ВИКОНАВЧИЙ ОРГАН КИЇВСЬКОЇ МІСЬКОЇ РАДИ

(КИЇВСЬКА МІСЬКА ДЕРЖАВНА АДМІНІСТРАЦІЯ)

РОЗПОРЯДЖЕННЯ

03.07.2018 № 1135

Про затвердження Положення про забезпечення захисту інформації в інформаційно-телекомунікаційних системах структурних підрозділів виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністрацій, підприємств, установ та організацій, що належать до комунальної власності територіальної громади міста Києва або передані до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації)

Відповідно до законів України «Про місцеве самоврядування в Україні», «Про місцеві державні адміністрації», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основні засади забезпечення кібербезпеки України», «Про захист персональних даних», Положення про технічний захист інформації в Україні, затвердженого Указом Президента України від 27 вересня 1999 року № 1229/99, постанов Кабінету Міністрів України від 08 жовтня 1997 року № 1126 «Про затвердження Концепції технічного захисту інформації в Україні», від 10 вересня 2003 року № 1433 «Про затвердження Порядку використання комп'ютерних програм в органах виконавчої влади», від 29 березня 2006 року № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», враховуючи розпорядження виконавчого органу Київської міської ради (Київської міської державної адміністрації) від 09 жовтня 2017 року № 1250 «Про заходи щодо забезпечення захисту інформації в автоматизованих системах», з метою забезпечення захисту інформації в інформаційно-телекомунікаційних системах та запобігання вірусним атакам на автоматизовані системи:

1. Затвердити Положення про забезпечення захисту інформації в інформаційно-телекомунікаційних системах структурних підрозділів виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністрацій, підприємств, установ та організацій, що належать до комунальної власності територіальної громади міста Києва або передані до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації).

2. Структурним підрозділам виконавчого органу Київської міської ради (Київської міської державної адміністрації), районним в місті Києві державним адміністраціям, підприємствам, установам та організаціям, що належать до комунальної власності територіальної громади міста Києва або передані до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації):

2.1. У разі володіння (адміністрування) інформаційно-телекомунікаційними системами, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимогу щодо захисту якої встановлено законом, утворити службу захисту інформації або визначити відповідальних працівників за захист інформації, на яких покласти обов'язки щодо забезпечення захисту інформації в інформаційно-телекомунікаційних системах.

2.2. Протягом трьох місяців з дня видання цього розпорядження привести програмне забезпечення, що використовується в роботі, у відповідність з Переліком програмного забезпечення, яке допускається для використання у структурних підрозділах виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністраціях, підприємствах, установах та організаціях, що належать до комунальної власності територіальної громади міста Києва або передані до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації), затвердженим Департаментом інформаційно-комунікаційних технологій виконавчого органу Київської міської ради (Київської міської державної адміністрації) у встановленому порядку.

2.3. Забезпечити наповнення Реєстру інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем у структурних підрозділах виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністраціях, підприємствах, установах та організаціях, що належать до комунальної власності територіальної громади міста Києва або передані до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації), після виконання пункту 3 цього розпорядження.

3. Департаменту інформаційно-комунікаційних технологій виконавчого органу Київської міської ради (Київської міської державної адміністрації) до 31 грудня 2018 року спільно з комунальним підприємством «Головний інформаційно-обчислювальний центр» забезпечити в установленому порядку розробку автоматизованої системи для ведення Реєстру інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем у структурних підрозділах виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністраціях, підприємствах, установах та організаціях, що належать до комунальної власності територіальної громади міста Києва або передані до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації).

4. Контроль за виконанням цього розпорядження покласти на заступників голови Київської міської державної адміністрації згідно з розподілом обов'язків.

Голова В. Кличко

ЗАТВЕРДЖЕНО
Розпорядження виконавчого
органу Київської міської ради
(Київської міської державної
адміністрації)
03.07.2018 № 1135

ПОЛОЖЕННЯ
про забезпечення захисту інформації в інформаційно-телекомунікаційних системах структурних підрозділів виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністраціях, підприємствах, установах та організаціях, що належать до комунальної власності територіальної громади міста Києва або передані до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації)

1. Загальні положення

1.1. Положення про забезпечення захисту інформації в інформаційно-телекомунікаційних системах структурних підрозділів виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністрацій, підприємств, установ та організацій, що належать до комунальної власності територіальної громади міста Києва або передані до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації) (далі – Положення), визначає заходи з антивірусного захисту, використання мережі Інтернет та електронної пошти, парольний захист, використання програмного забезпечення, доступ до інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, які перебувають у комунальній власності територіальної громади міста Києва або на які передано майнові права автора, або користувачами чи адміністраторами яких є структурні підрозділи виконавчого органу Київської міської ради (Київської міської державної адміністрації), районні в місті Києві державні адміністрації, підприємства, установи, організації, що належать до комунальної власності територіальної громади міста Києва або передані до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації), а також інші питання захисту інформації в інформаційно-телекомунікаційних системах структурних підрозділів виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністрацій, підприємств, установ та організацій, що належать до комунальної власності територіальної громади міста Києва або передані до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації).

1.2. У цьому Положенні терміни вживаються у значеннях, наведених у законах України «Про захист інформації в інформаційно-телекомунікаційних системах», «Про захист персональних даних», «Про електронні документи та електронний документообіг», «Про основні засади забезпечення кібербезпеки України», постановах Кабінету Міністрів України від 10 вересня 2003 року № 1433 «Про затвердження Порядку використання комп'ютерних програм в органах виконавчої влади», від 29 березня 2006 року № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», Положенні про технічний захист інформації в Україні, затвердженому Указом Президента України від 27 вересня 1999 року № 1229/99, та інших нормативно-правових актах.

1.3. Це Положення є обов'язковим для виконання працівниками всіх структурних підрозділів виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністрацій, підприємств, установ та організацій, що належать до комунальної власності територіальної громади міста Києва або передані до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації), які використовують у роботі комп'ютерну техніку (зокрема і роботі в локальних обчислювальних мережах).

1.4. Контроль за виконанням вимог цього Положення здійснює Департамент інформаційно-комунікаційних технологій виконавчого органу Київської міської ради (Київської міської державної адміністрації), розпорядник та адміністратор інформаційної, телекомунікаційної або інформаційно-телекомунікаційної системи, а також служба захисту інформації (працівники, відповідальні за захист інформації) відповідного структурного підрозділу виконавчого органу Київської міської ради (Київської міської державної адміністрації), районної в місті Києві державної адміністрації, підприємства, установи та організації, що належить до комунальної власності територіальної громади міста Києва або передана до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації) (далі – служба захисту інформації).

2. Заходи з антивірусного захисту

2.1. Заходи з антивірусного захисту здійснюються для запобігання втрат інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах структурних підрозділів виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністрацій, підприємств, установ та організацій, що належать до комунальної власності територіальної громади міста Києва або передані до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації) та зокрема мають на меті:

визначення складу та правил запуску, перевірки та оновлення антивірусного програмного забезпечення;

проведення профілактичних робіт із застосуванням антивірусного програмного забезпечення;

безперервне забезпечення захисту інформації від дії шкідливого програмного забезпечення на всіх етапах експлуатації інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем у структурних підрозділах виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністраціях, підприємствах, установах та організаціях, що належать до комунальної власності територіальної громади міста Києва або передані до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації).

