Додаток 63

ІНСТРУКЦІЯ

щодо забезпечення кіберзахисту працівниками Національної школи суддів України під час виконання службових обов'язків

1.Загальні положення

Інструкція щодо забезпечення кіберзахисту працівниками Національної школи суддів України під час виконання службових обов'язків (далі - Інструкція) є локальним нормативно-правовим актом, який спрямований на підвищення рівня кібербезпеки в Національній школі суддів України (далі - НШСУ) і регулює спеціальні аспекти кіберзахисту, зокрема щодо функціонування комплексної системи захисту інформації в НШСУ; регламентує поведінку її працівників, встановлює правила, деталізує настанови і приписи користування інформаційно-телекомунікаційною системою НШСУ (далі - ІТС НШСУ) під час виконання службових обов'язків.

Ця Інструкція є складовою частиною експлуатаційної документації комплексної системи захисту інформації ІТС НШСУ та Регламенту Національної школи суддів України, і конкретизує пункт 3.2. параграфа 3 глави 2 розділу VIII "Інформаційне забезпечення діяльності Національної школи суддів України".

Інструкція стосується всіх працівників, що мають доступ до користування ІТС НШСУ (далі - користувачі), і є обов'язковою до виконання.

2.Визначення термінів

Відповідно до статті 1 Закону України від 5 жовтня 2017 року № 2163-VIII "Про основні засади забезпечення кібербезпеки України" (зі змінами) нижченаведені терміни в цій Інструкції вживаються в такому значенні:

1) **кібербезпека** - захищеність життєво важливих інтересів людини і громадянина, суспільства і держави в цілому, її організацій та установ, зокрема під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі;

2) **кіберзахист** - сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання несанкціонованому доступу до інформаційно- телекомунікаційних систем (кіберінциденти), виявлення та

захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем;

3) **кіберзагроза** - наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів;

4) **кібератака** - спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно- комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту;

5) **інформаційно-телекомунікаційна система (ІТС)** - система передавання, комутації або маршрутизації даних, а також обладнання та інші технічні і технологічні ресурси незалежно від наявності доступу до мережі Інтернет та/або інших глобальних мереж передачі даних;

6) **технічні і технологічні ресурси ІТС НШСУ** - обладнання та інші ресурси, у тому числі засоби і пристрої зв'язку, комп'ютери, інша комп'ютерна техніка, програмне забезпечення тощо;

7) **користувачі** - працівники НШСУ, а саме: службові та посадові особи науково-викладацького складу, що мають доступ до користування ІТС НШСУ;

8) **адміністратор безпеки, адміністратор системи ІТС НШСУ** - працівник відділу інформаційних технологій НШСУ, відповідні повноваження якого визначені посадовою інструкцією, відповідною інструкцією адміністратора безпеки, адміністратора системи, або ж разовим дорученням начальника відділу.

3. Функції (предмет, зміст, перелік видів робіт) користувачів

На виконання службових обов'язків, керуючись правилами поведінки й етичними нормами державних службовців, працівники НШСУ реалізують такі функції під час користування ІТС НШСУ:

- експлуатація комп'ютерів та інших складових ІТС НШСУ, до яких користувач має доступ;

- створення, отримання/надсилання, обробка, збереження і друк інформації в ІТС НШСУ у межах їх обов'язків та повноважень, що визначені посадовими інструкціями та/або дорученнями і розпорядженнями керівництва НШСУ;

- дотримання конфіденційності щодо отриманих атрибутів доступу до ІТС НШСУ (логін, пароль, смарт карти та інші атрибути доступу, які надані користувачу) та її складових, сервісів і служб (службова електронна пошта та інше).

3.Права користувачів

Користувачі, за виключенням працівників відділу, відповідального за інформаційні технології НШСУ, мають лише ті права, що обмежені нижченаведеними положеннями:

- користуватись ІТС НШСУ тільки на виконання службових обов'язків відповідно до посадових інструкцій;

- отримувати технічні і технологічні ресурси ІТС НШСУ в належному технічному стані;

- одержувати від працівників відділу інформаційних технологій НШСУ роз'яснення щодо особливостей користування тими чи іншими технологічними ресурсами ІТС НШСУ;

- отримувати обладнання та інші технічні і технологічні ресурси ІТС НШСУ на заміну пошкодженим;

- мати особисті реквізити доступу до ІТС НШСУ (логін, пароль тощо);

- звертатися до адміністратора системи ІТС НШСУ щодо зміни реквізитів доступу до компонентів ІТС НШСУ, зокрема логіну, паролю тощо (особисті реквізити доступу, які користувач забув, відновленню не підлягають за відсутності в адміністраторів ІТС НШСУ зазначених даних).

