации и служебного телефона.

6.2. Всё программное обеспечение, устанавливаемое на рабочие станции пользователей должно быть лицензионным и включать в себя актуальные обновления производителя. Хранение на компьютере программ для установки нелицензионного программного обеспечения, серийных номеров и генераторов серийных номеров приравнивается к их использованию.

6.3. На основании заявки, сотрудниками группы аппаратно-технической поддержки ОВТПСиИС определяется техническая возможность подключения к СПД в указанном помещении, после чего рабочая станция настраивается и подключается к СПД.

6.4. Все сотрудники ННИИПК, получающие доступ в СПД, проходят аутентификацию по персональному имени (login) и паролю.

6.5. Заявка на доступ для нового пользователя назначается ответственным сотрудником ОВТПСиИС на администратора СПД, из числа сотрудников группы системного администрирования ОВТПСиИС. Сотрудник, для которого устанавливается рабочая станция, должен **лично** пройти первичный инструктаж по правилам работы в СПД, требованиям информационной и антивирусной безопасности, а также получить логин (login) и пароль для доступа к ресурсам СПД. Новому пользователю предоставляется доступ к общедоступным

информационным ресурсам СПД ННИИПК: порталу ННИИПК, электронной почте, общедоступным сетевым ресурсам, рабочим каталогам подразделений, глобальной сети Интернет. При выполнении первого подключения к ресурсам СПД пользователю необходимо выполнить процедуру смены пароля.

6.6. При возникновении проблем, связанных с работой на рабочих станциях, пользователь обязан сделать заявку в систему ServiceDesk, либо по внутреннему телефону **14-99** при невозможности сделать заявку в системе ServiceDesk, для инициирования работ по устранению указанных проблем.

6.7. Любые работы на компьютере, связанные с изменением программной или аппаратной конфигурации компьютера, проводятся специалистами ОВТПСиИС только на основании обоснованной заявки подразделений в ServiceDesk.

7. Обязанности должностных лиц и пользователей СПД

7.1. Администраторы СПД в рамках настоящего Положения обязаны обеспечить в соответствии с утвержденной эксплуатационной документацией:

- работоспособность активного и пассивного оборудования СПД;
- маршрутизацию в сети;
- функционирование базовых функциональных логических сервисов сети;
- проведение инструктажа пользователей правилам работы в СПД и требованиям информационной безопасности.

7.2. Администраторы сети должны обеспечить надежную авторизацию доступа к персональным компьютерам и сетевым сервисам, а также аутентификацию пользователей, получивших доступ в сеть.

7.3. Администраторы СПД несут ответственность за своевременное принятие организационных и технических мер по любым нарушениям настоящего Положения, а также:

- по пресечению попыток несанкционированного доступа к информационным ресурсам Института из внешних сетей и с компьютеров, подключенных к СПД;
- по пресечению доступа и распространения информации, запрещенной действующим законодательством, иными нормами, правилами и требованиями, распространяющимися на пользователей СПД ННИИПК;

7.4. При обнаружении факта нарушения информационной безопасности администратор СПД обязан немедленно принять меры к локализации нарушения, выявлению нарушителя, ограничению/отключению рабочей станции нарушителя от СПД до выяснения всех обстоятельств и получению документального объяснения нарушителя.

7.5. Пользователи СПД должны обладать квалификацией, позволяющей им использовать для выполнения должностных обязанностей необходимые информационные и программные системы. Пользователь, полагающий, что у него не достаточно квалификации для надлежащего выполнения трудовых обязанностей с использованием СПД, обязан обратиться для повышения квалификации к руководителю ОВТПСиИС. В противном случае он лишается права ссылаться на отсутствие квалификации или ее недостаток, как обоснование допущенного нарушения настоящего положения.

