|  |
| --- |
| **SPBRC** |
| Федеральное государственное бюджетное учреждение науки Санкт-Петербургский научный центр Российской академии наук**СПбНЦ РАН** |

|  |  |  |
| --- | --- | --- |
|  |  | **Утверждаю****Заместитель Председателя СПбНЦ РАН****по научной работе (приемка)****\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Говорухин В.П.****«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2021г.** |

**МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ**

**ПО ОРГАНИЗАЦИИ И ИСПОЛЬЗОВАНИЮ КОРПОРАТИВНОЙ ПОЧТЫ В НАУЧНЫХ УЧРЕЖДЕНИЯХ ПОДВЕДОМСТВЕННЫХ МИНОБРНАУКЕ РОССИИ**

**Выпуск 1.**

**Методические рекомендации**

**МР 2.2.4.в.1-2020**

**Санкт-Петербург**

**2020г.**

# Предисловие

1. РАЗРАБОТАНЫ ВПЕРВЫЕ Федеральным бюджетным учреждением науки Санкт-Петербургский научный центр Российской академии наук (СПбНЦ РАН) Николаевым В.А.

2. ВНЕСЕНЫ Отделом Телекоммуникаций СПбНЦ РАН

3. РАЗМЕЩЕНЫ на портале СПбНЦ РАН по адресу <http://spbrc.ru/ru/nir>

# Лист согласования

«**Методические рекомендации по организации и использованию корпоративной почты в научных учреждениях подведомственных Минобрнауки России»**

».

|  |  |  |  |
| --- | --- | --- | --- |
|  | Научный руководитель СПбНЦ РАН |  | Академик РАН В.А. Румянцев |
|  | Руководитель Научно-исследовательского отдела СПбНЦ РАН  |  | Д.э.н. А.Г. Бездудная |
|  | Главный ученый секретарь СПбНЦ РАН |  | Д.и.н. В.А. Попов |
|  |
|  |  |  |  |

Оглавление

[Предисловие 2](#_Toc62654393)

[Лист согласования 3](#_Toc62654394)

[Аннотация 5](#_Toc62654395)

[Термины и определения 6](#_Toc62654396)

[Правила организации деятельности корпоративной почты 7](#_Toc62654397)

[Регламент работы с корпоративной электронной почтой в Учреждении 9](#_Toc62654398)

[1. Общие положения 9](#_Toc62654399)

[2. Правила пользования корпоративной почтой работниками учреждения 9](#_Toc62654400)

[Рекомендации по безопасному использованию электронной почты 11](#_Toc62654401)

[1. Вредоносное программное обеспечение 11](#_Toc62654402)

[2. Подбор пароля 11](#_Toc62654403)

[3. Социальная инженерия, фишинг. 12](#_Toc62654404)

[4. Общий доступ к электронной почте 12](#_Toc62654405)

[5. Перехват пароля по открытым Wi-Fi-сетям 12](#_Toc62654406)

[6. Взлом почтового ящика 13](#_Toc62654407)

[Список литературы 14](#_Toc62654408)

[Приложение 1 15](#_Toc62654409)

[Приложение 2 16](#_Toc62654410)

[Приложение 3 18](#_Toc62654411)

# Аннотация

Настоящий документ определяет рекомендации по организации и использованию корпоративной почты организаций подведомственной Минобрнауки России. Выполнение данных рекомендаций позволит регламентировать работу с электронной почтой в организации, и обеспечит безопасный электронный документооборот в части обмена информацией как внутри организации, так и между внешними адресатами. Данные рекомендации разрабатывались с учетом имеющегося опыта внедрения почтовых сервисов в [академической сети РОКСОН](https://nw.ru/ru)[[7](#_Список_литературы_1)] и с учетом существующей нормативной базы РФ ([Федеральный закон о связи](http://www.consultant.ru/document/cons_doc_LAW_43224/)[[1](#_Список_литературы_1)] и федеральный [закон об информации, информационных технологиях и о защите информации](http://www.consultant.ru/document/cons_doc_LAW_61798/)[[2](#_Список_литературы_1)] ).

 Положения Методических рекомендаций распространяются на все организации подведомственные Минобрнауки и содержат общие правила создания и обслуживания корпоративной почты.

