

**Информация о мерах  
обеспечения кибергигиены, которым рекомендуется следовать при  
использовании веб-приложения**

г. Алматы  
2023 год

## **Общие положения**

1. Настоящий документ имеет рекомендательный характер. Пользователям рекомендуется ознакомиться с документом для исключения негативных ситуаций, связанных с информационной безопасностью, мошенничеством и иными инцидентами.

2. Пользователю необходимо:

- при обнаружении мошеннических действий, инцидентов информационной безопасности, отклонений в нормальной работе веб-приложения, затрудняющих эксплуатацию ПК, необходимо обращаться по контактам, указанным в веб-приложении.
- обеспечить сохранность персональных данных, банковских сведений, сведений об аутентификации и иной конфиденциальной информации.
- использовать только проверенные устройства и сеть Wi-Fi.
- использовать на устройствах только проверенное программное обеспечение (установленное из официальных источников), регулярно обновлять программное обеспечение.
- использовать сложные пароли и следовать рекомендациям парольной политики.

### **Пользователям категорически не рекомендуется.**

1. Открывать неизвестные письма из внешних почтовых сервисов (mail.ru, yandex.ru, gmail.com и др.), СМС, сообщения в мессенджерах и переходить по ссылкам, доверять и передавать им запрашиваемую ими информацию.

2. В случае отсутствия достаточной уверенности в надежности источника и/или прикрепленного (вложенного) файла открывать или запускать файлы (\*.pdf, \*.bat, \*.exe, \*.com, \*.doc, \*.xls, \*.jar, .exe, .com, .bat, .cmd) и файлы-архивы (.rar, .zip, .tar, .arj и др.), прикрепленные к почтовым сообщениям, а также загружать в сеть Интернет и распаковывать из сети Интернет и электронной корпоративной почты на ПК прикрепленный (вложенный) файл без предварительной проверки на наличие вредоносного кода.

3. Хранить пароли на доступных для чтения без авторизации носителях (например, на бумаге, в текстовом файле и т.д.).

4. Оставлять устройства разблокированными и без присмотра.

5. Загружать, публиковать и распространять материалы, содержащие логины, пароли и прочие средства для получения несанкционированного доступа к информационным ресурсам, а также ссылок на информацию о несанкционированных доступах к ним.

6. Передавать свои пароль и логин для доступа к информационным системам или устройству.

7. Сохранять (кэширование) на устройствах пароли на доступ к информационным ресурсам и различным информационным сервисам. При использовании браузера на устройстве предложения о сохранении логина и пароля необходимо отклонять.

8. Использовать сеть Интернет в целях передачи и распространения материалов, содержащих конфиденциальную информацию.

1) посещать сомнительные и вредоносные сайты;

2) загружать (передавать) вредоносные файлы и программы, а также программное обеспечение и материалы, защищенные авторским правом;

3) использовать службы интернет-чатов, коммуникаторов, служб Интернет-телефонии.

## **Парольная защита**

3. Основными требованиями по генерации паролей являются:

1) допустимые символы: для генерации пароля допустимыми являются буквы латинского алфавита (для пароля в корпоративную сеть (вход в компьютер), цифры и специальные символы (!@#\$%^&\*()\_+|}{<>?":);

2) требование по длине пароля: длина пароля для пользователей должна составлять не менее 8 символов.

3) требование по сложности пароля – наличие следующих символов:

- использование в пароле строчных букв (a-z);

- использование в пароле заглавных букв (A-Z); использование в пароле цифровых значений (0-9);

- использование в пароле специальных символов (!@#\$%^&\*()\_+|}{<>?":).

4) требование по неповторимости пароля: новый пароль не должен повторять предыдущие пароли.

5) нежелательно основывать генерацию пароля на словах, имеющих смысл – имена собственные, дни недели, слова и комбинации слов из словарей любого языка, использовать в пароле легко угадываемые комбинации символов и цифр, слова, клавиатурные последовательности, в том числе обратные (например, password, 87654321, Qwerty, 123456, 1q2w3e, 1111ww@@ и т.п.), а также даты рождения, телефонные номера, ИИН, номера лицевых счетов, государственные регистрационные номерные знаки личных автомашин и т.п.

6) нежелательно использовать в пароле регулярные комбинации цифр подряд – даты рождения, телефонные номера, индивидуальные идентификационные номера (ИИН), номера лицевых счетов и пр.;

7) нежелательно использовать один и тот же пароль для аутентификации в различных сервисах и личных сервисах (почта на интернет-ресурсе, пароли доступа к интернет-сайтам и прочих интернет-ресурсах);

4. При вводе пароля к информационным ресурсам необходимо убедиться, что никто не следит за данным процессом. При вводе пароля к информационным ресурсам необходимо убедиться в невозможности просмотра процесса ввода пароля иными лицами.

5. Должна отсутствовать либо быть отключена функция автозаполнения пароля к информационным системам на устройствах.

6. Хранение паролей может быть в электронном зашифрованном виде, с использованием специального программного обеспечения, при этом пароль к самому программному обеспечению должен соответствовать требованиям парольной политики.