7.6. Пользователи СПД обязаны:

- сохранять свой пароль в тайне;
- изменять личный пароль с периодичностью не реже одного раза в три месяца;
- вводить личный пароль и другие учётные данные, убедившись, что клавиатура находится вне поля зрения других лиц;
- перед началом работы убедиться в исправности своей рабочей станции;

- при работе на своей рабочей станции в СПД выполнять **только** служебные задания;
- при сообщениях антивирусных программ о появлении вирусов немедленно сообщить администратору СПД;
- неукоснительно выполнять предписания администратора СПД;
- предоставлять свою рабочую станцию администратору СПД для контроля;

8. Обеспечение информационной безопасности СПД

8.1. К нарушениям информационной безопасности СПД относится:

- деятельность, нарушающая действующее законодательство РФ (гражданское и уголовное);
- несанкционированный доступ к СПД (НСД). НСД определяется как доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных и нештатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами. Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения средств вычислительной техники или автоматизированных систем;
- организация точек доступа в СПД по коммутируемым, выделенным линиям, через фиктивные адреса, трансляцию адресов или транслирующий прокси-сервер, а также с использованием других технических и/или программных средств;
- использование чужих IP адресов, логинов и паролей при работе в СПД;
- передача своего пароля другому лицу. В случае попытки кого-либо узнать пароль пользователь обязан сообщить об этом инженеру по информационной безопасности ННИИПК;
- использование нелицензионного программного обеспечения;
- подключение личных сетевых устройств к СПД (в том числе ноутбуков, карманных компьютеров, смартфонов, телефонов и т.д.), кроме отдельных случаев производственной необходимости, согласованных с ОВТПСиИС;
- использование маршрутизаторов, модемов, рабочих станций и т.д. для подключения других компьютеров или удаленного доступа к СПД сетевых устройств;
- доступ к компьютерам, данным и программам лиц, не имеющих на это права;
- уничтожение (или фальсификация) данных и программ без разрешения их собственника;
- незапланированная и необоснованная производственной необходимостью загрузка СПД;
- передача по сети информации, оскорбляющей честь и достоинство других пользователей СПД, содержащую призывы к насилию, свержению существующего строя, разжиганию межнациональной розни, а также передача за рубеж информации, которая в соответствии с законами РФ не подлежит распространению;
- фиксация учётных данных (пароли, идентификаторы, имена входа и др.) на бумажных или иных твердотельных носителях, расположенных в общедоступных местах (в т.ч. рабочий стол, монитор, системный блок и т. д.);
- работа незарегистрированных пользователей на компьютере, подключенном к СПД;
- выполнение действий и команд, результаты и последствия которых пользователю не известны;

- запуск на рабочей станции любых системных или прикладных программ, не входящие в состав штатного программного обеспечения ННИИПК;
- запуск игровых программ на рабочих станция в т.ч. с выходом в Интернет;
- самостоятельная настройка свойств и параметров безопасности рабочей станции или приглашение для этой цели сторонних исполнителей.
- самовольное внесение изменения в конструкцию, конфигурацию, размещение рабочих станций сети и другие узлы СПД, в том числе их перемещение;
- оставление своей рабочей станции, подключенной к СПД, без присмотра после «входа в систему». В таких случаях необходимо выполнить процедуру «выхода из системы»;

8.2. Руководители подразделений ННИИПК организуют выполнение требований настоящего регламента сотрудниками подчинённых подразделений.

8.3. Политика защиты информации в СПД ННИИПК разрабатывается администраторами СПД совместно с администраторами прикладного программного обеспечения, в соответствии с действующим законодательством и нормативными актами путем реализации организационных и технических мероприятий.