2.2. Проведення заходів з антивірусного захисту здійснює служба захисту інформації.

2.3. До використання у структурних підрозділах виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністраціях, підприємствах, установах та організаціях, що належать до комунальної власності територіальної громади міста Києва або передані до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації), допускається тільки ліцензійне антивірусне програмне забезпечення.

2.4. Інсталяцію засобів антивірусного захисту та налаштування їх параметрів відповідно до технічної документації здійснює служба захисту інформації.

2.5. Оновлення антивірусних баз повинно проводитися автоматично не рідше одного разу на три доби.

У разі збою автоматичного оновлення проводиться ручне оновлення антивірусних баз з тією ж періодичністю.

2.6. Обов'язковій антивірусній перевірці підлягає уся інформація, що отримується та передається через телекомунікаційні канали зв'язку або міститься на носіях (як знімних, так і внутрішніх).

2.7. Файли резервних копій, що переміщуються в систему зберігання даних, повинні в обов'язковому порядку проходити антивірусну перевірку.

2.8. Заходи з антивірусного захисту на автоматизованих робочих місцях мають включати:

запобігання ушкодженню/зараженню комп'ютерними вірусами;

реагування на ушкодження/зараження комп'ютерними вірусами;

використання засобів антивірусного захисту;

проведення перевірки інцидентів, пов'язаних з ушкодженням/зараженням комп'ютерними вірусами.

2.9. З метою недопущення поширення комп'ютерних вірусів на автоматизованих робочих місцях служба захисту інформації повинна регулярно проводити профілактичні заходи, а саме:

щоденну автоматичну перевірку наявності комп'ютерних вірусів за розкладом;

регулярну (не рідше ніж один раз на 3 місяці) вибіркову перевірку автоматизованих робочих місць та серверів на наявність комп'ютерних вірусів, навіть у разі відсутності зовнішніх проявів комп'ютерних вірусів;

перевірку наявності комп'ютерних вірусів на автоматизованих робочих місцях та серверах, які повернулися з ремонту (в тому числі гарантійного) в сторонніх організаціях;

створення резервної копії програмного забезпечення одразу ж після первинного налаштування;

встановлення захисту від запису на знімні носії інформації, де це можливо;

ретельну перевірку всього придбаного програмного забезпечення;

обмеження доступу сторонніх осіб до автоматизованих робочих місць та серверів.

2.10. У разі виявлення комп'ютерних вірусів на автоматизованому робочому місці, розташованому в локальному сегменті мережі, перевірці підлягають усі автоматизовані робочі місця, що є в цьому локальному сегменті мережі або працюють із загальним ресурсом (інформаційною, телекомунікаційною, інформаційно-телекомунікаційною системою тощо).

2.11. У разі повідомлення антивірусним програмним забезпеченням про підозру наявності комп'ютерного вірусу на автоматизованому робочому місці користувачеві потрібно призупинити роботу та негайно повідомити про це службу захисту інформації.

2.12. Служба захисту інформації під час реагування на ушкодження/зараження комп'ютерним вірусом визначає джерело ушкодження/зараження, а саме:

якщо це знімний носій інформації або інше автоматизоване робоче місце, потрібно перевірити їх на наявність комп'ютерних вірусів;

якщо це глобальна мережа Інтернет або електронна пошта, потрібно негайно заблокувати Інтернет-ресурс або адресу електронної пошти.

2.13. Знищення комп'ютерних вірусів здійснює служба захисту інформації.

2.14. Після знищення вірусів та відновлення ушкоджених/заражених комп'ютерним вірусом програм і файлів з даними потрібно ще раз провести перевірку наявності вірусів з використання антивірусного програмного забезпечення.

3. Використання мережі Інтернет та електронної пошти

3.1. Доступ до мережі Інтернет та електронної пошти в структурних підрозділах виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністраціях, підприємствах, установах та організаціях, що належать до комунальної власності територіальної громади міста Києва або передані до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації), здійснюється із застосуванням спеціальних програмно-технічних засобів захисту інформації (міжмережевих екранів, системи фільтрації електронної пошти, захищеного вузла інтернет-доступу).

3.2. На автоматизованих робочих місцях користувачів, підключених до мережі Інтернет, обов'язково має бути встановлено антивірусне програмне забезпечення з актуальною антивірусною базою.

3.3. Доступ до мережі Інтернет надається користувачам з метою виконання ними своїх службових обов'язків, що вимагають безпосереднього підключення до зовнішніх інформаційних ресурсів, для отримання та обміну інформацією, після ознайомлення з цим Положенням під особистий підпис.

3.4. Доступ до корпоративного поштового сервісу надається всім користувачам з метою виконання ними своїх службових обов'язків, що вимагають безпосереднього обміну інформацією каналами електронної пошти, після ознайомлення з цим Положенням під особистий підпис.

3.5. Для доступу користувачів до мережі Інтернет та корпоративного поштового сервісу допускається застосування програмного забезпечення, що входить до Переліку програмного забезпечення, яке допускається для використання у структурних підрозділах виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністраціях, підприємствах, установах та організаціях, що належать до комунальної власності територіальної громади міста Києва або передані до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації), затвердженого Департаментом інформаційно-комунікаційних технологій виконавчого органу Київської міської ради (Київської міської державної адміністрації) у встановленому порядку.

3.6. Доступ користувачам до мережі Інтернет та корпоративного поштового сервісу забезпечується у таких випадках:

необхідності організації автоматизованого робочого місця для працівника;

необхідності виконання працівником нових (додаткових) службових обов'язків, виконання яких потребує доступу до зовнішніх ресурсів.

3.7. Надання користувачам доступу до мережі Інтернет та корпоративного поштового сервісу здійснюється у порядку, визначеному главою 6 цього Положення.

3.8. Під час використання мережі Інтернет та електронної пошти користувачі повинні:

3.8.1. Використовувати мережу Інтернет виключно для виконання своїх посадових обов'язків.

3.8.2. Ознайомитися з типовими загрозами під час роботи з мережею Інтернет та електронною поштою, дотримуватися рекомендацій щодо їх запобігання, визначених у додатку 1 до цього Положення.

3.8.3. Дотримуватися вимог, викладених у главі 3 цього Положення.

3.8.4. Уживати загальних заходів захисту під час роботи з мережею Інтернет та електронною поштою, визначених у додатку 2 до цього Положення.

3.8.5. Інформувати службу захисту інформації про будь-які факти порушення вимог глави 3 цього Положення.

3.9. Під використання мережі Інтернет та електронної пошти користувачам заборонено:

3.9.1. Використовувати наданий структурним підрозділам виконавчого органу Київської міської ради (Київської міської державної адміністрації), районним в місті Києві державним адміністраціям, підприємствам, установам та організаціям, що належать до комунальної власності територіальної громади міста Києва або передані до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації), доступ до мережі Інтернет та електронної пошти для особистих потреб.

3.9.2. Використовувати спеціалізовані апаратні та програмні засоби, що дають змогу користувачам отримати несанкціонований доступ до мережі Інтернет та електронної пошти.

