|  |
| --- |
| **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 соблюдению пользователями сети РОКСОН правил безопасной работы в сети Интернет, использования Интернет-ресурсов и обмена научной и технической информацией.**

**Выпуск 1.**

**Методические рекомендации**

**МР 2.2.2.в.1-2020**

**Санкт-Петербург**

**2020г.**

# Предисловие

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

2. ВНЕСЕНЫ Сектором междисциплинарных исследований СПбНЦ РАН

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

# Лист согласования

«Методические рекомендации по соблюдению пользователями сети РОКСОН правил безопасной работы в сети Интернет, использования Интернет-ресурсов и обмена научной и технической информацией».

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 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](#_Toc62655094)

[Лист согласования 3](#_Toc62655095)

[Аннотация 5](#_Toc62655096)

[Введение 6](#_Toc62655097)

[Типы угроз в сети интернет 7](#_Toc62655098)

[Принципы безопасности в сети интернет 9](#_Toc62655099)

[Защита пользователей сети РОКСОН от опасного контента в сети интернет 12](#_Toc62655100)

[Ресурсы сети РОКСОН, позволяющие сохранить конфиденциальность и сохранность научной и технической информации 12](#_Toc62655101)

[Список литературы 14](#_Toc62655102)

# Аннотация

Настоящий документ определяет рекомендации по соблюдению пользователями сети РОКСОН правил безопасной работы в сети Интернет, использования Интернет-ресурсов и обмена научной и технической информацией. Положения Методических рекомендаций распространяются на всех пользователей сети РОКСОН и содержат общие правила безопасности в сети Интернет и использования его ресурсов, а также рекомендации, связанные с использованием ресурсов Академической сети РОКСОН для повышения надежности хранения и передачи конфиденциальной информации.

# Введение

Основополагающими документами по информационной безопасности в Российской Федерации (РФ) являются Конституция РФ, Концепция национальной безопасности[[1]](#footnote-1), Доктрина информационной безопасности Российской Федерации[[2]](#footnote-2). В представленных документах описаны общие цели, задачи и основные направления обеспечения информационной безопасности и защиты информации. Системообразующим документом в области информационной безопасности и защиты информации является Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 8.06.2020) «Об информации, информационных технологиях и о защите информации», определяющий понятия общедоступной информации, ограничения на доступ информации, право на доступ к информации. Следует отметить, что изменения в данный законопроект вносятся регулярно[[3]](#footnote-3), что говорит о постоянном развитии информационной среды в Российской Федерации и важности актуализации нормативно-правовой базы.

Общая безопасность в любой сложной системе определяется самым уязвимым ее элементом. Установив сложную систему контроля доступа для штатных сотрудников организации, но предоставив полный доступ для подрядчиков, выполняющих уборку помещений, можно открыть двери для доступа злоумышленников к конфиденциальной информации. При обеспечении информационной безопасности в организации ключевую роль играет человеческий фактор, именно сотрудники организации часто являются слабым звеном в защите своих информационных активов. В научных учреждениях также неподготовленность пользователей к существующим угрозам, а не уязвимости в различных программных пакетах, приводит к утечке важной информации или повреждению оборудования.

Данные методические рекомендации будут полезны всем пользователям сети РОКСОН, так как содержат типы угроз, с которыми можно столкнуться в сети интернет, принципы безопасности при работе в интернете, информацию о защите пользователей в сети РОКСОН и её сервисах, способных снизить риск потери и утечки научной и технической информации.

