# Памятка по информационной безопасности для сотрудников федерального государственного бюджетного образовательного учреждения высшего образования «Сибирский государственный университет геосистем и технологий»

*(в соответствии с распоряжением «О дополнительных мерах обеспечения комплексной безопасности» от 28 июля 2025 г. № 6/13)*

**1. Парольная защита**

1.1 Никогда не сохраняйте Ваши пароли в программах, в текстовых файлах на компьютере, в браузерах либо на других электронных носителях информации (flash-носителях, внешних жестких дисках и т.п.) в открытом виде. Большинство программ хранят их в открытом виде и тот, кто получит доступ к вашему автоматизированному рабочему месту (персональному служебному компьютеру, ноутбуку, планшету), «автоматически» получит доступ и к ним.

1.2 Не записывайте пароли на листах бумаги, не храните их на листках, приклеенных к монитору и/или расположенных на рабочем столе в свободном доступе. Сохраняйте в тайне личный пароль. Никогда не сообщайте пароль другим лицам, в том числе коллегам.

1.3 Не используйте пароль доступа в локальную сеть в других программах и на сайтах, где требуется регистрация. Не используйте личные пароли (от соцсетей, личной почты и т.п.) для служебных программ (1С, сервер) и наоборот, не используйте служебные пароли для личных целей.

1.4 В случаях обнаружения факта несанкционированного использование Вашего персонального пароля немедленно доложите об этом руководителю начальнику своего структурного подразделения.

1.5 Где это возможно, подключайте дополнительную защиту – двухфакторную аутентификацию. Многие приложения и сервисы давно внедрили в свои системы SMS-коды или мобильные приложения-аутентификаторы, обеспечивающий дополнительный уровень защит. Это значительно усложнит злоумышленникам вход в аккаунт даже при известном пароле.

1.6 При временном оставлении рабочего места в течение рабочего дня в обязательном порядке блокируйте компьютер нажатием комбинации клавиш «Win + L».

**2. Антивирусная защита**

2.1 Если антивирус перестал обновляться или вовсе работать (на иконке антивируса появились восклицательные знаки, крестики или выдаются об этом сообщения на экране), то обязательно об этом сообщите сотруднику ЦТТ. Ни в коем случае не отключайте антивирус!

2.2 Проверяйте внешние носители информации и всегда сканируйте флешки, CD/DVD и другие внешние устройства антивирусом перед использованием. Вставляйте в системный

блок только проверенные USB-накопители. Многие вирусы распространяются через «чужие» носители информации (флешки, CD/DVD диски). Не вставляйте в рабочие станции флешки неизвестные носители информации (подобранные на улице, флешки студентов и т.п.). Старайтесь избегать использование любых внешних устройств.

2.3 Не открывайте вложенные файлы и документы из писем от неизвестных или подозрительных отправителей. В 90% случаев шифровальщики отправляются жертвам в виде спама по электронной почте. Поэтому не открывайте письма от незнакомых адресатов и с подозрительным содержанием. Обычно шифровальщики кочуют по интернету в виде псевдо-pdf (например, счет.pdf.exe, документ.zip). Также, они могут маскироваться под файлы со следующими расширениями:

| Подозрительные (потенциально опасные) расширения файлов | | | | | |
|---|---|---|---|---|---|
| пример.rtf | пример.lnk | пример.chm | пример.vhd | пример.bat | пример.js |

Не переходите по ссылкам, не запускайте программы (расширение файла [*.exe]) и не открывайте файлы, полученные по электронной почте от неизвестного. Если сомневаетесь, уточните наличие вложения у отправителя другим способом (позвоните по горячей линии, личный звонок отправителю, обратитесь в техподдержку и т.п.).

2.4 Внимательно проверяйте разрешение документов, открываемых из почты, даже от доверительных отправителей! Всегда можно позвонить отправителю лично и уточнить, действительно ли это письмо отправлял он!

**3. Защита от фишинга и мошеннических сообщений**

3.1 Не переходите по подозрительным ссылкам, если вы получили письмо (или сообщение), которого не ожидаете, не кликайте по ссылкам в нём. Например, вам якобы пишут из банка или магазина – лучше зайдите на их сайт вручную через браузер или позвоните по официальному номеру. Будьте внимательны к срочным призывам («срочно обновите пароль», «вы выиграли приз», «ваш счёт заблокирован» и т.п.) – это типичные уловки мошенников.

3.2 Проверяйте ссылки в мессенджерах и соцсетях: фишинг может прийти не только по электронной почте, но и в личных сообщениях. Даже если ссылка прислана от знакомого человека, убедитесь, что его аккаунт не взломали. Не нажимайте на неожиданные ссылки в чатах, сообщениях WhatsApp, Telegram, VK, MAX и т.п. – лучше уточните у коллеги лично, не посылал ли он вам это сообщение.

3.3 Если вам в мессенджере (WhatsApp, Telegram, MAX, VK и т.п.) присылают сообщения от имени руководящего состава СГУГиТ, или вас добавляют в чат-группы с руководящим составом, где просят предоставить любую информацию – не поддавайтесь на данные манипуляции! Свяжитесь с реальным руководящим составом, посредством личной встречи или звонка, и уточните, правда ли это они или это действия злоумышленников.

3.4 Не вводите личные данные на сомнительных ресурсах: никаких паролей, номером карт или кодов из SMS нельзя подтверждать через незнакомые сайты или приложения. Никогда не сообщайте коды одноразовой аутентификации по телефону или в ответ на письма – банки и официальные организации этого не просят.