4. Обов'язки користувачів

Користувачі під час експлуатації ІТС НШСУ зобов'язані:

обережно користуватись технічними і технологічними ресурсами ІТС НШСУ, підтримувати їх в належному робочому стані;

- додержуватись правил кібербезпеки під час роботи в ІТС НШСУ, знати і виконувати вимоги та настанови цієї Інструкції;

- не допускати витоку, розголошення інформації, зокрема технологічної, що циркулює в ІТС НШСУ і яка може зашкодити її діяльності;

- використовувати тільки ліцензійне/легалізоване програмне забезпечення, що встановлено працівниками відділу інформаційних технологій НШСУ, систематично і своєчасно оновлювати його на вимогу адміністраторів ІТС НШСУ та/або на запит відповідного програмного забезпечення;

- регулярно застосовувати встановлене антивірусне програмне забезпечення;

- виконувати правила кібербезпеки при підключенні віддалено з особистих та/або інших комп'ютерів, ноутбуків та смартфонів до сервісів, служб і складових ІТС НШСУ (службова пошта, службові акаунти тощо);

- не залишати без контролю після проходження автентифікації під час роботи у віддаленому онлайн-режимі увімкнені незаблоковані підключення до електронних сервісів і служб ІТС НШСУ (електронна пошта, службові акаунти тощо);

- забезпечувати конфіденційність автентифікаційних даних сервісів і служб ІТС НШСУ (логінів, паролів та інших реквізитів доступу), зокрема: додержуватись таємниці, не допускати розголошення або витоку зазначених даних; не зберігати їх у легкодоступних місцях, на робочому столі, у особистих та/або інших комп'ютерах, пам'яті браузера;

- використовувати надійні складні паролі, зокрема такі, що: містять літери, цифри та спеціальні символи (усього не менше 8 символів), які не стосуються персоніфікованих даних та особистої інформації (прізвища та/або ім'я, дати народження, адреси реєстрації номерів телефонів, номерів та серій документів у тому числі автотранспорту, банківської картки тощо);

- експлуатувати під час роботи надані службові технічні і технологічні ресурси ІТС НШСУ, та/або ж в порядку виключення - особисті, що зареєстровані у встановленому порядку, перевірені і дозволені для застосування;

- реєструвати у визначеного працівника відділу інформаційних технологій НШСУ особисті електронні носії інформації, зовнішні

диски та інше обладнання (відеокамери, мікрофони, модеми, маршрутизатори, мобільні телефони тощо) у випадку необхідності підключення до технічних і технологічних ресурсів ІТС НШСУ, здійснювати їх перевірку на наявність шкідливого програмного забезпечення;

- терміново доповідати адміністратору безпеки та/або адміністратору системи ІТС НШСУ про настання позаштатних ситуацій, зокрема: пошкодження обладнання; виявлення ознак кібератак, здійснених на ІТС НШСУ (підозрілої, незрозумілої роботи програмного забезпечення, порушень при роботі з інформацією тощо).

5. Заборони для користувачів

Користувачам забороняється діяти у такий спосіб:

1) розголошувати, повідомляти іншим особам службові логіни, паролі доступу та іншу технологічну інформацію до технологічних ресурсів ІТС НШСУ (електронних скриньок, службових акаунтів, службових комп'ютерів електронних сервісів і служб тощо), у тому числі вводити їх до сторонніх ресурсів при роботі в мережі інтернет, або зберігати їх у легкодоступних місцях, на робочому столі, в пам'яті браузера тощо;

2) надавати доступ іншим особам до користування технічними і технологічними ресурсами ІТС НШСУ (електронними скриньками, службовими акаунтами, комп'ютерами, електронними сервісами і службами);

3) встановлювати, видаляти та вносити зміни в програмне забезпечення на службових комп'ютерах без відповідного дозволу;

4) підключати до службових комп'ютерів стороннє незареєстроване обладнання (електронні носії інформації, відеокамери, мікрофони, модеми, маршрутизатори, мобільні телефони тощо);

5) оперувати ("схвалювати" чи "приймати") із спливаючими вікнами та повідомленнями у браузері користувача, його програмах і операційній системі; відкривати електронні листи, які надійшли з невідомих та підозрілих електронних адрес; не переходити за невідомими посиланнями та не завантажувати файли, що мають потенційно небезпечні розширення (.exe, .bin, .ini, .dll, .com, .sys, .bat, ,js, тощо) та навіть безпечні (.docx, .zip, .pdf), у яких можуть використовуватися вразливості, макроси та інше;

6) вимикати встановлене антивірусне програмне забезпечення або відмовлятися від його оновлення;

7) створювати віддалене підключення (та/або управління) до службових комп'ютерів, інших технологічних ресурсів ІТС НШСУ;

8) підключати до комп’ютерів ІТС НШСУ мережу Інтернет та/або інші глобальні мережі передачі даних за допомогою сторонніх модемів, маршрутизаторів, мобільних телефонів, смартфонів тощо;

9) завантажувати і надсилати інформацію, що циркулює в ІТС НШСУ, до сторонніх ресурсів, якщо це може зашкодити діяльності НШСУ.

6. Відповідальність користувачів

Порушення користувачами вимог цієї Інструкції тягне за собою дисциплінарну і матеріальну відповідальність, передбачену пунктами 4.8.-4.12. глави 4 розділу VII Регламенту НШСУ, а також адміністративну, кримінальну і цивільну відповідальність згідно з чинним законодавством України.