3.9.3. Опубліковувати, завантажувати та поширювати матеріали, які містять:

конфіденційну інформацію, а також інформацію, що становить таємницю, персональні дані, за винятком випадків, коли це входить до посадових обов'язків та забезпечується захист інформації під час передачі даних відкритими каналами зв'язку;

інформацію, повністю або частково захищену правами інтелектуальної власності, без дозволу суб'єкта права інтелектуальної власності;

шкідливе програмне забезпечення, призначене для порушення, знищення або обмеження функціональності будь-яких апаратних та програмних засобів, для здійснення несанкціонованого доступу, а також серійні номери до

комерційного програмного забезпечення та програмне забезпечення для їх генерації, паролі та інші засоби для отримання несанкціонованого доступу до інтернет-ресурсів, а також посилання на зазначену вище інформацію;

інформацію, що ображає честь та гідність інших осіб, спрямовану на розпалювання національної, расової чи релігійної ворожнечі та ненависті, на приниження національної честі та гідності або образу почуттів громадян у зв'язку з їхніми релігійними переконаннями.

3.9.4. Фальсифікувати свою IP-адресу, а також іншу технологічну інформацію.

3.9.5. Поширювати та інсталювати на інших автоматизованих робочих місцях користувачів будь-яке програмне забезпечення, отримане з використанням мережі Інтернет та електронної пошти.

3.9.6. Здійснювати спроби несанкціонованого доступу до ресурсів мережі Інтернет, проведення мережевих атак та мережевого злому, участь у них.

3.9.7. Переходити за посиланнями та відкривати вкладені файли вхідних електронних повідомлень, отриманих від невідомих адресатів.

3.9.8. З власної ініціативи здійснювати розсилку (зокрема і масову) електронних повідомлень, якщо розсилка не пов'язана з виконанням посадових обов'язків.

3.9.9. Використовувати адресу корпоративного поштового сервісу для отримання періодичної розсилки матеріалів з мережі Інтернет, не пов'язаних з виконанням посадових обов'язків.

3.9.10. Опубліковувати адресу корпоративного поштового сервісу (свою або інших працівників) на загальнодоступних інтернет-ресурсах (форуми, конференції, соціальні мережі тощо), якщо це не пов'язано зі службовою потребою.

3.9.11. Надавати третім особам доступ до своєї корпоративної поштової скриньки.

3.9.12. Перенаправляти електронні повідомлення з особистих поштових скриньок на адресу корпоративного поштового сервісу.

3.9.13. Використовувати як паролі для доступу до ресурсів корпоративного поштового сервісу аналогічні паролі, що використовуються для доступу до інших ресурсів мережі Інтернет.

3.9.14. Відключати встановлене на автоматизованому робочому місці антивірусне програмне забезпечення.

3.9.15. Використовувати зовнішні ресурси електронної пошти для виконання посадових (службових) або трудових обов'язків.

3.10. Зміст інтернет-ресурсів, а також файли, що завантажуються з мережі Інтернет та корпоративного поштового сервісу, підлягають обов'язковій перевірці на відсутність шкідливого програмного забезпечення.

3.11. Інформація про відвідання користувачами інтернет-ресурсів протоколюється для подальшого аналізу та в разі необхідності може бути надана керівникові відповідного структурного підрозділу виконавчого органу

Київської міської ради (Київської міської державної адміністрації), районної в місті Києві державної адміністрації, підприємства, установи та організації, що належить до комунальної власності територіальної громади міста Києва або передана до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації), для контролю.

3.12. Департамент інформаційно-комунікаційних технологій виконавчого органу Київської міської ради (Київської міської державної адміністрації) має право обмежувати доступ користувачів до інтернет-ресурсів, зміст яких не стосується виконання посадових обов'язків, або які заборонено законодавством України.

У зазначених в абзаці першому цього пункту випадках Департамент інформаційно-комунікаційних технологій виконавчого органу Київської міської ради (Київської міської державної адміністрації) дає доручення адміністраторові відповідної системи (сервісу) про відключення автоматизованого робочого місця користувача від мережі Інтернет та/або заблокування електронної пошти з повідомленням про це керівництва відповідного структурного підрозділу виконавчого органу Київської міської ради (Київської міської державної адміністрації), районної в місті Києві державної адміністрації, підприємства, установи та організації, що належить до комунальної власності територіальної громади міста Києва або передана до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації).

4. Парольний захист

4.1. Особисті паролі користувачів, зокрема і паролі облікових записів в автоматизованих системах, користувачі повинні обирати з урахуванням таких вимог:

довжина пароля має становити не менше ніж 8 символів;

серед символів пароля обов'язково мають бути літери, цифри та/або спеціальні символи (@, #, $, &, *, % тощо), окрім автоматизованих систем, у яких використання таких символів є неприпустимим з технічних причин;

пароль не повинен включати легко обчислювані поєднання символів (імена, прізвища, назви робочих станцій тощо), а також загальноприйняті скорочення і терміни (qwerty, pa$$w0rd тощо);

у разі зміни пароля новий пароль має відрізнятися від старого не менше, ніж двома символами.

4.2. Паролі адміністративних облікових записів, які використовуються для управління роботою автоматизованих систем, повинні обиратися з урахуванням таких вимог:

довжина пароля має становити не менше ніж 12 символів;

серед символів пароля обов'язково мають бути цифри та/або спеціальні символи (@, #, $, &, *, % тощо), окрім автоматизованих систем, у яких використання таких символів є неприпустимим з технічних причин;

пароль не повинен включати легко обчислювані поєднання символів (імена, прізвища, назви робочих станцій тощо), а також загальноприйняті скорочення і терміни (qwerty, pa$$w0rd тощо), пароль не повинен бути словом української, російської або англійської мови, в якому замінено деякі символи (o = 0, s = $, a = @ тощо);

у разі зміни пароля новий пароль має відрізнятися від старого не менше, ніж чотирма символами, розташованими не підряд;

у разі створення паролів адміністративних облікових записів можливе використання спеціалізованого програмного забезпечення для генерації складних для підбору паролів.

4.3. Стандартні локальні облікові записи користувачів (Guest, User тощо) потрібно заблокувати (деактивувати) під час первинного налаштування операційної системи.

4.4. Створення та використання локальних облікових записів користувачів на автоматизованих робочих місцях, підключених до домену kmda.gov.ua або до будь-якого іншого домену, користувачам заборонено.

4.5. Вбудований локальний адміністративний обліковий запис має бути захищений паролем згідно з пунктом 4.2 цього Положення.

4.6. BIOS (Basic Input/Output System, базова система введення/виведення) автоматизованих робочих місць у складі автоматизованих систем структурних підрозділів виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністрацій, підприємств, установ та організацій, що належать до комунальної власності територіальної громади міста Києва або передані до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації), має бути захищений паролем згідно з пунктом 4.2 цього Положення.

4.7. Користувачам забороняється повідомляти пароль іншим особам, а також зберігати записаний пароль у загальнодоступних місцях.

4.8. У разі проведення службою захисту інформації перевіркових заходів, можливе скидання пароля користувача для доступу до облікового запису.

Після закінчення перевіркових заходів обов'язково встановлюється параметр «Вимагати зміну пароля під час наступного входу в систему», а користувачі під час наступного входу в систему самостійно змінюють пароль на новий.

4.9. У разі виникнення нестандартних ситуацій або технічної необхідності зміни імені та/або пароля користувача під час його відсутності допускається зміна паролів адміністратором автоматизованої системи. В таких випадках, користувачі, чиї паролі було змінено, зобов'язані одразу ж після з'ясування факту зміни своїх паролів, створити їх нові значення.

