ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ
імені Володимира Гнатюка

Н А К А З

10.12.2018 р. м. Тернопіль **№ 313**

Про Пам'ятку з питань забезпечення інформаційної безпеки при роботі в мережі Інтернет

З метою недопущення нанесення шкоди національній безпеці України в інформаційній сфері та з урахуванням положень Указу Президента України від 25.02.2017 р. № 47 "Про рішення Ради національної безпеки від 29 грудня 2016 року "Про Доктрину інформаційної безпеки України", Закону України "Про основні засади забезпечення кібербезпеки України" та листа Управління Служби безпеки України в Тернопільській області від 03.12.2018 р. № 69/30-3433 **н а к а з у ю:**

1. Довести до відома працівників університету Пам'ятку з питань забезпечення інформаційної безпеки при роботі в мережі Інтернет.

2. Наказ набуває чинності з дня його підписання та підлягає офіційному оприлюдненню на офіційному сайті університету.

3. Начальнику відділу кадрів Бзовській У.М. ознайомити під підпис працівників університету згідно за списком (список додається).

3. Контроль за виконанням даного наказу залишаю за собою.

Підстава: лист Управління Служби безпеки України в Тернопільській області від 03.12.2018 р. № 69/30-3433.

Ректор **Б.Б.Буяк**

ПОГОДЖЕНО:

Начальник юридичного відділу

_____ Р.В. Комар-Чорний

З оригіналом згідно:
Зав. канцелярії_____

ПАМ'ЯТКА
з питань забезпечення інформаційної безпеки в мережі інтернет

Перелік основних чинників, що впливають на стан інформаційної безпеки у зв'язку із використанням загальнодоступних та соціально орієнтованих ресурсів мережі Інтернет:

- Військова агресія Російської Федерації та пов'язані з нею масштабні кібератаки, масові антиукраїнські інформаційні кампанії та їх психологічний вплив на користувачів українського сегменту мережі Інтернет, отримання несанкціонованого доступу до персональних даних та іншої важливої інформації з електронних поштових скриньок та соціальних мереж тощо.
- Існування загрози для державних установ (міністерств, відомств, агентств, фінансових установ тощо) у зв'язку із використанням працівниками у службовій діяльності та повсякденному житті програмного забезпечення російського виробництва, а також поштових електронних сервісів та соціальних мереж «ВКонтакте» та «Одноклассники», доступ до яких на даний час обмежено відповідно до Указу Президента України № 133/2017 від 15.05.2017 року.
- Підконтрольність найбільших та найвпливовіших медіа особам, котрі використовують дані ресурси для лобіювання та відстоювання особистих, а не державних інтересів.
- Активне наповнення соціальних мереж замовними дописами відповідного контенту із використанням так званих бот-мереж («ботів») та технології масового «тролінгу».
- Маніпуляції у засобах масової інформації та соціальних мережах з метою приваблення більшої аудиторії шляхом використання методів соціальної інженерії.
- Використання соціальних мереж для поширення недостовірної (фейкової), викривленої, деструктивної інформації та здійснення маніпулятивного впливу на суспільну свідомість користувачів українського сегменту мережі Інтернет.

Характеристика ключових факторів ризику та рекомендації щодо їх нейтралізації:

1. Зберігання та передача даних

Недотримання окремих правил безпеки під час здійснення службових обов'язків працівниками органів виконавчої влади та місцевого самоврядування, посадовими особами державних підприємств, установ, організацій, а також військовослужбовцями може призвести до втрати чи крадіжки мобільних телефонів, персональних ноутбуків, магнітних носіїв інформації тощо. Вказане ставить під загрозу збереження персональних даних та може призвести до розголошення інформації з обмеженим доступом.

З метою уникнення негативних наслідків у випадку втрати або викрадення носіїв інформації необхідно:

- встановити паролі на усі пристрої, що перебувають у користуванні (PIN-коди, паролі на вхід до всіх облікових записів, паролі на планшетах та ноутбуках тощо);
- систематично робити резервне копіювання важливих файлів;
- блокувати пристрої щоразу після закінчення роботи з ними.