8.4. Организационные мероприятия включают в себя:

- организацию постоянного контроля соблюдения правил работы в СПД ННИИПК;
- реализация антивирусной политики;
- ограничение доступа сотрудников и посетителей в помещения, в которых установлены серверы и коммутационное оборудование СПД;
- контроль структуры сети и пресечение несанкционированного подключения средств вычислительной техники к СПД;

8.5. Технические мероприятия включают в себя:

- регулярную смену сетевых паролей пользователями;
- настройка контроля сложности пароля;
- антивирусный контроль;
- регулярное резервное копирование информации;
- физическое или логическое выделение сегментов сети, критичных с точки зрения информационной безопасности;
- отслеживание запуска и пресечение использования программного обеспечения, затрудняющего или нарушающего нормальную работоспособность сети, компьютеров в ней, и/или нарушающего безопасность сети;
- логическое выделение средств вычислительной техники и/или групп пользователей, обладающих строгим разграничением доступа к разделяемым устройствам;
- ограничение пропуска сетевых протоколов на маршрутизаторах в соответствии с определенными в утвержденных проектах потребностями отдельных сегментов сети;
- ограничения на возможность подключения персональных компьютеров, не принадлежащих ННИИПК путём создания правил фильтрации по MAC-адресам сетевых карт.

9. Ответственность должностных лиц и пользователей СПД

9.1. Администраторы СПД несут ответственность за:

- нарушение функционирования СПД вследствие некорректного управления маршрутизацией;

- нарушение функционирования СПД вследствие некорректного администрирования домена Active Directory;
- нарушения работы базовых функциональных логических сервисов сети (DNS, почтовой службы и др.);
- несвоевременное уведомление начальника отдела ОВТПСиИС о фактах нарушения информационной и антивирусной безопасности СПД;
- разглашение какой-либо информации пользователей, доступ к которой они получили при выполнении своих обязанностей.

9.2. Пользователи СПД несут ответственность за:
- нарушение установленных правил работы в СПД и требований информационной безопасности;
- все действия, совершенные в СПД и Интернет от их имени;

9.3. Администраторы СПД при выявлении нарушений требований информационной безопасности или правил эксплуатации СПД должны немедленно принять меры к локализации и выявлению нарушителя, ограничению его работы в сети (вплоть до полного отключения), выяснения всех обстоятельств нарушения и получению письменного объяснения от нарушителя, а также незамедлительно информировать руководителя отдела ОВТПСиИС о нарушении.

9.4. В случае нарушения требований информационной безопасности и правил эксплуатации СПД нарушители несут ответственность в соответствии с внутренними нормативными актами Института, настоящим Положением и действующим законодательством Российской Федерации (Приложение 2).

10. Перечень внутренних нормативных документов, которые утрачивают силу с вводом в действие настоящего документа.

1. Регламент доступа к сети передачи данных ННИИПК им. Акад. Е.Н. Мешалкина от 05.05.2012г.

Приложение 1.

Заявка на доступ к СПД ННИИПК
«___» _____ 2014 г.

Ф.И.О.	
Должность	
Подразделение	
№ помещения	
Номер служебного телефона	
Необходимость установки принтера	

Руководитель структурного подразделения Ф.И.О.

Приложение 2. Уголовный кодекс РФ.
Глава 28. Преступления в сфере компьютерной информации.

Статья 272. Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации:
- наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. То же деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности:
- наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо арестом на срок до шести месяцев, либо лишением свободы на тот же срок.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения:
- наказываются штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех

лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок.

4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления:
- наказываются лишением свободы на срок до семи лет.

Примечания. 1. Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

2. Крупным ущербом в статьях настоящей главы признается ущерб, сумма которого превышает один миллион рублей.

Статья 273. Создание, использование и распространение вредоносных компьютерных программ

1. Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации:
- наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

2. Деяния, предусмотренные частью первой настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности:
- наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо лишением свободы на срок до пяти лет со штрафом в размере от ста тысяч до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от двух до трех лет или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления:
- наказываются лишением свободы на срок до семи лет.

Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

1. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-

телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб:
- наказывается штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. Деяние, предусмотренное частью первой настоящей статьи, если оно повлекло тяжкие последствия или создало угрозу их наступления:
- наказывается принудительными работами на срок до пяти лет либо лишением свободы на тот же срок.

Согласовано:

Начальник ОВТПСиИС Никитин М.А.

Начальник юридического отдела Шмыкова А.В.

Разработал:
инженер по информационной безопасности ОВТПСиИС Сурков В.В.