4.10. Управління доменними обліковими записами користувачів здійснюється з урахуванням принципу мінімально потрібних привілеїв, тобто користувач має право доступу як до локальної системи, так і до ресурсів автоматизованої системи не більше, ніж це потрібно йому для виконання своїх посадових обов'язків.

4.11. Повна планова зміна паролів користувачів проводиться регулярно, не рідше ніж один раз на шість місяців. Планова зміна паролів передбачає інформування користувача про необхідність зміни пароля та можливість його зміни без звернення до адміністратора автоматизованої системи та служби захисту інформації.

4.12. Позапланову зміну особистого пароля або видалення облікового запису користувача автоматизованої системи в разі припинення його повноважень (звільнення, перехід на роботу в інший підрозділ тощо) проводить адміністратор автоматизованої системи негайно після закінчення останнього сеансу роботи такого користувача в автоматизованій системі.

4.13. Позапланова повна зміна паролів всіх користувачів проводиться в разі припинення повноважень (звільнення, перехід на роботу в інший підрозділ тощо) адміністратора автоматизованої системи або інших працівників, яким було надано повноваження з управління парольним захистом автоматизованої системи.

4.14. У разі тривалої відсутності (більше ніж 30 календарних днів) користувача автоматизованої системи (відрядження, хвороба, відпустка для догляду за дитиною до досягнення нею трирічного віку) його обліковий запис блокується та в разі потреби змінюються права доступу інших користувачів щодо ресурсів такого користувача.

4.15. У разі компрометації особистого пароля користувача автоматизованої системи або підозри на компрометацію негайно вживаються заходи щодо позапланової зміни особистого пароля самим користувачем з негайним інформуванням про це служби захисту інформації.

4.16. Зміну забутого пароля користувача здійснює адміністратор автоматизованої системи на підставі повідомлення з обов'язковим встановленням параметра «Вимагати зміну пароля під час наступного входу в систему».

4.17. Для запобігання підбору паролів адміністратор автоматизованої системи налаштовує механізм блокування облікового запису на 20 хвилин у разі п'яти випадків неправильного введення пароля.

4.18. У разі тимчасового залишення автоматизованого робочого місця протягом робочого дня користувач в обов'язковому порядку повинен його заблоковувати (в операційній системі Windows натисканням комбінації клавіш «Win + L»).

4.19. Для надання тимчасового доступу до ресурсів автоматизованих систем (для осіб, які не є працівниками структурних підрозділів виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністрацій, підприємств, установ та організацій, що належать до комунальної власності територіальної громади міста Києва або передані до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації), або для працівників, яким потрібно отримати тимчасовий доступ до ресурсів автоматизованих систем тощо), використовується процедура тимчасових облікових записів.

4.20. Тимчасовий обліковий запис – обліковий запис, що має обмеження за часом дії та обмежені права щодо доступу. Для тимчасових облікових записів проводиться протоколювання їх використання.

Процедура отримання тимчасових облікових записів полягає в такому:

працівник структурного підрозділу виконавчого органу Київської міської ради (Київської міської державної адміністрації), районної в місті Києві державної адміністрації, підприємства, установи та організації, що належить до комунальної власності територіальної громади міста Києва або передана до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації), через керівника свого структурного підрозділу оформлює у встановленому порядку заявку на надання доступу до автоматизованої системи із зазначенням мети тимчасового облікового запису та меж його використання;

заявка надсилається структурному підрозділу виконавчого органу Київської міської ради (Київської міської державної адміністрації), районній в місті Києві державній адміністрації, підприємству, установі або організації, що належить до комунальної власності територіальної громади міста Києва або передана до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації), яка є розпорядником автоматизованої системи, для розгляду;

тимчасовий обліковий запис створює адміністратор автоматизованої системи;

користувача, який отримав тимчасовий обліковий запис, адміністратор автоматизованої системи інформує про обмеження, пов'язані з його використанням.

4.21. Адміністративні облікові записи створюються з урахуванням принципу мінімально потрібних повноважень у системі та лише особам, визначеним адміністраторами в установленому порядку.

4.22. Використання облікових записів адміністратора в щоденній роботі, не пов'язаній з необхідністю їх використання (інсталяція, конфігурація, відновлення операційної системи, сервісів тощо), забороняється.

У разі необхідності запуску програми під обліковим записом адміністратора користувач зобов'язаний використовувати команду «Run As» або «вторинний вхід у систему».

4.23. Обліковий запис адміністратора домену використовується тільки в разі інсталяції, конфігурування, відновлення контролера домену та інших дій, за яких використання інших облікових записів є неможливим.

4.24. Для служб і сервісів, що працюють в операційних системах на серверах автоматизованих систем, встановлюються мінімально потрібні повноваження для їх коректної роботи.

4.25. Сервери критичного ступеня безпеки (контролери домену, сервери баз даних, інші сервери, від яких залежить безперебійна робота автоматизованих систем) мають відповідати підвищеним вимогам до мінімізації привілеїв доступу з боку як віддалених, так і локальних користувачів і служб.

4.26. У разі компроментації або підозри компрометації адміністративного облікового запису здійснюється позапланова зміна паролів усіх залежних від нього облікових записів.

4.27. Для підвищення ступеня захисту критично важливих автоматизованих систем (об'єктів критичної інформаційної інфраструктури) від несанкціонованого доступу використовується двофакторна автентифікація (паролем та електронним цифровим підписом на носії ключової інформації).

4.28. У разі припинення необхідності використання носія особистого ключа (звільнення користувача, припинення функціонування об'єкта тощо) інформація з такого носія стирається або знищується сам носій у разі неможливості його очищення.

4.29. Користувачам автоматизованих систем категорично забороняється залишати без особистого нагляду, а також передавати іншим особам носії особистого ключа, повідомляти паролі від носія особистого ключа.

4.30. У разі втрати носія особистого ключа користувач зобов'язаний негайно повідомити про це керівника свого структурного підрозділу та службу захисту інформації.

4.31. Щоденний контроль за дотриманням вимог глави 4 цього Положення полягає в контролі процесів використання та зміни облікових записів, процесів доступу до ресурсів, процесів зміни облікових записів, надання доступу до ресурсів автоматизованої системи.

4.32. Служба захисту інформації здійснює щоквартальний вибірковий контроль за виконанням працівниками відповідного структурного підрозділу виконавчого органу Київської міської ради (Київської міської державної адміністрації), районної в місті Києві державної адміністрації, підприємства, установи або організації, що належить до комунальної власності територіальної громади міста Києва або передана до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації), вимог глави 4 цього Положення.

Про факти невідповідності якості паролів або умов забезпечення їх збереження служба захисту інформації письмово повідомляє керівника відповідного структурного підрозділу виконавчого органу Київської міської ради (Київської міської державної адміністрації), районної в місті Києві державної адміністрації, підприємства, установи або організації, що належить до комунальної власності територіальної громади міста Києва або передана до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації).

4.33. Контроль за виконанням вимог глави 4 цього Положення покладається на службу захисту інформації та адміністратора відповідної інформаційної, телекомунікаційної або інформаційно-телекомунікаційної системи.

5. Використання програмного забезпечення

5.1. З метою автоматизації виробничої, управлінської, допоміжної діяльності у структурних підрозділах виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністраціях, підприємствах, установах та організаціях, що належать до комунальної власності територіальної громади міста Києва або передані до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації), допускається використання програмного забезпечення, визначеного в Переліку програмного забезпечення, яке допускається для використання у структурних підрозділах виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністраціях, підприємствах, установах та організаціях, що належать до комунальної власності територіальної громади

міста Києва або передані до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації).