2. Соціальні мережі

Соціальні мережі у наш час стали зручним та ефективним засобом комунікації. За допомогою соціальних медіа можна обмінюватись повідомленнями, публікувати особисті фото- та відеоматеріали, розміщувати інформацію про місце роботи і відпочинку, колег, друзів, навчання, дозвілля, політичні погляди тощо. Така кількість приватної інформації у разі її потрапляння до зацікавлених осіб може поставити під загрозу як службову діяльність так і приватне життя державних службовців, керівників підприємств, установи, організації, працівників органів виконавчої влади та місцевого самоврядування, а також військовослужбовців.

З метою уникнення несанкціонованого доступу до персональних акаунтів, зареєстрованих у соціально орієнтованих ресурсах мережі Інтернет, необхідно:

- встановити надійний пароль для входу в обліковий запис. При цьому рівень захищеності акаунту та інформації, що знаходиться у ньому, залежить від складності встановленого паролю;
- використовувати функцію подвійної авторизації. Щоб увійти до профілю з незнайомого пристрою, сервіс вимагатиме пройти додаткову ідентифікацію як власника акаунту. При цьому на вказаний номер телефону або на поштову скриньку буде надіслано повідомлення з кодом підтвердження, або необхідно буде ввести один із паролів, які попередньо були збережені через інший обраний спосіб підтвердження;
- здійснити додаткові налаштування профілю в соціальних мережах з метою отримання інформації щодо несанкціонованих входів до ресурсів з невідомого пристрою або Інтернет-браузера;
- при створенні акаунтів у соціальних мережах використовувати у якості «логіна» поштову адресу надійного сервісу (наприклад, «Google», «Yahoo») або українських поштових сервісів. Не рекомендується користуватися російськими сервісами, доступ до яких заборонено в Україні, оскільки через персональну електронну скриньку можна отримати пароль, а відтак доступ до профілів, зареєстрованих у соціальних мережах;

• не здійснювати авторизацію особистих чи робочих, корпоративних профілів з незнайомих чи незахищених пристроїв. Існує ймовірність, що після завершення роботи не буде здійснено вихід із свого облікового запису або пристрій запам'ятає вказаний при вході логін та пароль. Крім того, існує ймовірність ураження такого пристрою шкідливим програмним забезпеченням, що може здійснювати збір та передачу відомостей щодо паролів та логінів зацікавленим особам;
• пам'ятайте, що саме фішинг (довідково: фішинг – вид шахрайства, метою якого є виманювання у довірливих або неуважних користувачів мережі Інтернет персональних даних клієнтів, сервісів із переказу або обміну валюти, Інтернет-магазинів) є найпоширенішим способом отримання зловмисниками паролів до поштових скриньок та сторінок у соціальних мережах.

Крім того, у ході гібридної агресії з боку РФ соціальні мережі активно використовуються для збору додаткових відомостей щодо місць регулярного перебування особи, її родичів, колег, особистих уподобань та іншої приватної інформації. Водночас, через соцмережі здійснюється збір та передача інформації щодо місць дислокації та складу окремих підрозділів Збройних сил України, які залучені до проведення операції об'єднаних сил на сході України, яка частково є конфіденційною.

З метою недопущення отримання зацікавленими особами додаткової (приватної) інформації щодо особи, членів її сім'ї, колег, уподобань тощо, стосовно військовослужбовців – інформації щодо місць дислокації та складу окремих підрозділів Збройних сил України, які залучені до проведення операції об'єднаних сил на сході України, необхідно дотримуватись наступних правил:

