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, *.jr, .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 изнепроверенных 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 сымитированы/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.

Веб-қосымшаны пайдалану кезінде ұстануға ұсынылатын кибергигиенаны қамтамасыз ету шаралары туралы ақпарат

Алматы қ.
2023 жыл

Жалпы ережелер

1. Бұл құжат ұсынымдық сипатқа ие. Пайдаланушыларға ақпараттық қауіпсіздікке, алаяқтыққа және өзге де оқиғаларға байланысты жағымсыз жағдайларды болдырмау үшін құжатпен танысу ұсынылады.

2. Пайдаланушы:

- егер алаяқтық әрекеттер, ақпараттық қауіпсіздік инциденттері, ДК-ны пайдалануды қиындататын, веб-қосымшаның қалыпты жұмысындағы ауытқулар анықталса, веб-қосымшада көрсетілген контактілер бойынша хабарласуы;
- дербес деректердің, банктік мәліметтердің, аутентификация туралы мәліметтердің және өзге де құпия ақпараттың сақталуын қамтамасыз етуі;
- тек тексерілген құрылғылар мен Wi-Fi желісін пайдалануы;
- құрылғыларда тек тексерілген (ресми көздерден орнатылған) бағдарламалық қамтылымды қолдануы, бағдарламалық қамтылымды үнемі жаңартып отыруы;
- күрделі құпия сөздерді қолдануы және құпия сөз саясатының ұсынымдарын ұстануы қажет

Пайдаланушыларға үзілді-кесілді тыйым салынады.

1. Сыртқы пошта сервистерінен (mail.ru, yandex.ru, gmail.com және т. б.) белгісіз хаттарды ашға, SMS, мессенджерлердегі хабарламалар және сілтемелер бойынша өтуге, оларға сенуге және олар сұраған ақпаратты беруге.

2. Дереккөздің және/немесе тіркелген (кірістірілген) файлдың сенімділігіне толық көзіңіз жетпеген жағдайда, файлдарды (*.pdf, *.bat, *.exe, *.com, *.doc, *.xls, *.jr, .exe, .com, .bat, .CMD) және пошта хабарларына тіркелген мұрағат-файларды (.rar, .zip, .tar, .пошта хабарламаларына тіркелген arj және т. б.) ашуға немесе іске қосуға, сондай-ақ зиянды кодтың бар-жоғын алдын ала тексерусіз тіркелген (қоса салынған) файлды Интернет желісіне жүктеуге және интернет желісінен және электрондық корпоративтік поштадан ДК-ге жүктеп алуға.

3. Құпия сөздерді авторландырусыз оқуға болатын тасымалдағыштарда сақтауға (мысалы қағазда, мәтіндік файлда және т.б.).

4. Құрылғыларды ашық күйде және қараусыз қалдыруға.

5. Ақпараттық ресурстарға рұқсатсыз қол жеткізу, сондай-ақ оларға рұқсатсыз қол жеткізу туралы ақпаратқа сілтемелер алу үшін логиндер, құпия сөздер және өзге де құралдар бар материалдарды жүктеуге, жариялауға және таратуға.

6. Ақпараттық жүйелерге немесе құрылғыға кіру үшін өзіңіздің құпия сөзіңіз бен логиніңізді жіберуге.

7. Ақпараттық ресурстарға және түрлі ақпараттық сервистерге қол жеткізуге арналған құпия сөздерді құрылғыларда сақтауға (кэштеуге). Құрылғыда браузерді пайдаланған кезде логин мен құпия сөзді сақтау туралы ұсыныстардан бас тарту керек.

8. Интернет желісін құпия ақпаратты қамтитын материалдарды беру және тарату мақсатында пайдалануға.

1) күмәнді және зиянды сайттарға кіруге;

2) зиянды файлдар мен бағдарламаларды, сондай-ақ авторлық құқықпен қорғалған бағдарламалық қамтылым мен материалдарды жүктеуге (беруге);

3) интернет-чаттар, коммуникаторлар, Интернет-телефония қызметтерін пайдалануға.

Құпия сөзді қорғау

3. Құпия сөздерді жасаудың негізгі талаптары:

1) рұқсат етілген таңбалар: құпия сөзді жасау үшін латын әліпбиінің

әріптері (корпоративтік желіге кіретін (компьютерге кіретін) құпия сөз үшін сандар мен (!@#$%^&*()_+|}{<>?":) арнайы таңбалар) қолданылады;

2) құпия сөздің ұзындығы бойынша талап: пайдаланушылар үшін құпия сөздің ұзындығы кемінде 8 таңба болуы керек.