5.2. Перелік програмного забезпечення, яке допускається для використання у структурних підрозділах виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністраціях, підприємствах, установах та організаціях, що належать до комунальної власності територіальної громади міста Києва або передані до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації), затверджує Департамент інформаційно-комунікаційних технологій виконавчого органу Київської міської ради (Київської міської державної адміністрації) у встановленому порядку.

5.3. У разі необхідності використання в роботі програмного забезпечення, якого немає в Переліку програмного забезпечення, яке допускається для використання у структурних підрозділах виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністраціях, підприємствах, установах та організаціях, що належать до комунальної власності територіальної громади міста Києва або передані до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації), Департамент інформаційно-комунікаційних технологій виконавчого органу Київської міської ради (Київської міської державної адміністрації) вносить відповідні зміни до Переліку програмного забезпечення, яке допускається для використання у структурних підрозділах виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністраціях, підприємствах, установах та організаціях, що належать до комунальної власності територіальної громади міста Києва або передані до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації), у встановленому порядку на підставі письмового звернення структурного підрозділу виконавчого органу Київської міської ради (Київської міської державної адміністрації), районної в місті Києві державної адміністрації, підприємства, установи та організації, що належить до комунальної власності територіальної громади міста Києва або передана до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації).

5.4. Склад встановленого програмного забезпечення на кожному автоматизованому робочому місці визначається на підставі виробничих потреб, посадових (службових) або трудових обов'язків та переліку інформаційних ресурсів, до яких отримує доступ користувач.

5.5. Опис конфігурації автоматизованого робочого місця та перелік встановленого програмного забезпечення фіксується в Реєстрі інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем у структурних

підрозділах виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністраціях, підприємствах, установах та організаціях, що належать до комунальної власності територіальної громади міста Києва або передані до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації).

5.6. Усі дії щодо встановлення та видалення програмного забезпечення виконуються безпосередньо або за участю служби захисту інформації відповідного структурного підрозділу виконавчого органу Київської міської ради (Київської міської державної адміністрації), районної в місті Києві державної адміністрації, підприємства, установи або організації, що належить до комунальної власності територіальної громади міста Києва або передана до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації).

5.7. Забороняється зміна конфігурації апаратних засобів та/або програмного забезпечення автоматизованих робочих місць та серверів без погодження зі службою захисту інформації відповідного структурного підрозділу виконавчого органу Київської міської ради (Київської міської державної адміністрації), районної в місті Києві державної адміністрації, підприємства, установи або організації, що належить до комунальної власності територіальної громади міста Києва або передана до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації).

Роботи щодо зміни конфігурації автоматизованих робочих місць виконуються у присутності працівника служби захисту інформації відповідного структурного підрозділу виконавчого органу Київської міської ради (Київської міської державної адміністрації), районної в місті Києві державної адміністрації, підприємства, установи або організації, що належить до комунальної власності територіальної громади міста Києва або передана до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації), та користувача цього автоматизованого робочого місця.

5.8. Під час експлуатації програмного забезпечення користувачам потрібно:

дотримуватися вимог цього Положення;

використовувати встановлене на автоматизованому робочому місці програмне забезпечення виключно для виконання своїх службових обов'язків;

забезпечувати збереження переданих у складі автоматизованих робочих місць сертифікатів автентичності програмного забезпечення, наклеєних на корпус системного блоку;

сприяти адміністраторам у виконанні робіт щодо встановлення, налаштування, усунення несправностей та аудиту встановленого програмного забезпечення;

інформувати службу захисту інформації про будь-які факти порушення вимог цього Положення.

5.9. Під час експлуатації програмного забезпечення користувачам заборонено:

використовувати автоматизоване робоче місце для інших цілей, не пов'язаних з виконанням своїх посадових (службових) або трудових обов'язків;

самостійно вносити зміни в конструкцію, конфігурацію, розміщення автоматизованого робочого місця та іншого обладнання автоматизованих систем;

змінювати склад встановленого на автоматизованому робочому місці програмного забезпечення (встановлювати нове, змінювати склад компонентів, видаляти програмне забезпечення тощо);

приносити на знімних носіях інформації, завантажувати та несанкціоновано запускати на своєму або іншому автоматизованому робочому місці будь-яке програмне забезпечення.

5.10. Запит (доручення) на встановлення програмного забезпечення може бути ініційований керівником структурного підрозділу виконавчого органу Київської міської ради (Київської міської державної адміністрації), районної в місті Києві державної адміністрації, підприємства, установи або організації, що належить до комунальної власності територіальної громади міста Києва або передана до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації), на підставі доповідної записки за підписом безпосереднього керівника структурного підрозділу, в якому працює користувач, у таких випадках:

необхідності організації автоматизованого робочого місця для нового працівника;

необхідності виконання працівниками нових (додаткових) обов'язків, виконання яких потрібує додаткового програмного забезпечення або повної заміни автоматизованого робочого місця;

появи якісно нового (альтернативного) програмного забезпечення, замість того, що використовується у складі автоматизованого робочого місця користувача.

У зазначених в цьому пункті випадках керівник структурного підрозділу виконавчого органу Київської міської ради (Київської міської державної адміністрації), районної в місті Києві державної адміністрації, підприємства, установи або організації, що належить до комунальної власності територіальної громади міста Києва або передана до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації):

дає доручення системному адміністраторові відповідного структурного підрозділу виконавчого органу Київської міської ради (Київської міської

державної адміністрації), районної в місті Києві державної адміністрації, підприємства, установи або організації, що належить до комунальної власності територіальної громади міста Києва або передана до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації) (у разі наявності повноважень у системного адміністратора на встановлення програмного забезпечення);

направляє запит на встановлення програмного забезпечення розпорядникові відповідної інформаційної, телекомунікаційної або інформаційно-телекомунікаційної системи (якщо розпорядником інформаційної, телекомунікаційної або інформаційно-телекомунікаційної системи є інший структурний підрозділ виконавчого органу Київської міської ради (Київської міської державної адміністрації), районна в місті Києві державна адміністрація, підприємство, установа або організація, що належить до комунальної власності територіальної громади міста Києва або передана до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації)).

5.11. Запит служби захисту інформації про встановлення програмного забезпечення, функціональність якого пов'язана із захистом інформації, подається у таких випадках:

усунення вразливостей систем інформаційної безпеки;

необхідності встановлення програмного забезпечення для захисту інформації.

У зазначених в цьому пункті випадках запит на встановлення програмного забезпечення подається системному адміністраторові відповідного структурного підрозділу виконавчого органу Київської міської ради (Київської міської державної адміністрації), районної в місті Києві державної адміністрації, підприємства, установи або організації, що належить до комунальної власності територіальної громади міста Києва або передана до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації), або розпорядникові відповідної інформаційної, телекомунікаційної, інформаційно-телекомунікаційної системи.