# Типы угроз в сети интернет

1. **Социальная инженерия.** Способ атаки, при котором не используются технические средства взлома, а применяются психологические методы воздействия на людей для получения нужной информации. Любой пользователь сети уязвим к методам социальной инженерии. Основные пути воздействия: электронная почта, телефон, сервисы мгновенного обмена сообщениями, социальные сети. Методы социальной инженерии не требуют специализированного оборудования и серьезных затрат, обладают высокой эффективностью, поэтому представляют повышенную опасность.
2. **Фишинг.** Один из самых распространенных видов интернет-мошенничества, целью которого является получение доступа к идентификационным данным пользователей (например, логин и пароль) путём проведения массовых рассылок электронных писем, личных сообщений внутри различных сервисов, социальных сетей от имени популярных брендов, администраторов системы, банков, силовых ведомств и др., а также с помощью сайтов полностью копирующих дизайн оригинального. Фишинг близок к социальной инженерии, так как в его основе незнание пользователями сетевой безопасности, также он связан с 3-ей группой - мошенничеством в социальных сетях и электронной почте, так как выуживание данных часто происходит через социальные сети и электронную почту.

Данные представляющие интерес для фишинга:

* паспортные и другие персональные данные
* логины и пароли
* коды доступа
* данные для входа в личные кабинеты
* реквизиты банковских карт или счетов
* личная переписка
* служебная информация
* базы данных
* информация, представляющая государственную или коммерческую тайну

1. **Мошенничество в социальных сетях и электронной почте.** Мошеннические предложения продажи вещей, продукции не надлежащего качества, оказания услуг, сборы денег на «лечение ребенка», «возведение храма», «помощь детскому дому» и др.
2. **Поддельные антивирусы.** Загрузить на компьютер поддельный антивирус можно через рекламу в баннере. Чаще всего пользователей привлекают фразы: обнаружено {произвольное число} угроз, обнаружено {произвольное число} уязвимостей, ваш компьютер заражен. В лучшем случае, поддельный антивирус начинает предлагать платную подписку для удаления несуществующих в системе вирусов, в худшем – начинает передавать данные пользователя на сторонние сервера.
3. **Пиратское программное обеспечение.** Обычно, пиратское ПО не обновляется, содержит в себе вредоносные программы или получило уязвимости вследствие взлома, и представляет опасность для рабочего места пользователя.
4. **Вирусные атаки.** Внешние (например, при интернет серфинге) или внутренние (с других зараженных компьютеров в локальной сети) вирусные атаки приводят к краже или потере данных, утрате контроля над рабочем местом (компьютер может стать частью ботнета[[4]](#footnote-4)) или к перенаправлению производительных мощностей системы на майнинг криптовалюты.
5. **Потенциально опасная реклама.** Рекламные баннеры и прероллы, затрудняющие работу со страницами сайта (перемещаются одновременно с их пролистыванием вниз или вверх). Такая реклама плохо поддаётся закрытию, поскольку иконка крестика тщательно замаскирована. Цель подобной рекламы – заставить пользователя перейти на сайт рекламодателя, в котором представлены товары или услуги сомнительного качества.
6. **Фальшивые магазины.** Могут маскироваться под реально существующие или быть со своим дизайном и названием, но, в итоге, после оплаты товаров в таком магазине, покупатель не получает ничего. Признаки мошеннического магазина:
   1. большие скидки на весь ассортимент
   2. отсутствие контактной информации
   3. отсутствие форм оплаты или оплата через сомнительные сервисы
   4. разделы о деятельности компании либо отсутствуют, либо ненадлежащего форматирования
7. **Уязвимость браузера.** Зачастую атаки злоумышленников производятся с помощью уязвимостей в самих браузерах, их особенностей и дефектов, с помощью которых можно получить контроль над компьютером пользователя, нанести ему вред, украсть информацию или использовать зараженную машину в качестве составной части ботнета.
8. **Кибершпионаж.** Программы-шпионы попадают в компьютер вместе со скачанными из интернета файлами. Чаще всего шпион содержится в архиве с установочными файлами якобы бесплатной программы. Программы-шпионы по степени опасности можно разделить на 3 условных вида:
   1. После загрузки собирает данные поисковых запросов пользователя и формирует набор объявлений для контекстной рекламы.
   2. получает доступ к личным файлам владельца ПК, паролям от аккаунтов в социальных сетях, банковским данным. Вред от таких программ может быть финансовым, при хищении средств с банковского счета, или моральным, например, при публикации личных фотографий, документов в общедоступном месте.
   3. Попадая в компьютер, программа не только похищает данные, но и отключает защитные системы: антивирус, браузерные фильтры и дополнительные утилиты. ПК становится уязвим для более серьёзных угроз.

