

УТВЕРЖДЕНА
приказом ФГАОУ ВО «СПбПУ»
от 18.11.2022 № 2634

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

**«САНКТ-ПЕТЕРБУРГСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ПЕТРА
ВЕЛИКОГО»**



ПОЛИТЕХ

Санкт-Петербургский
политехнический университет
Петра Великого

**ИНСТРУКЦИЯ
ПОЛЬЗОВАТЕЛЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ
ФГАОУ ВО «СПбПУ» ПО ОБЕСПЕЧЕНИЮ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Санкт-Петербург
2022 г.

1. Общие положения

1.1. Настоящая Инструкция пользователя информационной системы ФГАОУ ВО «СПбПУ» по обеспечению информационной безопасности (далее – Инструкция) разработана в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», методическими рекомендациями ФСТЭК России от 15.02.2008, утвержденными приказом ФСТЭК России от 05.02.2010 № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных», ГОСТ Р ИСО/МЭК 17799-2015 «Практические правила управления информационной безопасностью» и другими нормативными правовыми актами.

1.2. Настоящий документ определяет основные правила обеспечения информационной безопасности для пользователей информационной системы ФГАОУ ВО «СПбПУ».

1.3. Целью настоящей Инструкции является обеспечение информационной безопасности информационной инфраструктуры ФГАОУ ВО «СПбПУ», включая автоматизированные и телекоммуникационные системы, от внешних и внутренних компьютерных атак, случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи, а также минимизацию рисков информационной безопасности.

1.4. Действие настоящей Инструкции распространяется на работников и студентов ФГАОУ ВО «СПбПУ», использующих информационные системы, сервисы и другие ресурсы ФГАОУ ВО «СПбПУ».

2. Основные термины, сокращения и определения

2.1. АРМ – автоматизированное рабочее место пользователя (персональный компьютер с прикладным программным обеспечением) для выполнения определенной производственной задачи.

2.2. Безопасность информации – состояние защищенности информации, характеризующееся способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность (т.е. сохранение в тайне от субъектов, не имеющих полномочий на ознакомление с ней), целостность и доступность информации при ее обработке техническими средствами.

2.3. Вредоносное ПО – программное обеспечение или изменения в программном обеспечении, приводящие к нарушению конфиденциальности, целостности и доступности критичной информации.

2.4. Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

2.5. Информационная система ФГАОУ ВО «СПбПУ» – совокупность информационных систем, используемых ФГАОУ ВО «СПбПУ».

2.6. ПК – персональный компьютер.

2.7. ПО – программное обеспечение.

2.8. Пользователь – физическое лицо, зарегистрированное в информационной системе ФГАОУ ВО «СПбПУ».

2.9. Служба поддержки пользователей – это служба, в которую пользователи могут обратиться за оказанием технической поддержки по решению возникшей проблемы, а также за получением дополнительной информации по интересующему вопросу (support@spbstu.ru, +7 (812) 535-81-08, <https://it.spbstu.ru>).

2.10. Средства защиты информации – совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, вещных элементов, используемых для решения различных задач по защите информации, а также программы, специально предназначенные для выполнения функций, связанных с защитой информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации.

3. Порядок обеспечения информационной безопасности на персональных компьютерах и автоматизированных рабочих местах

3.1. Использовать лицензионное ПО и своевременно выполнять обновления. В обновленных версиях разработчики ПО исправляют ошибки, которыми злоумышленники могли бы воспользоваться в своих целях. Чем старше версия операционной системы, программы или браузера, тем уязвимее устройство. ФГАОУ ВО «СПбПУ» ежегодно производит закупку лицензионных копий ПО актуальных версий. Для получения лицензионных копий ПО обратитесь в службу поддержки.

3.2. Использовать средства защиты информации, в том числе антивирусы. Персональные компьютеры, на которых отсутствует антивирусная защита, взламывают в среднем в 5,5 раз чаще. ФГАОУ ВО «СПбПУ» ежегодно производит закупку промышленных отечественных средств защиты информации актуальных версий: Kaspersky Total Security и Dr.Web. Для получения средств защиты информации обратитесь в службу технической поддержки.

3.3. Если установленное на компьютере средство защиты информации перестало работать (например, на иконке антивируса появились восклицательные знаки, крестики или на экран выводится сообщение с предупреждением), сообщите об этом в службу поддержки пользователей. Некорректно работающее средство защиты информации не обеспечивает обнаружение вредоносного ПО и предотвращение компьютерных атак.

3.4. Удалять программы и приложения, которыми вы перестали пользоваться или которые больше не поддерживаются разработчиками.