5.12. У разі недостатнього обсягу ліцензій на програмне забезпечення або відсутності програмного забезпечення в Переліку програмного забезпечення, яке допускається для використання у структурних підрозділах виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністраціях, підприємствах, установах та організаціях, що належать до комунальної власності територіальної громади міста Києва або передані до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації), керівник структурного підрозділу виконавчого органу Київської міської ради (Київської міської державної адміністрації), районної в місті Києві державної адміністрації, підприємства, установи або організації, що належить до комунальної власності територіальної громади міста Києва або

передана до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації), подає Департаменту інформаційно-комунікаційних технологій виконавчого органу Київської міської ради (Київської міської державної адміністрації) заявку на придбання додаткових ліцензій або придбання необхідного програмного забезпечення.

5.13. Перед встановленням програмного забезпечення служба захисту інформації здійснює його перевірку на працездатність, відсутність небезпечних функцій та недокументованих можливостей, антивірусну перевірку.

5.14. Після встановлення програмного забезпечення працівник служби захисту інформації вносить відомості про встановлене програмне забезпечення до Реєстру інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем у структурних підрозділах виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністраціях, підприємствах, установах та організаціях, що належать до комунальної власності територіальної громади міста Києва або передані до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації).

5.15. Підтримку та супровід програмного забезпечення здійснюють:

системні адміністратори адміністратора інформаційної, телекомунікаційної, інформаційно-телекомунікаційної системи;

системні адміністратори відповідного структурного підрозділу виконавчого органу Київської міської ради (Київської міської державної адміністрації), районної в місті Києві державної адміністрації, підприємства, установи або організації, що належить до комунальної власності територіальної громади міста Києва або передана до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації);

інші системні адміністратори на договірних засадах.

5.16. Підтримка та супровід програмного забезпечення полягає у проведенні таких видів робіт:

налагодження та адаптація;

встановлення оновлень;

створення резервних копій (архівування);

усунення несправностей, пов'язаних з використанням;

консультування користувачів з питань використання.

5.17. Проведення робіт з підтримки та супроводу програмного забезпечення може бути ініційовано користувачем автоматизованого робочого місця або безпосередньо системним адміністратором відповідного структурного підрозділу виконавчого органу Київської міської ради (Київської міської державної адміністрації), районної в місті Києві державної адміністрації, підприємства, установи або організації, що належить до

комунальної власності територіальної громади міста Києва або передана до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації).

5.18. Будь-які зміни, що виникли під час проведення робіт з підтримки та супроводу програмного забезпечення або апаратних засобів, відображаються в Реєстрі інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем у структурних підрозділах виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністраціях, підприємствах, установах та організаціях, що належать до комунальної власності територіальної громади міста Києва або передані до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації).

5.19. Програмне забезпечення виводиться з експлуатації в таких випадках:

закінчення ліцензійного терміну використання програмного забезпечення;

заміна використовуваного програмного забезпечення на альтернативне;

припинення використання програмного забезпечення у зв'язку з відсутністю потреби, моральним старінням або виходом з ладу;

заборона використання програмного забезпечення.

5.20. Виведення програмного забезпечення з експлуатації здійснює системний адміністратор відповідного структурного підрозділу виконавчого органу Київської міської ради (Київської міської державної адміністрації), районної в місті Києві державної адміністрації, підприємства, установи або організації, що належить до комунальної власності територіальної громади міста Києва або передана до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації).

5.21. Після виведення програмного забезпечення з експлуатації здійснюється відповідний запис у Реєстру інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем у структурних підрозділах виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністраціях, підприємствах, установах та організаціях, що належать до комунальної власності територіальної громади міста Києва або передані до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації).

5.22. Системний адміністратор відповідного структурного підрозділу виконавчого органу Київської міської ради (Київської міської державної адміністрації), районної в місті Києві державної адміністрації, підприємства,

установи або організації, що належить до комунальної власності територіальної громади міста Києва або передана до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації), в разі необхідності, забезпечує збереження призначених для користувача даних, налаштувань, які містяться у програмному забезпеченні, що видаляється, шляхом резервного копіювання.

5.23. Аудит використання програмного забезпечення проводиться з метою виявлення невідповідності фактично встановленого програмного забезпечення перелікам, зафіксованим у Реєстрі інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем у структурних підрозділах виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністраціях, підприємствах, установах та організаціях, що належать до комунальної власності територіальної громади міста Києва або передані до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації), а також порушень вимог цього Положення.

5.24. Аудит використання програмного забезпечення проводить служба захисту інформації відповідного структурного підрозділу виконавчого органу Київської міської ради (Київської міської державної адміністрації), районної в місті Києві державної адміністрації, підприємства, установи або організації, що належить до комунальної власності територіальної громади міста Києва або передана до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації), а також Департамент інформаційно-комунікаційних технологій виконавчого органу Київської міської ради (Київської міської державної адміністрації).

5.25. Для проведення аудиту використання програмного забезпечення може застосовуватися спеціалізоване програмне забезпечення.

5.26. У разі виявлення несанкціонованого встановлення програмного забезпечення таке програмне забезпечення підлягає негайному видаленню, а фактично встановлене програмне забезпечення на автоматизованому робочому місці користувача приводиться у відповідність з переліком програмного забезпечення, зазначеним у Реєстрі інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем у структурних підрозділах виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністраціях, підприємствах, установах та організаціях, що належать до комунальної власності територіальної громади міста Києва або передані до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації).

5.27. Якщо програмне забезпечення встановлено санкціоновано, але не зазначено в Реєстрі інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем у структурних підрозділах виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністраціях, підприємствах, установах та організаціях, що належать до комунальної власності територіальної громади міста Києва або передані до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації), посадова особа, що проводить аудит використання програмного забезпечення, дає доручення відповідному системному адміністраторові щодо внесення змін до Реєстру інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем у структурних підрозділах виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністраціях, підприємствах, установах та організаціях, що належать до комунальної власності територіальної громади міста Києва або передані до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації).

5.28. Плановий аудит використання програмного забезпечення проводиться щодо всіх автоматизованих робочих місць, що використовуються, не менше ніж один раз на рік.

5.29. Позаплановий аудит використання програмного забезпечення (повний або вибірковий) проводиться в міру потреби.

Необхідність, час та обсяг проведення позачергових аудитів визначає служба захисту інформації відповідного структурного підрозділу виконавчого органу Київської міської ради (Київської міської державної адміністрації), районної в місті Києві державної адміністрації, підприємства, установи або організації, що належить до комунальної власності територіальної громади міста Києва або передана до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації), а також Департамент інформаційно-комунікаційних технологій виконавчого органу Київської міської ради (Київської міської державної адміністрації) відповідно до цього Положення.

6. Доступ до інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем

6.1. Надання і припинення доступу до інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем працівникам структурних підрозділів виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністрацій, підприємств, установ та організацій, що належать до комунальної власності територіальної громади міста Києва або передані до сфери управління виконавчого органу Київської міської ради (Київської міської

державної адміністрації), здійснює розпорядник інформаційної, телекомунікаційної та інформаційно-телекомунікаційної системи.

6.2. Користувачі допускаються до роботи з інформаційними, телекомунікаційними та інформаційно-телекомунікаційними системами тільки після ознайомлення з главою 6 цього Положенням та проходження інструктажу, проведеного службою захисту інформації.

6.3. Діяльність користувачів під час роботи з інформаційними, телекомунікаційними та інформаційно-телекомунікаційними системами може протоколюватися та періодично перевірятися на предмет дотримання вимог положення роботи в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах структурних підрозділів виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністрацій, підприємств, установ та організацій, що належать до комунальної власності територіальної громади міста Києва або передані до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації), будь-якими засобами, що не суперечать законодавству України.