• не публікувати у соціальних мережах інформацію, що може поставити під загрозу особисте життя особи, життя членів її сім 'ї та інших осіб;
• військовослужбовцям та членам їх сімей не варто публікувати фото- та відеоматеріали, за допомогою яких можна визначити місцезнаходження військової частини, окремих збройних військових формувань, що беруть участь у проведенні операції об'єднаних сил на сході України. Вказані дії можуть загрожувати життю та здоров'ю людей;
• обмежити доступ до приватної інформації в налаштуваннях конфіденційності соціальної мережі. Вибрати налаштування, які найбільше захищають додаткові відомості про власника акаунта. Зокрема, не зазначати геолокацію (місце розташування) та доступність пошуку акаунта в соціальній мережі за номером мобільного телефону та адресою поштової скриньки;
• періодично переглядати список друзів у соціальній мережі. Якщо серед них є незнайомі або підозрілі люди (акаунти), необхідно їх видалити, оскільки статус «друга» відкриває доступ до більшого обсягу приватної інформації про особу. В подальшому необхідно бути уважними під час додавання до списку «друзів» нових користувачів;
• не рекомендується використовувати російські соціальні мережі, «ВКонтакте» та «Одноклассники» доступ до яких заборонено, оскільки останні на вимогу спецслужб РФ можуть передавати відомості щодо персональних даних власників акаунтів (e-mail, номер мобільного телефону, дата та IP-адреса реєстрації, дата та IP-адреса останнього відвідування тощо).

3. Використання російських соціально орієнтованих ресурсів мережі Інтернет

З 2016 року усі російські сервіси відповідно до федеральних законів РФ «О внесений изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» від 05.05.2014 року № 97-ФЗ, «О внесений изменений в Федеральний закон «О противодействии терроризму» від 06.07.2016 року № 374-ФЗ, «О внесений изменений в Уголовный кодекс РФ и Уголовно-процессуальный кодекс РФ в части установлення дополнительных мер противодействия терроризму и обеспечения общественной безопасности» від 06.07.2016 року № 375-ФЗ та інших окремих законодавчих актів на постійній основі надають спецслужбам РФ відомості щодо персональних даних користувачів та їх особистого листування. Зважаючи на це, українські Інтернет-провайдери зобов'язані обмежити доступ користувачам до російських соціальних мереж та сервісів.

Крім того, слід пам'ятати, що доступ до російських соціальних мереж «ВКонтакте» та «Одноклассники» на території України заборонено рішенням Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)», введеного в дію Указом Президента України від 15.04.2017 року № 133.

Головна порада – перехід па західні та українські сервіси, такі як «Gmail», «Google+», «Facebook», «Twitter», «Ukr.net» тощо.

4. Використання додатків до смартфонів

Під час встановлення тих чи інших додатків на власний телефон ці програмні продукти можуть вимагати доступу до певної інформації на використовуваному пристрої, насамперед геолокації, списку контактів, акаунтів у соціальних мережах та поштових скриньок.

За наявними даними, більшість шпигунських програм «вшиваються» саме в мобільні додатки, які цікавлять конкретну аудиторію. Тому необхідно бути уважним під час встановлення додатків, особливо якщо робити це з невідомих та неперевірених сервісів.

З метою унеможливлення завантаження на особистий пристрій програм-шпигунів необхідно дотримуватись таких правил:

- встановлювати додатки лише з офіційних та перевірених сервісів (Chrome Store, Add-ons та Play Market для Android, App Store для OS);
- заборонити операційній системі смартфона (планшета, ПЕОМ) автоматично встановлювати додатки з невідомих джерел шляхом здійснення відповідних налаштувань пристрою;
- періодично здійснювати чистку усіх особистих пристроїв від додатків, які не використовуються.

5. Електронне листування

Електронні поштові скриньки зберігають не тільки величезний обсяг особистих та робочих даних (листів), але й зазвичай прикріплені до акаунтів у соціальних мережах, месенджерах, хмарних сервісах тощо. Тому несанкціонований доступ до поштової скриньки може мати серйозні наслідки, такі як отримання інформації конфіденційного характеру, зміна паролів до сайтів, акаунтів без відома їх власників, отримання доступу до особистих фотографій та відео, розсилання спаму від імені інших осіб тощо.

Щоб уникнути зламу електронної поштової скриньки, необхідно:

- увімкнути двофакторну автентифікацію за допомогою мобільного пристрою. В такому випадку під час спроби отримання паролю до поштової скриньки сторонніми особами буде надходити попередження на мобільний телефон у вигляді SMS-повідомлення про спробу злому;
- встановити надійний пароль;
- не використовувати для відновлення паролю російські сервіси («Yandex.ru», «Mail.ru» тощо);
- не запускати на пристроях вкладення підозрілих листів, що містять виконуваний файл з такими розширеннями як «.exe», «.bat», «.cmd», «.vbs», «.docm», «.xlsm» тощо;
- державні службовці та військовослужбовці повинні пам'ятати, що службові електронні скриньки не слід використовувати для приватного листування.