# Термины и определения

|  |  |
| --- | --- |
| Администратор (ы) корпоративной почты | Лицо или группа лиц, ответственных за обслуживание технических и программных средств почтовой системы, ее мониторинг, развитие и надежное функционирование |
| Active Directory | Служба каталогов доменов |
| Антиспам | Автоматическая система сканирования почтовых сообщений на наличие нежелательной рекламной рассылки (спам) |
| Электронная почта | Сетевая служба, построенная на открытых и стандартных протоколах, позволяющая пользователям обмениваться информацией с помощью программно-аппаратного комплекса через локальные и глобальные информационно-телекоммуникационные сети без применения бумажных носителей |
| Электронное почтовое сообщение | Электронное сообщение, формируемое отправителем и предназначенное для передачи получателю через информационно-телекоммуникационные сети. Почтовое сообщение состоит из служебной информации (адрес отправителя, адрес получателя, тема и т.д.), текста сообщения и вложенных файлов (могут отсутствовать). |
| Электронный почтовый ящик/почтовый ящик | Индивидуально названное и закрепленное за конкретным пользователем дисковое пространство на почтовом сервере для получения, использования и хранения почтовых сообщений, поступающих на ассоциированные с этим почтовым ящиком адреса электронной почты |
| Лимит почтового ящика | Ограничение на совокупный объем сообщений, хранящихся в электронном почтовом ящике |
| Электронный почтовый адрес | Обозначение, однозначно идентифицирующее адрес электронного почтового ящика. |
| Почтовый сервер | Информационный сервис, включающий в себя почтовые службы и функции администрирования, а также позволяющий содержать почтовые ящики пользователей, хранить и производить обмен почтовыми сообщениями. |
| Почтовый клиент/клиент электронной почты | Программное обеспечение, предназначенное для написания, хранения, получения и отправки сообщений электронной почты. Различают устанавливаемые на компьютер пользователя почтовые клиенты и Web-клиенты |
| Web-клиент | Почтовый клиент, обеспечивающий доступ к сервису электронной почты через браузер по протоколу https |
| Пользователь | Работник Учреждения, которому предоставлено право пользования корпоративной почтой |
| Спам | Ненужные адресату электронные сообщения, рекламные письма и т. п., рассылаемые по электронной почте |

# Правила организации деятельности корпоративной почты

* 1. Функционирование корпоративной почты обеспечивают отдел телекоммуникаций и отдел кадров.
	2. Отдел телекоммуникаций:
		1. является администратором системы корпоративной почты;
		2. ведет учет адресов, мониторинг пользования корпоративной почтой;
		3. обеспечивает создание, блокирование и ликвидацию адресов;
		4. осуществляет программное сопровождение работы корпоративной почты, устранение ошибок и неисправностей в ее работе.
	3. Отдел кадров:
		1. направляет в отдел телекоммуникаций сведения о необходимости создания, блокирования и ликвидации адресов;
		2. предоставляет работникам Учреждения информацию о реквизитах электронных адресов.
	4. Индивидуальный адрес работника Учреждения создается при приеме на работу в Учреждения, смене работником фамилии, а также по инициативе руководителей организации, руководителей структурных подразделений.
	5. Ликвидация индивидуального адреса работника Учреждения осуществляется при его увольнении, смене им фамилии, а также при систематическом нарушении работником настоящих Правил.
	6. Адреса структурных подразделений создаются при необходимости, по требованию руководителей организации или руководителей соответствующих структурных подразделений.
	7. Ликвидация адресов структурных подразделений осуществляется при ликвидации данных структурных подразделений, их переименовании, реорганизации (если в результате реорганизации изменяется наименование подразделения).
	8. Адреса мероприятий создаются по инициативе работников Учреждения, которым поручено проведение мероприятия.
	9. Адреса мероприятий ликвидируются после окончания осуществления соответствующей деятельности. Срок действия адреса указывается в заявке на его создание.
	10. Заявка с инициативой создания, обоснованием необходимости ликвидации адресов направляется в отдел телекоммуникаций.
	11. Содержимое почтового ящика работника Учреждения может быть проверено администратором системы корпоративной почты без предварительного уведомления работника по требованию непосредственного (вышестоящего) руководителя данного работника.
	12. Отдел телекоммуникаций блокирует доступ к адресам, используемым в системе корпоративной почты, в случаях:
		1. осуществления рассылки писем, содержащих вредоносные программы, спам, информацию, распространение которой запрещено нормативными правовыми актами;
		2. возможности доступа к соответствующим почтовым ящикам третьих лиц;
		3. использования работником корпоративной почты не по назначению;
		4. в иных случаях нарушения настоящих Правил по решению начальника отдела телекоммуникаций.
	13. Администратор системы корпоративной почты в течение рабочего дня направляет уведомление о блокировании адреса его пользователю и руководителю соответствующего структурного подразделения.
	14. Блокирование почтового ящика может быть прекращено администратором системы корпоративной почты при устранении причин блокирования. О прекращении блокирования администратор информирует пользователя и его руководителя посредством электронной почты или телефона.
	15. Отдел кадров совместно с отделом телекоммуникаций следит за актуальностью почтовых адресов сотрудников на сайте **http://домен учреждения /contact**. В случае возникновения кадровых, структурных или иных изменений, затрагивающих работу с почтовыми адресами, отдел кадров сообщает необходимые данные в отдел телекоммуникаций электронным письмом на адрес **admin@домен учреждения** .