6.4. Інформаційні, телекомунікаційні та інформаційно-телекомунікаційні системи структурних підрозділів виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністрацій, підприємств, установ та організацій, що належать до комунальної власності територіальної громади міста Києва або передані до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації), вносяться до Реєстру інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем у структурних підрозділах виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністраціях, підприємствах, установах та організаціях, що належать до комунальної власності територіальної громади міста Києва або передані до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації).

6.5. Наповнення Реєстру інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем у структурних підрозділах виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністраціях, підприємствах, установах та організаціях, що належать до комунальної власності територіальної громади міста Києва або передані до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації), потрібною інформацією та її актуалізацію здійснює відповідний структурний підрозділ виконавчого органу Київської міської ради (Київської міської державної адміністрації), районна в місті Києві державна

адміністрація, підприємство, установа або організація, що належить до комунальної власності територіальної громади міста Києва або передана до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації).

6.6. Ведення Реєстру інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем у структурних підрозділах виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністраціях, підприємствах, установах та організаціях, що належать до комунальної власності територіальної громади міста Києва або передані до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації), здійснює Департамент інформаційно-комунікаційних технологій виконавчого органу Київської міської ради (Київської міської державної адміністрації).

6.7. Форму Реєстру інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем у структурних підрозділах виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністраціях, підприємствах, установах та організаціях, що належать до комунальної власності територіальної громади міста Києва або передані до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації), затверджує Департамент інформаційно-комунікаційних технологій виконавчого органу Київської міської ради (Київської міської державної адміністрації) у встановленому порядку.

6.8. Інформація про нову інформаційну, телекомунікаційну та інформаційно-телекомунікаційну систему структурного підрозділу виконавчого органу Київської міської ради (Київської міської державної адміністрації), районної в місті Києві державної адміністрації, підприємства, установи або організації, що належить до комунальної власності територіальної громади міста Києва або передана до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації), та зміни в наявній системі доводиться до відома Департаменту інформаційно-комунікаційних технологій виконавчого органу Київської міської ради (Київської міської державної адміністрації) протягом п'яти робочих днів з моменту появи таких змін.

6.9. Внесення змін до Реєстру інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем у структурних підрозділах виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністраціях, підприємствах, установах та організаціях, що належать до комунальної власності територіальної громади міста Києва або передані до сфери

управління виконавчого органу Київської міської ради (Київської міської державної адміністрації), здійснюється протягом п'яти робочих днів з дня надходження відповідної інформації, зазначеної в пункті 6.8 цього Положення.

6.10. Доступ до інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем надається користувачам для:

виконання посадових (службових) або трудових обов'язків.

проведення технічних та інших робіт з налагодження функціонування інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем третіми особами.

6.11. Для отримання доступу до інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем розпорядникові відповідної інформаційної, телекомунікаційної або інформаційно-телекомунікаційної системи подається заявка про надання доступу за підписом керівника відповідного структурного підрозділу виконавчого органу Київської міської ради (Київської міської державної адміністрації), районної в місті Києві державної адміністрації, підприємства, установи або організації, що належить до комунальної власності територіальної громади міста Києва або передана до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації).

6.12. Розпорядник відповідної інформаційної, телекомунікаційної або інформаційно-телекомунікаційної системи протягом трьох робочих днів з дня отримання заявки про надання доступу перевіряє наявність у користувача підстав на отримання доступу до інформаційної, телекомунікаційної або інформаційно-телекомунікаційної системи та в разі позитивних результатів розгляду дає доручення адміністраторові відповідної інформаційної, телекомунікаційної або інформаційно-телекомунікаційної системи щодо здійснення фактичного надання доступу до відповідної системи.

6.13. Інформація про всіх користувачів, яким надається доступ до інформаційної, телекомунікаційної або інформаційно-телекомунікаційної системи, фіксується у відповідному журналі заявок про надання доступу до системи, який веде адміністратор відповідної інформаційної, телекомунікаційної або інформаційно-телекомунікаційної системи.

6.14. Використання інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем здійснюється відповідно до методичних документів для користування відповідною інформаційною, телекомунікаційною та інформаційно-телекомунікаційною системою (регламент системи, інструкція користувача, інструкція адміністратора тощо).

6.15. Забороняється умисне виведення інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем з ладу,

блокування доступу до них та будь-які інші дії, що перешкоджають нормальному режиму експлуатації цих систем.

6.16. У разі виявлення збою в роботі інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем користувач зобов'язаний повідомити про це службу захисту інформації.

6.17. У разі потреби в розширенні або зміні (повній або частковій) користувачеві рівня доступу до інформаційної, телекомунікаційної або інформаційно-телекомунікаційної системи, до якої у нього вже є доступ, подається відповідна заявка згідно з пунктом 6.11 цього Положення.

6.18. Доступ до інформаційної, телекомунікаційної або інформаційно-телекомунікаційної системи припиняється користувачам з таких підстав:

зміни посадових обов'язків користувача;

закінчення терміну дії заявки про надання доступу;

зміни технологічних процесів обробки інформації таким чином, що доступ користувачеві до системи більше не потрібен;

порушення користувачем положення та/або регламенту роботи, інструкції користувача, правил доступу та інших методичних документів для користування інформаційною, телекомунікаційною або інформаційно-телекомунікаційною системою;

вихід користувача у відпустку по догляду за дитиною;

звільнення користувача;

в інших випадках, передбачених положенням та/або регламентом роботи відповідної системи, інструкцією користувача та іншими методичними документами для користування інформаційною, телекомунікаційною або інформаційно-телекомунікаційною системою.

6.19. У разі виникнення підстав для припинення доступу до інформаційної, телекомунікаційної або інформаційно-телекомунікаційної системи, зазначених у пункті 6.18 цього Положення:

зміни посадових обов'язків, звільнення, надання відпустки для догляду за дитиною по досягненню нею трирічного віку, зміни технологічних процесів обробки інформації таким чином, що доступ користувачеві до системи більше не потрібен, – керівник структурного підрозділу виконавчого органу Київської міської ради (Київської міської державної адміністрації), районної в місті Києві державної адміністрації, підприємства, установи або організації, що належить до комунальної власності територіальної громади міста Києва або передана до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації), в якому працює користувач, протягом одного робочого дня з моменту виникнення таких підстав надсилає розпорядникові відповідної системи лист про припинення користувачу доступу до системи;

закінчення терміну дії заявки про надання доступу, порушення користувачем положення та/або регламенту роботи, інструкції користувача,

правил доступу або інших методичних документів для користування інформаційною, телекомунікаційною або інформаційно-телекомунікаційною системою – адміністратор відповідної інформаційної, телекомунікаційної або інформаційно-телекомунікаційної системи протягом одного робочого дня з моменту виникнення таких підстав надсилає розпорядникові відповідної системи лист про припинення користувачу доступу до системи.

6.20. За результатами розгляду листа про припинення користувачеві доступу до системи розпорядник відповідної інформаційної, телекомунікаційної або інформаційно-телекомунікаційної системи дає доручення адміністратору системи про здійснення фактичного припинення доступу користувачу до системи.