# Принципы безопасности в сети интернет

При работе в сети интернет следует придерживаться следующих принципов работы:

1. никому не передавать конфиденциальные данные (логин, пароль), в том числе администраторам системы, родственникам, коллегам. *Пример: мошенники часто маскируются под администраторов системы и отправляют email о необходимости прислать им логин и пароль (может использоваться ссылка, где на страничке необходимо будет ввести логин и пароль) для совершения каких-либо действий с учетной записью*
2. использовать сложные пароли, состоящие из букв, цифр и специальных символов. Не включать в пароль слова, известные комбинации, не использовать один пароль для разных порталов, следует избегать повторяющихся много раз подряд букв, цифр и полностью исключить использование паролей по умолчанию. Следует регулярно осуществлять смену паролей, обеспечить их конфиденциальность; *Пример: злоумышленники, при помощи программных средств, пытаются подобрать пароли пользователей. Современные системы защиты блокируют доступ к учетной записи на определенное время после нескольких неправильных попыток ввода пароля, однако при использовании простых паролей «qwerty» или «123456» велика вероятность подбора до блокировки. Также периодически происходят утечки персональных данных с популярных ресурсов сети Интернет, в том числе логинов и паролей. Мошенники покупают подобные базы, пытаются использовать данную комбинацию не только на скомпрометированном ресурсе, но и, например, для входа в банк-клиент.*
3. Использовать в работе лицензионное программное обеспечение с установленными последними обновлениями безопасности; *Пример: нелицензионное программное обеспечение (ПО) часто модифицировано и может содержать вирусы и шпионское программы, что приведет к компрометации узла сети и потере конфиденциальных данных.*
4. на всех устройствах, должно быть установлено лицензионное антивирусное программное обеспечение с актуальными обновлениями; *Пример: Антивирусное программное обеспечение позволяет выявлять и предотвращать вирусную активность, обновление антивирусной базы должно происходить не реже нескольких раз в неделю для ПК не подключенных к интернету и каждые несколько часов для активных интернет-пользователей.*
5. следует исключить использование общественных беспроводных сетей и устройств для работы с личной информацией и конфиденциальными данными *Пример:* *Используя общественные беспроводные сети, особенно без защиты паролем, нужно понимать, что радиоволны могут перехватываться кем угодно, и данные могут оказаться в руках мошенников.*
6. Следует использовать программные продукты только с официальных сайтов, избегать программное обеспечение, полученное из сомнительных источников (пиринговые и файлообменные сети). Модифицированные программные продукты представляют повышенную опасность. *Пример: загрузка вирусного или шпионского ПО вместе с программным продуктом, или встроенное в пакет вредоносная программа.*
7. Следует избегать ресурсов с сомнительной репутацией, если существует необходимость посетить подозрительный сайт, то перед переходом следует проверить ссылку на сайте DrWeb <https://vms.drweb.ru/online/> (или другом подобном сервисе) на наличие вирусов и переадресации. *Пример: При переходе по ссылке загружается вирусное ПО в кэш браузера.*
8. личную информацию вводить только при безопасном соединении (URL веб-сайт должен начинаться с «https://», в интерфейсе браузера должна появиться иконка замка); *Пример: Данные по протоколу http передаются без шифрования. Если вы вводите логин и пароль на сайте открытом по http, то на промежуточных узлах связи (маршрутизаторах или коммутаторах) можно легко их перехватить, достаточно только иметь доступ к оборудованию.*
9. выполнять резервное копирование важной информации. При этом использование локальных хранилищ, сетевых папок или дисков без дополнительного резервирования на backup-сервер не гарантирует сохранность информации. *Пример: Существует вирус шифровальщик, который шифрует файлы, используя ассиметричные алгоритмы шифрования, с расширениями: doc, docx, ppt, pptx, xls, xlsx, pdf, jpg и другие в любом хранилище, доступном ПК. Расшифровка данных после подобной атаки, при современных мощностях, может достигать 4-ех лет. Обычно, мошенники предлагают жертве купить кодовую фразу для расшифровки за биткоины.* *Если Вы подверглись атаке вируса шифровальщика и у Вас нет резервной копии данных - не спешите переводить деньги мошенникам, существует полезный сервис от производителя антивируса DrWeb, который поможет восстановить зашифрованные файлы:* <https://support.drweb.ru/new/free_unlocker/for_decode/>
10. всегда проверять правильность написания доменного имени сайта, особенно перед вводом логина и пароля в форме. *Пример: Мошенники часто выбирают доменные имена похожие на название банков, чтобы пользователь попадал на подложную страницу при ошибке ввода адреса или чтобы вызывать меньше подозрений при переходе по мошеннической ссылке, например, sberbak.ru. Чтобы повысить безопасность, многие банки стали использовать в онлайн-банках EV (Extended Validation) ssl-сертификаты[[5]](#footnote-5). Чтобы получить данный сертификат нужно быть юридическим лицом, также проверяется владение доменом, сама компания. Для проверки требуются нотариально заверенные переводы документов на английский язык, а также подтверждения данных третьей стороной. В результате в окне браузера появляется изображение зеленого замочка и название организации зеленым текстом, что гарантировано означает, что Вы попали на сайт компании.*