6. Вихід до мережі Інтернет

Одним із найпоширеніших способів входу до мережі Інтернет у публічних місцях є підключення до відкритих точок Wi-Fi. Зазвичай вони є безплатними та вхід до них здійснюється без введення паролів. Саме відсутність паролю робить їх вразливішими для злому з боку зацікавлених осіб, які мають на меті отримати доступ до персональних даних та відомостей, що зберігаються на телефоні, планшеті, ПЕОМ тощо.

Щоб уникнути перехоплення даних сторонніми особами, необхідно:

- під час здійснення входу до мережі використовувати лише ті точки доступу до Wi-Fi, які мають протоколи безпеки для захисту бездротового з 'єднання WPA чиЗУРА-2;
- у публічних місцях найкраще користуватись особистим Wi-Fi модемом або здійснювати вхід до мережі Інтернет з мобільного пристрою за передплаченим пакетом послуг мобільного оператора;
- на ПЕОМ, мобільних пристроях та планшетах необхідно вимкнути функцію «Автоматичне підключення до Wi-Fi»;
- військовослужбовцям, які виконують завдання в зоні проведення ООС, обмежити використання особистих модемів чи роутерів для входу до мережі Інтернет через передачу сигналу, який можна зафіксувати спеціальною технікою та визначити місцезнаходження.

7. Перелік російських веб-ресурсів, якими не рекомендовано користуватись:

Указом Президента України від 15.05.2017 року № 133/2017 введено у дію рішення РНБО щодо обмеження діяльності в Україні російських соціальних мереж та сервісів. У переліку російських компаній, щодо яких вжито санкційні заходи, зазначено сервіси «Mail.Ru Group» та «Яндекс». Повний перелік ресурсів з Додатку до Указу, доступ до яких повинні заборонити Інтернет-провайдери:

1. afisha.yandex.ru;	*27.*	*rasp.yandex.ru;*
2. audience.yandex.ru;	*28.*	*realty.yandex.ru;*
3. auto.ru;	*29.*	*speechkit.yandex.ru;*
4. avia.yandex.ru;	*ЗО.*	*sprav.yandex.ru;*
5. brouser.yandex.ru;	*31.*	*stat.yandex.ru;*
6. calendar.yandex.ru;	*32.*	*taxi.yandex.ru;*
7. elivery.yandex.ru/promo;	*33.*	*tech.yandex.ru;*
8. direct.yandex.ru;	*34.*	*telephony.yandex.ru;*
9. disk.yandex.ru;	*35.*	*translate.yandex.ru;*
10. dns.yandex.ru;	*36.*	*travel.yandex.ru;*
11. fotki.yandex.ru;	*37.*	*tv.yandex.ru;*
12. kassa.yandex.ru;	*38.*	*webmaster.yandex.ru;*
13. mail.yandex.ru;	*39.*	*www.kinopoisk.ru;*
14. market.yandex.ru;	*40.*	*xml.yandex.ru;*
15. meU-ika.yandex.ru;	*41.*	*yandcx.ru;*

16. metro.yandex.ru;	*42.*	*yandex.ru/adv?from=all;*
17. money.yandex.ru;	*43.*	*yandex.ru/blog;*
18. money.yandex.ru/card2card;	*44.*	*yandex.ru/images;*
19. money.yandex.ru/new;	*45.*	*yandex.ru/intemet;*
20. money.yandex.ru/newcard;	*46.*	*yandex.ru/maps;*
21. music.yandex.ua;	*47.*	*yandex.ru/people;*
22. yandex.ru/pogoda/moscov;	*48.*	*n.maps.yandex.ru;*
23. news.yandex.ru;	*49.*	*yandex.ru/suvenirka;*
24. partner.yandex.ru;	*50.*	*yandex.ru/time;*
25. pdd.yandex.ru;	*51.*	*yandex.ru/yaca;*
26. yandexdatafactory.com/ru;	*52.*	*rabota.yandex.ru.*