7. Запрещено хранить пароли в открытом виде (например, на стикерах, приклеенных к монитору и/или под клавиатурой, в ежедневниках/блокнотах, оставленных без присмотра и т.п.), в текстовых файлах на рабочей станции на общедоступных информационных ресурсах, и иных общедоступных местах.

8. Пароль необходимо немедленно сменить в случае компрометации или подозрения на компрометацию.

9. Запрещается передавать пароли от учетных записей иным лицам.

#### **Средства защиты от вредоносного программного обеспечения**

10. На устройствах необходимо установить средства защиты от вредоносного программного обеспечения (антивирусные программы). При их использовании следует придерживаться следующих правил:

1) обновление антивирусных средств на рабочих станциях производится

автоматически, не реже одного раза в день;

2) необходимо осуществлять проверку всех съемных носителей информации (HDD, Flash, CD, DVD и т.п.) на вирусы в момент подключения, до начала работы с информацией на них.

11. Во избежание проникновения вирусов на устройства пользователей нельзя:

- 1) отключать функцию мониторинга антивирусных средств;
- 2) прерывать процесс автоматического обновления антивирусных средств;
- 3) прерывать процесс проверки на наличие вирусов;
- 4) использовать непроверенные антивирусными средствами съемные носители информации;
- 5) открывать файлы и ссылки, вложенные в почтовые сообщения, полученные из непроверенных источников либо вызывающие подозрения (язык сообщения не соответствует языку, которым мог пользоваться адресант, сомнения в содержании текста письма и иное сомнительное содержание/вложение).

### **Защита от методов социальной инженерии**

12. Социальная инженерия – это способ атаки, когда злоумышленник с использованием слабостей человеческого фактора, путем проникновения в организацию или телефонного разговора, пытается получить конфиденциальную или ценную информацию. Самым популярным видом такой атаки является фишинг, когда злоумышленник применяет методы социальной инженерии с использованием информационных технологий, например, посылает поддельное письмо (от банка, платежной системы, другой организации), требующее «проверки» определенной информации или совершения определенных действий, с целью получить необходимые данные. При этом письмо может содержать ссылку на фальшивую web-страницу, имитирующую официальную и требующую ввести критичную информацию от логина и пароля в информационную систему до ПИН-кода личной банковской карты. Также мошенники часто применяют метод IP-телефонии для подмены телефонных номеров на схожие с банковскими, иными организациями. В дальнейшем, представляясь сотрудниками службы безопасности или Call Centre, пытаются получить личные данные клиентов, их ИИН, номера карт, ПИН-коды, одноразовые СМС-сообщения, иную важную информацию.

13. Чтобы избежать негативных последствий, связанных с методами «социальной инженерии», каждый пользователь должен соблюдать минимальные требования:

1) при получении почтовых сообщений нельзя отправлять/вводить в веб-формы авторизационные и/или личные данные (номер платежной карты, номер банковского счета, логин/пароль, ПИН-код банковской карты, одноразовые SMS-пароли и 3D Secure пароли, срок действия карты и коды безопасности CVV2 (Card Verification Value)/CVC2 (Card Validation Code)), а также открывать вложенные файлы.

2) никому не разглашать свои авторизационные данные (имя пользователя/пароль) даже руководитель или администратор системы не имеет права запрашивать личные авторизационные данные пользователя.

3) не сообщать никакой информации о роде своей деятельности случайным знакомым, даже если они внушают полнейшее доверие, как правило, злоумышленник, действующий методами «социальной инженерии», обладает

навыками психологического воздействия и способны легко расположить к себе людей, войти к ним в доверие.

4) не разглашать конфиденциальную информацию в телефонных разговорах, мгновенных сообщениях и переписке по электронной почте – помните, что как голос, так и электронное сообщение могут быть симитированы/подделаны.

5) при наличии в электронном письме электронной цифровой подписи проверять ее подлинность, также проверять подлинность сертификатов веб-узлов.

6) не переходить по ссылкам/вложениям, присланным по электронной почте, за исключением ссылок/вложений, присланных администраторами систем в письмах, поддельное письмо со ссылкой/вложением может перенаправить пользователя на сайт, внешне неотличимый от веб-страницы одной из информационных систем, с помощью которого злоумышленник может украсть авторизационные данные, внедрять вредоносные программы и осуществлять иные злонамеренные действия.

7) никогда не вводить логин, пароль, адрес электронной почты, номер платежной карты, номер банковского счета и другую личную информацию, если сайт открывается по открытому протоколу http, а также, если интернет браузер выводит вам предупреждение о недостоверном сертификате или выдает предупреждение о фишинговом (мошенническом) сайте.

8) всегда проверять через адресную строку на том ли сайте вы вводите свой пароль (мошенники подделывают домен, максимально похожий на свой оригинал, различие может быть всего лишь в одной букве). Данный прием мошенников называется спуфинг и используется ими для всевозможных лжеопросов, лжерозыгрышей призов и бонусов.

9) в случае подозрения фишинговой атаки пользователь должен сообщить о данном факте уполномоченному органу.