# Защита пользователей сети РОКСОН от опасного контента в сети интернет

В соответствии с 149-ФЗ оператор связи обязан ограничивать доступ к ресурсам в сети интернет, попавшим в "ЕДИНЫЙ РЕЕСТР доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой запрещено в Российской Федерации (http://eais.rkn.gov.ru/), либо в "Федеральный список экстремистских материалов" Минюста РФ (http://minjust.ru/ru/extremist-materials).

В целях выполнения закона, постановлений правительства и распоряжений Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций в сети РОКСОН был развёрнут программно-аппаратный комплекс, осуществляющий анализ трафика пользователей сети (DPI) и фильтрацию обращений к запрещённым ресурсам.

В основе комплекса сервер Supermicro на базе CPU Intel Xeon E3-1240v5 со специализированной сетевой картой Silicom PE2G6BPI35, поддерживающей режимы работы TAP и Bypass, и ПО Фильтр трафика Carbon Reductor DPI (<https://www.carbonsoft.ru/products/carbon-reductor/>). Комплекс способен обрабатывать трафик на канале ёмкостью до 3 Гбит/с.

# Ресурсы сети РОКСОН, позволяющие сохранить конфиденциальность и сохранность научной и технической информации

В настоящее время невозможно представить себе научную организацию, сотрудники которой не использовали бы электронную почту. Для пользователей сети РОКСОН существует возможность организации корпоративной электронной почты на базе почтового сервера академической сети mail.nw.ru.

Для обеспечения высокой стабильности и производительности в электронной почте РОКСОН используется почтовый сервер postfix в связке с агентом доставки dovecot.

Почта в домене mail.nw.ru проходит антивирусную фильтрацию средствами clamav и спам-фильтрацию системой spamassassin. Конфиденциальность содержимого при передаче письма обеспечивается шифрованным соединением.

Веб-интерфес roundcube поддерживает работу с планшетными компьютерами и смартфонами, делает работу с почтой безопасной и удобной.

При обмене деловой информацией рекомендуется всегда использовать корпоративную почту. Ее использование позволяет сохранить конфиденциальность данных, организовать необходимый уровень их защиты, оперативно получить техническую поддержку.

Для обмена файлами большого объема можно использовать облачное хранилище академической сети РОКСОН (owncloud2.nw.ru) на базе owncloud 10. Owncloud – это свободная и открытая платформа, распространяемая под лицензией AGPL v3.0, для синхронизации данных и общего доступа к файлам. Платформа установлена на одном из виртуальных серверов РОКСОН и обмен данными происходит исключительно между клиентским приложением пользователя и серверным ПО, что существенно снижает риск утечки данных.