**4. Правила реагирования, если вы стали жертвой злоумышленников или вирусов**

4.1 Не паникуйте! Выключите свой рабочий компьютер и отсоедините интернет-кабель от системного блока. Сообщите о инциденте в ЦТТ по телефону 361-00-19 или +7 (913) 378-65-07.

4.2 Не пытайтесь самостоятельно решить возникшую проблему – обратитесь к уполномоченным, по данным вопросам, коллегам (ЦТТ, аудитория 139).

4.3 Не удаляйте подозрительные письма – отправляйте их в спам или игнорируйте. Если действует преступная группировка мошенников, данные письма понадобятся для дальнейших проверок/расследований.

4.4 Если вам поступил звонок с неизвестного номера, особенно если собеседник требует передать данные о банковских счетах, аккаунтах или просит выполнить какие-либо действия «в целях безопасности», необходимо прекратить разговор. Никогда не сообщайте секретные коды, приходящие от портала «Госуслуги» или других официальных сервисов. Не стоит доверять и ссылкам, которые присылаются через мессенджеры или электронную почту от неизвестных адресантов. Важно помнить: официальные лица никогда не будут запрашивать личные данные по телефону или в каналах мессенджеров без предварительной верификации источника.

4.5 Для защиты от телефонного мошенничества рекомендуется использовать определитель номера (например, Kaspersky Who Calls или бесплатный аналог от Яндекса), а также настроить блокировку нежелательных вызовов в мессенджерах.

**5. Дополнительные рекомендации**

5.1 Для ведения деловой переписки, обмена электронными сообщениями с целью обработки общедоступной информации Вам необходимо использовать корпоративную электронную почту Организации и мессенджер MAX.

5.2 Не размещайте и не обсуждайте в сети Интернет информацию о деятельности Организации, если это не входит в Ваши служебные обязанности (должностные инструкции, положение об структурном подразделении).

5.3 Не принимайте никаких соглашений при посещении сайтов, смысла которых Вы не понимаете, не знаете.

5.4 Соблюдайте «политику чистого стола». Не оставляйте документы, распечатанные материалы, личные дела на своем рабочем месте в момент отсутствия.

5.5 Запрещается самостоятельно устанавливать программное обеспечение, если это не входит в Ваши должностные обязанности. Запрещается запускать программное обеспечение, не относящееся к выполнению Ваших должностных обязанностей.

5.6 Запрещается вносить изменения в конфигурацию автоматизированного рабочего места (персонального служебного компьютера, ноутбука, планшета), а также вносить изменения, препятствовать или ограничивать работоспособность установленных средств защиты информации (антивирусы, межсетевые экраны, системы обнаружения и предотвращения вторжений и др.).

5.7 Избегайте работы с конфиденциальной информацией через открытые Wi-Fi без VPN (например, общедоступные сети Wi-Fi в торговых центрах). Общественные сети могут прослушиваться злоумышленниками.

5.8 Стоит с подозрением относиться к баннерам – картинка на них может не иметь ничего общего с сайтом, на который вас перекинет. Ресурсы, где размещены баннеры, как правило, не могут контролировать, что именно увидит и куда перейдет пользователь. Так что даже с вполне респектабельного сайта по баннеру вы можете перейти на фишинговую страницу или куда похуже.

5.9 Не подключайте к системному блоку рабочего автоматизированного места (АРМ) сторонние устройства. Не используйте АРМ как способ зарядки батарее Ваших личных устройств (телефонов, power-банков, гарнитур и т.п.).

5.10 Для получения дополнительной информации рекомендуем ознакомиться со следующими интернет-ресурсами и новостными порталами, где приводятся актуальные схемы мошенничества и реальные примеры:

– https://www.sberbank.ru/ru/person/kibrary/articles/top-10-aktualnykh-skhem-moshennichestva;
– https://iz.ru/tag/moshennichestvo;
– https://1prime.ru/moshennichestvo/;
– https://www.gazprombank.ru/pro-finance/safety/novye-skhemy-moshennichestva/;
– https://ndfp.ru/blog/novye-shemy-mosennicestva-v-2025-godu-kak-ne-poterat-dengi-117;

5.11 По всем вопросам, связанным с обеспечением безопасности информации, обращайтесь в ЦТТ:

– 361-00-19 (городской номер);

– 292 (внутренний номер);

– +7 (913) 378-65-07 (мобильный номер);

– аудитория 139 (лабораторный корпус, 1 этаж);

– по почте: support@ssga.ru;

***Пример фишингового письма:***

***Тема****: «Уведомление о блокировке корпоративной почты»*

***От****: «support@sgugit-ru.com» (обратите внимание — домен не наш!)*

***Текст****:*

*«Уважаемый Иванов Иван Иванович! Ваша почта будет заблокирована через 24 часа. Для разблокировки перейдите по ссылке: sgugit-ru.link/update Не отвечайте на это письмо — оно сгенерировано автоматически.»*

***Что не так?***

✗ *Поддельный адрес отправителя (sgugit-ru.com вместо sgugit.ru).*

✗ *Угроза блокировки и срочность.*

✗ *Ссылка ведёт на фейковый сайт (при наведении курсора видно sgugit-ru.link, а не официальный адрес).*

Проректор по ЦТ С.В. Середович

26.08.2025