Отдел телекоммуникаций не несет ответственности за работу сторонних почтовых серверов. В случае возникновения проблем при отправке почты на сторонние сервера, отдел телекоммуникаций сообщает информацию о проблеме администраторам соответствующей системы (при условиях наличия соответствующей контактной информации).

# Регламент работы с корпоративной электронной почтой в Учреждении

## Общие положения

* 1. Настоящие Правила регулируют порядок пользования работниками Учреждения корпоративной электронной почтой Учреждения (далее - корпоративная почта).
	2. Система корпоративной почты организована в домене **«домен учреждения»**. Использование иных почтовых серверов для внутренней служебной переписки запрещается.
	3. В рамках корпоративной почты используются следующие электронные адреса (далее - адреса):
		1. официальные адреса структурных подразделений и органов управления (далее - адреса структурных подразделений);
		2. индивидуальные адреса работников учреждения;
		3. служебные (технические) адреса, предназначенные для организации определенных видов деятельности (далее - адреса мероприятий).
	4. Система корпоративной почты используется в информационных целях, в том числе в целях оповещения, организации работы, обеспечения внутренних и внешних коммуникаций.
	5. Распоряжения должностных лиц Учреждения, оформленные средствами корпоративной электронной почты имеет такую же юридическую силу как и аналогичные распоряжения в письменной форме.

## Правила пользования корпоративной почтой работниками учреждения

* 1. Работник Учреждения имеет право пользоваться корпоративной почтой при осуществлении своих трудовых обязанностей, в том числе отправлять и получать электронные письма (далее - письма) внутренним и внешним корреспондентам с использованием индивидуального адреса.
	2. Отправление и получение писем с использованием адресов структурных подразделений и адресов мероприятий осуществляется соответственно руководителями данных структурных подразделений и/или другими работниками Учреждения по поручению соответствующего руководителя, ответственного за проведение мероприятия.
	3. Пользование корпоративной почтой осуществляется с помощью программы Thunderbird [[3](#_Список_литературы_1)] (версии 69 или выше) или Web приложения (**https://домен учреждения** ). Объем почтового ящика, выделяемого для каждого пользователя, не ограничен. Размер почтового сообщения ограничен 50 Mb (для внутреннего оборота, при отправке почты на другие почтовые сервера объем почтового сообщения может быть ограничен принимающей стороной, например, до 20 Мб).
	4. Работник Учреждения при подготовке письма должен:
		1. указывать тему письма, соответствующую его содержанию;
		2. при подготовке ответа на письмо, обозначенное какой-либо темой, давать ответ строго по обозначенной теме;
		3. при ответе на письмо сохранять историю переписки, но не более 3-ёх шагов, при этом более новые сообщения должны быть сверху;
		4. в случае, если к письму прилагаются файлы-вложения, указать на данное обстоятельство в основном тексте письма;
		5. в случае отправки вложением редактированного файла в конце названия файла необходимо указать фамилию вносившего изменения и дату последних поправок;
		6. в конце письма разместить свою подпись (фамилию, имя, отчество), указание на свою должность, место работы (структурное подразделение Учреждения), рабочий телефон, включая междугородний код города, адрес корпоративной почты.
	5. Образец оформления письма и инструкции по оформлению автоматической подписи[[4](#_Список_литературы_1)] к письму размещены в приложении к настоящим Правилам. (Приложение 1,2)
	6. Работнику Учреждения запрещается:
		1. использовать корпоративную почту для целей, не связанных с исполнением трудовых обязанностей в Учреждения;
		2. осуществлять массовую рассылку писем внешним адресатам с использованием корпоративной почты, в том числе писем рекламного характера, если данная рассылка не связана с исполнением должностных инструкций или не согласованна с руководством Учреждения;
		3. рассылать письма, содержащие:
			1. конфиденциальную информацию, доступ к которой ограничен федеральным законом, в том числе содержащую государственную тайну, коммерческую тайну, персональные данные граждан в открытом виде (при отсутствии согласия последних), материалы, использование которых нарушает права на результаты интеллектуальной деятельности;
			2. недостоверную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, порочащую деловую репутацию, способствующую разжиганию национальной розни, призывающую к совершению противоправной деятельности и т.п.;
			3. компьютерные коды;
			4. файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования;
			5. программы для осуществления несанкционированного доступа;
			6. серийные номера к программным продуктам и программы для их генерации;
			7. логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в Интернете;
			8. ссылки на вышеуказанную информацию.
		4. без разрешения администраторов системы корпоративной почты (адрес: **admin@домен учреждения**):
			1. использовать адрес корпоративной почты для оформления подписок на почтовые рассылки;
			2. публиковать любые индивидуальные адреса, используемые в рамках корпоративной почты, на общедоступных Интернет-ресурсах;
			3. сообщать пароль доступа к своему почтовому ящику другим лицам.
	7. При систематическом (два и более раза) нарушении запретов, указанных в пункте 6 настоящих Правил, работник Учреждения может быть привлечен к дисциплинарной ответственности.
	8. Работнику Учреждения рекомендуется регулярно (не менее одного раза в течение рабочего дня) проверять поступление почты на свой адрес.
	9. При отправке на сторонние почтовые сервера важной корреспонденции необходимо дополнительно указывать в настройках почтовой программы настройки: уведомление о доставке, уведомление о прочтении. Работник должен самостоятельно проконтролировать процесс доставки такого сообщения и в случае возникновения проблем своевременно проинформировать администраторов системы сообщением на почту: **admin@ домен учреждения** , указав причину обращения, краткое описание проблемы, адреса отправителя и получателя.
	10. При отправке почтовых сообщений внутри организации работник, прежде всего, должен руководствоваться данными в адресной книге на сайте **http://домен учреждения/contact**