# Список литературы

1. С. А. Нестеров «Основы информационной безопасности. Учебное пособие» (2016)
2. А.А. Бирюков "Информационная безопасность: защита и нападение" 2-е изд. (2017)
3. Ю.А. Родичев "Нормативная база и стандарты в области информационной безопасности" (2017)
4. <https://мвд.рф/вопросы/внимание-мошенники/безопасность-в-сети-интернет>
5. <https://www.nic.ru/info/blog/fishprot/?ipartner=4444&adv_id=180920blog_usl_fz_ban&utm_source=sbscr&utm_medium=ban&utm_campaign=180920blog_usl_fz>
6. <https://securelist.ru/spam-and-phishing-in-q1-2020/96806/>
7. <https://www.avast.ru/c-botnet>
8. <https://safe-surf.ru/upload/common/UserSecurityGuidance2017.pdf>
9. <https://hackware.ru/?p=7441>
10. <https://habr.com/ru/company/tuthost/blog/150433/>
11. <https://yandex.ru/turbo/internet-technologies.ru/s/articles/newbie/ugrozy-interneta.html>
12. <https://www.saferunet.ru/expert/article/829/>
13. <https://www.gsconto.com/ru/blogs/post/417/Moshennichestvo.-Falshivye-internet-magaziny>
14. <https://owncloud.com/>
15. <https://roundcube.net/>
16. <http://www.postfix.org/>
17. <https://www.dovecot.org/>

1. Указ Президента РФ от 17.12.1997 N 1300 (ред. от 10.01.2000) "Об утверждении Концепции национальной безопасности Российской Федерации" [↑](#footnote-ref-1)
2. Указ Президента РФ от 5 декабря 2016 г. № 646 “Об утверждении Доктрины информационной безопасности Российской Федерации” [↑](#footnote-ref-2)
3. 27 июля 2010 г., 6 апреля, 21 июля 2011 г., 28 июля 2012 г., 5 апреля, 7 июня, 2 июля, 28 декабря 2013 г., 5 мая, 21 июля, 24 ноября, 31 декабря 2014 г., 29 июня, 13 июля 2015 г., 23 июня, 3 июля, 19 декабря 2016 г., 1 мая, 7, 18 июня, 1, 29 июля, 25 ноября, 31 декабря 2017 г., 23 апреля, 29 июня, 19 июля, 28 ноября, 18 декабря 2018 г., 18 марта, 1 мая, 2, 27 декабря 2019 г., 3 апреля, 8 июня 2020 г. [↑](#footnote-ref-3)
4. Ботнет представляет из себя сеть компьютеров, которые инфицированы вредоносным ПО, позволяющим злоумышленникам осуществлять удаленный контроль за ними, рассылать спам-сообщения и вирусы, служить местом размещения ПО, осуществляющего DDoS-атаки - и все это без ведома настоящих хозяев компьютеров. [↑](#footnote-ref-4)
5. SSL — это сокращение от Secure Socket Layer — это стандартная интернет технология безопасности, которая используется, чтобы обеспечить зашифрованное соединение между веб-сервером (сайтом) и браузером. SSL сертификат позволяет использовать https протокол. Самый простой способ получить ssl-сертификат - сгенерировать прямо на веб-сервере. Однако, тогда в браузере появится надпись «Сертификат безопасности не является доверенным.» Это означает, что шифрованное соединение будет установлено, но не факт, что владелец сайта, является владельцем домена и, при возникновении такой надписи, возможно, мы имеем дело с сайтом-обманкой. Для того, чтобы такой надписи не возникало владельцы сайта не генерируют сертификат сами, а получают его в доверенных центрах сертификации, где производятся различные проверки от владения доменом (физического или юридического лица) до, в случае получения более высокого по статусу сертификата, проверки надежности юридического лица получающего сертификат. [↑](#footnote-ref-5)