3) ұпия сөздің күрделілігі бойынша талап – келесі символдардың болуы:

- құпия сөзде кіші әріптерді (a-z) қолдану;

- құпия сөзде бас әріптерді (A-Z) қолдану; құпия сөзде цифрлық мәндерді (0-9) пайдалану;

- құпия сөзде арнайы символдарды (!@#$%^&*()_+|}{<>?":) *пайдалану.*

4) құпия сөздің қайталанбауы бойынша талап: жаңа құпия сөз алдыңғы құпия сөздерді қайталамауы керек.

5) құпия сөзді жасауда мағынасы бар сөздерге – жалқы есімдер, апта күндері, кез-келген тілдің сөздіктеріндегі сөздер мен сөз тіркестеріне негіздеу, құпия сөзде таңбалар мен сандардың, сөздердің, пернетақта тізбектерінің, соның ішінде кері (мысалы, password, 87654321, Qwerty, 123456, 1q2w3e, 1111ww@@ және т. б.), сондай-ақ туған күндерді, телефон нөмірлерін, ЖСН, дербес шот нөмірлерін, жеке автомашиналардың мемлекеттік тіркеу нөмірлік белгілерін және т.с.с. пайдалану қажет емес.

6) құпия сөзде цифрлардың тұрақты комбинациясын – туған күнді, телефон нөмірлерін, жеке сәйкестендіру нөмірлерін (ЖСН), дербес шот нөмірлерін және т. б. пайдалану қажет емес;

7) әртүрлі сервистерде және жеке сервистерде аутентификаттау үшін бірдей құпия сөзді (интернет-ресурстағы пошта, интернет-сайттарға және басқа интернет-ресурстарға кіру құпия сөздерін) пайдалану қажет емес;

4. Ақпараттық ресурстарға құпия сөзді енгізген кезде, бұл процесті ешкім бақылап тұрмағанына көз жеткізу керек. Ақпараттық ресурстарға құпия сөзді енгізу кезінде өзге адамдардың құпия сөзді енгізу барысын көре алмайтындығына көз жеткізу қажет.

5. Құрылғылардағы ақпараттық жүйелерге құпия сөзді автоматты түрде толтыру қыметі болмауы немесе өшірілуі тиіс.

6. Құпия сөздерді сақтау арнайы бағдарламалық қамтылымды қолдана отырып, электронды шифрланған түрде болуы мүмкін, бұл ретте бағдарламалық қамтылымның өзіне кіретін құпия сөз құпия сөз саясатының талаптарына сәйкес келуі керек.

7. Құпия сөздерді ашық (мысалы, мониторға және/немесе пернетақтаның астына желімделген жапсырмаларда, қараусыз қалған күнделіктерде /блокноттарда және т. с.с.), жұмыс станциясындағы мәтіндік файлдарда жалпыға қолжетімді ақпараттық ресурстарда және өзге де жалпыға қолжетімді орындарда сақтауға тыйым салынады.

8. Жала жабылған немесе жала жабылуына күдіктенген жағдайда, құпия сөзді дереу ауыстыру қажет.

9. Есептік жазбаға кіретін құпия сөздерді өзге адамдарға беруге тыйым салынады.

Зиянды бағдарламалық қамтылымнан қорғау құралдары

10. Құрылғыларда зиянды бағдарламалық қамтылымнан қорғау құралдарын (вирусқа қарсы бағдарламалар) орнату қажет. Оларды пайдалану кезінде келесі ережелерді сақтау керек:

1) жұмыс станцияларында вирусқа қарсы құралдарды жаңарту күніне

кемінде бір рет автоматты түрде жүргізіледі;

2) қосылу сәтінде, олардағы ақпаратпен жұмыс бастағанға дейін барлық алынбалы ақпарат тасымалдағыштарды (HDD, Flash, CD, DVD және т.с.с.) вирустарға тексеру қажет.

11. Пайдаланушылардың құрылғыларына вирустардың енуіне жол бермеу үшін:

1) вирусқа қарсы құралдарды бақылау қызметін өшіруге;

2) вирусқа қарсы құралдарды автоматты түрде жаңарту барысын үзуге;

3) вирустардың бар-жоғын тексеру барысын үзуге;

4) вирусқа қарсы құралдармен тексерілмеген алынбалы ақпарат тасымалдағыштарды пайдалануға;

5) тексерілмеген көздерден алынған не күдік туғызатын (хабарлама тілі адресат қолдана алатын тілге сәйкес келмейді, хат мәтінінің мазмұнына күмәндану және өзге де күмән тудыратын мазмұндағы) пошта хабарларына салынған файлдар мен сілтемелерді ашуға).