3.5. Не запускать исполняемые файлы на внешних носителях (дисках и картах памяти), полученные не из доверенного источника. С каждым днем все больше распространяются вирусы-вымогатели. Они блокируют устройство и угрожают удалить с него все данные, если вы не заплатите выкуп.

3.6. Создавать резервные копии важной информации на внешних носителях (дисках и картах памяти). Резервные копии, хранящиеся в облаке или на запасном диске, помогут, если устройство все-таки подверглось компьютерной атаке.

3.7. Корректно завершать все активные задачи и блокировать АРМ при необходимости покинуть рабочее место на некоторое время.

3.8. В случае возникновения подозрения на угрозу информационной безопасности необходимо срочно сообщить об этом в службу поддержки пользователей.

3.9. Не вносить изменения в топологию сети путем подключения внешних устройств.

4. Порядок обеспечения информационной безопасности при работе с электронной почтой

4.1. Внимательно проверять адрес отправителя сообщения электронной почты, даже в случае совпадения имени с уже известным контактом.

4.2. Внимательно проверять электронные письма, в которых содержатся призывы к действиям (например, «открой», «прочитай», «ознакомься»), а также с темами про финансы, банки, геополитическую обстановку или угрозы.

4.3. Не переходить по ссылкам, которые содержатся в электронных письмах, особенно если они длинные или наоборот, используют сервисы сокращения ссылок (bit.ly, tinyurl.com и т.д.). Злоумышленники осуществляют массовую рассылку с просьбой перейти по ссылке в

сообщении. После перехода по указанной ссылке может начаться загрузка компьютерного вируса на ваш компьютер, который в дальнейшем зашифрует файловую систему и потребует выкуп для восстановления утраченных данных.

4.4. Не переходить по ссылке из электронного письма, если они заменены на слова, не наводить на них мышкой и просматривать полный адрес сайтов.

4.5. Проверять ссылки, даже если электронное письмо получено от другого пользователя ФГАОУ ВО «СПбПУ».

4.6. Не открывать вложения в электронные письма, особенно если в них содержатся исполняемые файлы, документы с макросами, архивы с паролями, а также файлы с расширениями RTF, LNK, CHM, VHD.

5. Порядок обеспечения информационной безопасности при работе в сети Интернет

5.1. При скачивании файлов из сети Интернет внимательно проверять URL-адрес сайта. Официальные сайты производителей ПО имеют защищенное соединение (https-протокол, значок закрытого замка). Скачивать файлы из неофициальных источников – это большой риск, так как в файл может быть вшито вредоносное ПО.

5.2. Избегать подключения к общедоступным публичным точкам доступа (Wi-Fi без пароля). Такие точки доступа часто используются злоумышленниками для реализации фишинговых атак и компьютерных атак типа «Человек посередине».

5.3. Использовать двухфакторную аутентификацию везде, где это возможно. Данный подход позволяет значительно снизить риски, связанные со слабой парольной политикой и разделенным использованием устройств и аккаунтов.

5.4. Не передавать конфиденциальную информацию по открытым каналам связи.

5.5. Не делиться слишком личной информацией в социальных сетях. Не публикуйте в открытом доступе дату своего рождения, не указывайте свой адрес, местоположение и контакты. Отключите геотеги на фотографиях. Хотя сами по себе такие данные кажутся безобидными, с их помощью злоумышленники могут многое о вас узнать.

6. Порядок создания безопасных паролей

6.1. Длина пароля должна быть не менее 8 символов.

6.2. В числе символов пароля должны присутствовать три из четырех видов символов: буквы в верхнем регистре, буквы в нижнем регистре, цифры, специальные символы (! @ # \$ % ^ & * () - _ + = ~ [] { } | \ : ; ' " < > , . ? /).

6.3. Пароль не должен содержать легко вычисляемые сочетания символов: имена, фамилии, номера телефонов, даты, последовательно расположенные на клавиатуре символы («12345678», «QWERTY», и т.д.), общепринятые сокращения («USER», «TEST» и т.п.).

6.4. При смене пароля значение нового должно отличаться от предыдущего не менее чем в 4 позициях.

6.5. Для различных информационных систем необходимо устанавливать разные пароли (в том случае, если не используется авторизация по единой учетной записи ФГАОУ ВО «СПбПУ»).

6.6. Не сообщать свой пароль кому-либо.

6.7. Не указывать пароль в сообщениях электронной почты.

6.8. Не хранить пароли, записанные на бумаге, в легко доступном месте.

6.9. Не использовать тот же самый пароль, что и для других систем (например, домашний интернет-провайдер, форумы и т.п.).

6.10. В случае подозрения на то, что пароль стал кому-либо известен, необходимо поменять пароль и сообщить о факте компрометации в службу поддержки пользователей.