# Рекомендации по безопасному использованию электронной почты

Использование электронной почты без соблюдения определенных мер безопасности может угрожать безопасности вашего компьютера и тем самым нанести вред не только вашему пользователю но и Учреждению в целом. Ниже приводятся описание основных угроз и рекомендации по защите от них.

1. Вредоносное программное обеспечение

Письма, приходящие по электронной почте, могут содержать вредоносные файлы или ссылки, ведущие на зараженные сайты [[5](#_Список_литературы_1)]. При открытии такого файла или переходе по ссылке вирус попадает на компьютер пользователя.

Для защиты компьютера от заражения вирусом необходимо:

* установить на компьютер средство антивирусной защиты и регулярно обновлять антивирусные базы,
* регулярно обновлять ОС и ПО, установленные на компьютере,
* не переходить по ссылкам из подозрительных писем,
* не открывать письма с вложениями, полученные от неизвестных отправителей.
1. Подбор пароля

Злоумышленник может попытаться угадать пароль от электронной почты путем перебора наиболее часто встречающихся комбинаций, например 123, qwerty, p@ssw0rd. Пароли, состоящие из фамилии, даты рождения, номера телефона также могут быть легко угаданы. Подобрав пароль, злоумышленник получает полный доступ к почте жертвы.

Чтобы оградить свою электронную почту от рук злоумышленника, рекомендуется:

* Создать сложный пароль
* Менять пароли
* Не хранить пароль на компьютере
* Не использовать основной адрес электронной почты для регистрации на каких-либо ресурсах
* Придумать разные пароли для разных сайтов
* Указать контрольный вопрос и номер телефона для восстановления пароля электронной почты
1. Социальная инженерия, фишинг.

По электронной почте могут приходить письма, якобы от лица администратора соцсети или от сотрудников банка — с просьбой прислать свои логин и пароль, например якобы для восстановления после сбоя базы данных, или с просьбой перейти по ссылке для подтверждения адреса электронной почты. Зачастую, перейдя по ссылке, можно обнаружить запрос на ввод данных (пароля, логина, номера банковской карты и т. п.). При этом страница сайта внешне может быть похожа на ресурс, которым вы привыкли пользоваться (соцсеть, интернет-банкинг). Однако если обратить внимание на адрес такой страницы, то можно заметить, что он незначительно отличается от оригинального, например вместо «о» может стоять «0».

Как только запрашиваемые данные будут введены на такой лжестранице, они сразу же попадут в руки злоумышленника, который сможет воспользоваться ими в своих корыстных целях.