Әлеуметтік инженерия әдістерінен қорғау

12. Әлеуметтік инженерия – бұл кезде шабуылдаушы адам адами фактордың әлсіз жақтарын қолданып, ұйымға кіру немесе телефон әңгімесіне қосылу арқылы құпия немесе құнды ақпаратты алуға тырысатын шабуыл түрі. Мұндай шабуылдың ең танымал түрі фишинг, бұл кезде шабуылдаушы ақпараттық технологияларды қолдана отырып әлеуметтік инженерия әдістерін пайдаланады, мысалы, қажетті деректерді алу үшін белгілі бір ақпаратты «тексеруді» немесе белгілі бір әрекеттерді жасауды талап ететін жалған хат (банктен, төлем жүйесінен, басқа ұйымнан) жібереді. Бұл ретте хатта түпнұсқадан айнымайтын және ақпараттық жүйеге логин мен құпия сөзден бастап жеке банк картасының ПИН-кодына дейін енгізуді талап ететін, жалған web-бетке сілтемеден тұруы мүмкін. Сондай-ақ, алаяқтар телефон нөмірлерін банктік және басқа ұйымдарға ұқсас етіп ауыстыру үшін IP-телефония әдісін жиі қолданады. Бұдан әрі өздерін қауіпсіздік қызметінің немесе Call Centre қызметкерлері ретінде таныстырып, клиенттердің жеке деректерін, олардың ЖСН, карта нөмірлерін, ПИН-кодтарын, бір реттік СМС-хабарларды, өзге де маңызды ақпаратты алуға тырысады.

13. «Әлеуметтік инженерия» әдістерімен байланысты жағымсыз салдарды болдырмау үшін әр пайдаланушы тым болмаса мына талаптарды сақтауы керек:

1) пошта хабарларын алған кезде веб-нысандарға авторландыру және/немесе жеке деректерді (төлем картасының нөмірі, банк шотының нөмірі, логин / құпия сөз, банк картасының ПИН-коды, бір реттік SMS-құпия сөздер және 3D Secure құпия сөздері, картаның жарамдылық мерзімі және CVV2 (Card Verification Value)/CVC2 (Card Validation Code) қауіпсіздік кодтарын) жіберуге/енгізуге, сондай-ақ қоса тіркелген файлдарды ашуға болмайды.

2) өзінің авторландыру деректерін (пайдаланушы аты/құпия сөз) ешкімге жария етпеу, тіпті жүйе жетекшісінің немесе әкімшісінің де пайдаланушының жеке авторландыру деректерін сұратуға құқығы жоқ.

3) тіпті олар толық сенімге ие болса да, кездейсоқ таныстарға өз қызметінің түрі туралы ешқандай ақпарат бермеуге, әдетте, «әлеуметтік инженерия» әдістерімен әрекет ететін шабуылдаушы психологиялық әсер ету дағдыларын меңгерген және адамдарды өздеріне оңай қаратып, сенімдеріне кіре алады.

4) телефон арқылы сөйлесулерде, жедел хабарларда және электрондық пошта арқылы хат алмасуда құпия ақпаратты жария етпеуге – дауыс сияқты электрондық хабарды да жасауға/бұрмалауға болатынын естен шығармаңыз.

5) электрондық хатта электрондық цифрлық қолтаңба болған кезде оның түпнұсқалығын тексеру, сонымен қатар веб-тораптардың сертификаттарының түпнұсқалығын тексеру.

6) хаттардағы жүйе әкімшілері жіберген сілтемелерді/тіркемелерді қоспағанда, электрондық пошта арқылы жіберілген сілтемелер/тіркемелер бойынша өтпеу, сілтеме/тіркемесі бар жалған хат пайдаланушыны сырттай ақпараттық жүйелердің бірінің веб-бетінен ажырата алмайтын сайтқа бағыттай алады, оның көмегімен шабуылдаушы авторландыру деректерін ұрлай алады, зиянды бағдарламаларды енгізе алады және өзге де зиянды әрекеттерді жүзеге асыра алады.

7) гер сайт ашық httpхаттамасы бойынша ашылса, сондай-ақ интернет браузер сізге жалған сертификат туралы ескерту берсе немесе фишингтік (алаяқтық) сайт туралы ескерту берсе, ешқашан логинді, құпия сөзді, электрондық пошта мекенжайын, төлем картасының нөмірін, банктік шот нөмірін және басқа да жеке ақпаратты енгізбеу.

8) өзіңіздің құпия сөзіңізді шынайы сайтқа енгізіп жатқаныңызды мекенжай жолы арқылы әрдайым тексеріп отырыңыз (алаяқтар доменді тұпұсқаға барынша ұқсатып жасайды, айырмашылық тек бір әріпте болуы мүмкін). Алаяқтардың бұл әдісі спуфинг деп аталады және олар түрлі жалған сұрақтар қою, сыйлықтар мен бонустар ойнату үшін қолданылады.

9) фишингтік шабуылға күдік болған жағдайда, пайдаланушы осы факті туралы уәкілетті органға хабарлауға тиіс.

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, *.jr, .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 изнепроверенных 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 сымитированы/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.