6.21. Усю інформацію про припинення доступу користувачів до системи адміністратор відповідної інформаційної, телекомунікаційної або інформаційно-телекомунікаційної системи вносить протягом одного робочого дня до відповідного журналу заявок про надання доступу до системи.

7. Відповідальність

7.1. Відповідальність за виконання заходів з антивірусного захисту інформації на засобах комп'ютерної техніки, що експлуатуються у відповідному структурному підрозділі виконавчого органу Київської міської ради (Київської міської державної адміністрації), районної в місті Києві державної адміністрації, підприємства, установи та організації, що належить до комунальної власності територіальної громади міста Києва або передана до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації), за забезпечення антивірусного захисту та знищення виявлених вірусів, за несанкціоноване встановлення програмного забезпечення на автоматизованих робочих місцях користувачів, здійснення періодичного контролю за станом та дотриманням встановленого порядку антивірусного захисту користувачами покладається на службу захисту інформації.

7.2. Відповідальність за виконання заходів з антивірусного захисту інформації на автоматизованому робочому місці, за дотримання вимог щодо доступу до мережі Інтернет та електронної пошти, за збереження в таємниці особистого пароля покладається на користувачів – працівників структурних підрозділів виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністрацій, підприємств, установ та організацій, що належать до комунальної власності територіальної громади міста Києва або передані до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації).

7.3. Користувачі інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах за порушення вимог законодавства про інформацію, цього Положення несуть відповідальність згідно із законами України.

Директор Департаменту інформаційно-комунікаційних технологій Ю. Назаров

Додаток 1
до Положення про забезпечення захисту інформації в інформаційно-телекомунікаційних системах структурних підрозділів виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністрацій, підприємств, установ та організацій, що належать до комунальної власності територіальної громади міста Києва або передані до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації)

Типові загрози
під час роботи з мережею Інтернет та електронною поштою

№	Загроза	Примітка	Рекомендовані заходи безпеки
1.	Ушкодження/ зараження комп'ютерним вірусом під час відвідування веб-сторінок	Найчастіше відбувається під час відвідування спеціально створених веб-сторінок	Не відвідувати підозрілі веб-сторінки; встановити, своєчасно оновлювати та не відключати антивірусне програмне забезпечення
2.	Ушкодження/ зараження комп'ютерним вірусом під час перегляду поштових повідомлень	Зазвичай відбувається під час відкриття прикріпленого до листа файла	Не відкривати листи з незнайомої або нетипової електронної адреси; не відкривати файли, прикріплені до листа невідомого відправника; встановити, своєчасно оновлювати та не відключати антивірусне програмне забезпечення
3.	Витік інформації з автоматизованого робочого місця	Уразливим може виявитися програмне забезпечення (найчастіше таким є загальнодоступне, а також	Використовувати тільки прийняте до використання програмне забезпечення;

		невідомих або маловідомих виробників); також може статися внаслідок ушкодження/зараження комп'ютерним вірусом	встановити, своєчасно оновлювати та не відключати антивірусне програмне забезпечення
4.	Надання можливості віддаленого управління комп'ютером	Може бути отримано як з відома користувача (в разі використання ним програмного забезпечення, що виконує цю функцію), так і без його відома (в разі ушкодження/зараження комп'ютерним вірусом)	Використовувати тільки прийняте до використання програмне забезпечення; встановити, своєчасно оновлювати та не відключати антивірусне програмне забезпечення
5.	Втрата функціональності (повної або часткової) автоматизованого робочого місця	Найчастіше відбувається внаслідок використання вразливостей програмного забезпечення зловмисником або через ушкодження/зараження комп'ютерним вірусом	Використовувати тільки прийняте до використання програмне забезпечення; встановити, своєчасно оновлювати та не відключати антивірусне програмне забезпечення
6.	Викрадення особистої інформації	Найчастіше спричинюється введенням такої інформації на веб-сторінках (зокрема і сайтах-двійниках), зовні ідентичних справжнім сайтам (наприклад, сайт банку), але насправді є підробкою	Не відкривати листи (особливо вкладення) незнайомих адресатів; уважно перевіряти адресу сторінки, на якій маєте намір залишити особисту інформацію; ніколи не зберігати паролі у формах веб-сторінок
7.	Захоплення адрес електронної пошти, веб-сторінок та інше	Найчастіше відбувається у разі використання слабкого пароля для доступу до ресурсу, а також підбору відповіді на контрольне запитання, що ставиться для відновлення пароля у випадках його втрати	Використовувати стійкі паролі (відповідно до вимог цього Положення); не використовувати як відповіді на контрольні запитання (і як власне паролі) інформацію, яку легко можна дізнатися: дату народження, ім'я, прізвище (ваші або близьких родичів), кличку собаки, дівоче

			прізвище; ніколи не розкривати зазначену вище інформацію (якщо вона використовується для описаних цілей) незнайомим людям; ніколи не зберігати паролі в формах веб-сторінок

Додаток 2
до Положення про забезпечення захисту інформації в інформаційно-телекомунікаційних системах структурних підрозділів виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністрацій, підприємств, установ та організацій, що належать до комунальної власності територіальної громади міста Києва або передані до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації)

Загальні заходи захисту інформації
під час використання мережі Інтернет та електронної пошти

№	Заходи захисту інформації	Примітка
1.	Використання тільки програмного забезпечення, зазначеного в Переліку програмного забезпечення, яке допускається для використання у структурних підрозділах виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністраціях, підприємствах, установах та організаціях, що належать до комунальної власності територіальної громади міста Києва або передані до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації)	Використання нерегламентованого програмного забезпечення може призвести до витоку інформації, ушкодження/зараження комп'ютерним вірусом, виходу комп'ютера з ладу через помилки в програмному забезпеченні
2.	Відстеження появи оновлень програмного забезпечення, що використовується на автоматизованому робочому місці, яке взаємодіє з мережею Інтернет	Програмне забезпечення може містити вразливості, використання яких зловмисником може призвести до втрати інформації, виходу компонента з ладу

3.	Призупинення експлуатації програмного забезпечення у разі виявлення в ньому критичних з точки зору безпеки вразливостей та неможливості їх усунення	Програмне забезпечення може містити вразливості, використання яких зловмисником може призвести до втрати інформації, виходу компонента з ладу
4.	Обов'язкове використання та своєчасне оновлення антивірусного програмного забезпечення на компонентах автоматизованих систем, які взаємодіють з мережею Інтернет, у режимі моніторингу подій	Ушкодження/зараження комп'ютерним вірусом може статися і без участі користувача – через мережу Інтернет
5.	Під час роботи з електронною поштою не відкривати листи з вкладеними файлами від невідомих авторів, перед запуском/відкриттям будь-яких файлів виконувати антивірусну перевірку	Найбільш розповсюдженим каналом поширення вірусів та викрадення особистої інформації є електронна пошта. У таких випадках слід звертатися до служби захисту інформації для прийняття рішення щодо подальших дій
6.	Заборонено автоматичне збереження та/або запуск файлів, елементів ActiveX, скриптів з мережі Інтернет на автоматизованому робочому місці користувача	Більшість вразливостей у програмному забезпеченні використовуються через файли, що завантажуються з веб-сторінок, або через самі веб-сторінки, які містять шкідливий або небезпечний код
7.	Не рекомендовано зберігати паролі у формах під час відвідування веб-сторінок	Зловмисники можуть скористатися ресурсом, захищеним паролем (зокрема змінити пароль)