Для того чтобы этого избежать[[6](#_Список_литературы_1)], необходимо руководствоваться несколькими простыми правилами:

* Не отвечайте на письма от неизвестных отправителей
* Не переходите по ссылкам, содержащимся в письмах
* Не сообщайте приватную информацию, запрашиваемую в письмах, приходящих по электронной почте.
1. Общий доступ к электронной почте

Не рекомендуется сообщать пароль от почты кому бы то ни было. Если в какой-то момент вам пришлось предоставить друзьям или коллегам доступ к своему электронному ящику или если у вас возникло подозрение, что кто-то посторонний узнал ваш пароль, — необходимо как можно скорее его сменить.

1. Перехват пароля по открытым Wi-Fi-сетям

При подключении к незащищенным точкам доступа[[8](#_Список_литературы_1)] передаваемые данные не шифруются, поэтому злоумышленник может перехватить их при помощи ноутбука с Wi-Fi-адаптером. Используя специальную программу для «прослушивания», злоумышленник сможет увидеть все данные, передаваемые по такой сети, в частности пароль от электронной почты.

Для того чтобы обезопасить себя от перехвата паролей рекомендуется:

* не пользоваться открытыми Wi-Fi-сетями для доступа к электронной почте, соцсетям и прочим ресурсам, требующим ввода пароля;
* использовать VPN при подключении к открытым точкам доступа Wi-Fi;
* отключить общий доступ к файлам на устройстве.
1. Взлом почтового ящика

Скорее всего, ваш почтовый ящик взломали, если:

* не удается войти в электронную почту (пароль не подходит);
* вам сообщили, что с вашего адреса приходят письма, которых вы не отправляли (или в папке «Отправленные» появились такие подозрительные письма);
* исчезли письма, которых вы не удаляли;
* письма, которых вы не читали, помечены как прочитанные;
* установлен пароль на папку «Входящие».

В этом случае необходимо:

* проверить компьютер на вирусы;
* попробовать восстановить пароль по секретному вопросу, с помощью дополнительного адреса или номера мобильного телефона (если это удастся, нужно немедленно сменить пароль и секретный вопрос);
* обратиться в службу поддержки и сообщить о проблеме.

#

# Список литературы

1. О связи [Текст]: Федеральный закон от 07.07.2003г. № 126-ФЗ (ред. от 08.12.2020) // Собрание законодательства РФ. - 14.07.2003.- № 28.- ст. 2895.
2. Об информации, информационных технологиях и о защите информации [Текст]: Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 08.06.2020) // Собрание законодательства РФ. - 31.07.2006- № 31.- ст. 3448.
3. Возможности Thunderbird [Электронный ресурс]: – Режим доступа: <https://www.thunderbird.net/ru/features/>
4. Подписи в Thunderbird [Электронный ресурс] / Unghost, Harry.– Поддержка Mozilla Thunderbird.– Режим доступа: <https://support.mozilla.org/ru/kb/podpisi>
5. [Ищейнов В.Я.](https://www.combook.ru/authors/%D0%98%D1%89%D0%B5%D0%B9%D0%BD%D0%BE%D0%B2%20%D0%92.%D0%AF./) Информационная безопасность и защита информации: теория и практика [Текст]: учебное пособие / В.Я. Ищейнов. - Москва : ДиректМедиа, 2020. - 272 с.
6. Как защититься от фишинга [Электронный ресурс] / Катерина Кочеткова.– Режим доступа: <https://www.kaspersky.ru/blog/phishing-ten-tips/9744/>
7. Академическая сеть РОКСОН [Электронный ресурс]: – Режим доступа: <https://nw.ru/ru>
8. Опасный Wi-Fi. Как защитить компьютеры и телефоны от взлома [Электронный ресурс] / Ангелина Кречетова . – Режим доступа: <https://www.forbes.ru/tehnologii/351555-opasnyy-wi-fi-kak-zashchitit-kompyutery-i-telefony-ot-vzloma>

# Приложение 1

**ОБРАЗЕЦ оформления электронного письма**

****

Подпись

Тело письма

Адресаты

****

Подпись

Тело письма

Адресаты

# Приложение 2

**Создание автоматической подписи в Thunderbird:**

* 1. В меню нажать на пункт инструменты и выбрать параметры учетной записи (если меню отсутствует, то следует вызвать его щелчком правой кнопки мыши по верхней области окна thunderbird)







* 1. Щелкнуть на название соответствующей учетной записи (выделено полужирным шрифтом)



* 1. Ввести нужный текст подписи в форме «текст подписи» и нажать «Ок».

# Приложение 3

**Создание автоматической подписи в Web-интерфейсе:**

* 1. Выбрать в правом верхнем углу пункт настройки



* 1. В левом появившемся меню выбрать пункт профили



* 1. Выбрать единственный профиль в меню правее



* 1. Создать подпись в форме подписи и нажать сохранить.