Крім того, з огляду на введення в дію у Російській Федерації «антитерористичного» закону від 01.08.2014 року, що надав право спеціальним службам отримувати особисті дані користувачів Інтернет- ресурсів, сервери яких знаходяться на території РФ, не рекомендовано користуватись наступними Інтернет-ресурсами:

1. Автокадабра – autokadabra.ru;
2. БебиБлог – babyblog.ru;
3. Bnont@mail.Ru – blogs.mail.ru;
4. Блогус – blogus.ru/blog.php;
5. Вебкруг-webkrug.ru;
6. Дневник на TKS.RU – blogs.tks.ru/portal.php;
7. За Баранкой – zabarankoi.ru;
8. Карта для любителей рыбалки - fishingmap.ru;
9. Клерк.ги – klerk.ru;
10. ЛИМП – limpa.ru;
11. Мой Круг – moikrug.ru;
12. Моя живая страница – mylivepage.ru;
13. Отдохнули.ру – otdohnuli.ru;
14. Привет.ру – privet.ru;
15. Рыбловньїй клуб — fion.ru;
16. Сообщество влюбленньїх в кино – ilovecinema.ru;
17. Соседи-Онлайн – sosedi-online.ru;
18. Тейст – mmm-tasty.ru;
19. Факультет.ру – facultet.ru;
20. Фотострана – fotostrana.ru;
21. Юмама – u-mama.ru;
22. Я талант – yatalant.ru;
23. Beon.ru – beon.ru;
24. Diary.ru – diary.ru;
25. Dogster-dogster.ru;
26. ITBlogs – itblogs.ru;
27. Liveintemet — liveintemet.ru;
28. LiveLib – livelibe.ru;
29. LJ.Rossia.org-lj.rossia.org;
30. MirTesen.ru-mirtesen.ru;
31. Re;vision – revision.ru;
32. RuSpace – ruspace.ru;
33. Spaces.ru – spaces.ru;
34. Telefoner.ru – telefoner.ru;
35. TooDoo – toodoo.ru;
36. VeniVidi – venividi.ru;
37. 100 Друзей – 100druzei.ru.

8. Рекомендації посадовій особі органу виконавчої влади, місцевого самоврядування, представникам міністерств та відомств:

• прес-службам державних органів під час суспільно-політичних подій в країні необхідно надавати коментарі та роз'яснення рішень на випередження, щоб уникнути інтерпретацій та викривлень у ході обговорення тієї чи іншої ситуації в загальнодоступних та соціально орієнтованих ресурсах мережі Інтернет;

• державним органам, установам необхідно розробити та затвердити чіткий план дій для оприлюднення представниками їхніх прес-служб інформації у випадку виникнення резонансних інцидентів;

• офіційні представники органів державної влади повинні оприлюднювати суспільно значущу інформацію, якщо вона не належить до тієї категорії, що не підлягає оприлюдненню. Не варто забувати, що приховування такої інформації від суспільства може знизити довіру до них;

• представникам органів державної влади під час надання коментарів, інтерв'ю, брифінгів не рекомендується використовувати оціночні судження, що можуть призвести до неоднозначного тлумачення наданої інформації її споживачами;

• органам державної влади необхідно розробити правила використання офіційних сторінок та акаунтів у соціальних мережах для уникнення непорозумінь з користувачами та окреслення формату комунікації через соціальні мережі. Крім того, вважається за доцільне здійснити верифікацію (довідково: верифікація – це офіційне підтвердження походження сторінки, її офіційного власника (фізичної, юридичної особи) автентичності викладеної інформації через службу технічної підтримки) офіційних представництв органів державної влади та установ, які у своїй діяльності використовують акаунти у соціальних мережах, насамперед «Facebook», «Twitter», «Google+» та канали у відеохостингу «Youtube»;

• держслужбовцям та військовослужбовцям, а також іншим особам, які відповідно до своїх функціональних обов'язків працюють з інформацією з обмеженим доступом, необхідно пам'ятати, що під час оформлення допуску до державної таємниці при заповненні відповідних анкет вони повинні вносити достовірні дані про свої контакти з іноземними громадянами, наявність власних електронних скриньок, сайтів, профілів у соціальних мережах та тематичних форумах.