МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

Львівський державний університет внутрішніх справ

ЗАТВЕРДЖЕНО
ухвалою Вченої ради Львівського державного університету внутрішніх справ від 30.04.2025 (протокол № 15)

ВВЕДЕНО В ДІЮ
наказом Львівського державного університету внутрішніх справ від 05.05.2025 № 216

ПОЛОЖЕННЯ ПРО ІНФОРМАЦІЙНУ БЕЗПЕКУ ЛЬВІВСЬКОГО ДЕРЖАВНОГО УНІВЕРСИТЕТУ ВНУТРІШНІХ СПРАВ

Львів
2025

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Положення про інформаційну безпеку Львівського державного університету внутрішніх справ (далі – Положення) визначає основні правила організації та функціонування системи управління інформаційною безпекою у Львівському державному університеті внутрішніх справ (далі – ЛьвДУВС), зокрема щодо додержання вимог, обмежень і рекомендацій у сфері безпеки електронних інформаційних ресурсів.

1.2. Положення відповідає вимогам законів України «Про інформацію», «Про захист інформації в інформаційно-комунікаційних системах», «Про Національну програму інформатизації», «Про електронну ідентифікацію та електронні довірчі послуги», Положення про технічний захист інформації в Україні, затвердженого Указом Президента України від 27 вересня 1999 року № 1229, Загальним вимогам до кіберзахисту об’єктів критичної інфраструктури, затвердженим постановою Кабінету Міністрів України від 19 червня 2019 року № 518.

1.3. Положення спрямоване на забезпечення ефективного захисту інформації в електронних інформаційних ресурсах та інформаційно-комунікаційних системах ЛьвДУВС від зовнішніх і внутрішніх загроз, зокрема які пов’язані з умисними або необережними діями працівників ЛьвДУВС, забезпечення безперервного функціонування ЛьвДУВС шляхом ефективного захисту електронних інформаційних ресурсів та інформаційно-комунікаційних систем.

1.4. Дотримання інформаційної безпеки ЛьвДУВС забезпечує відділ інформаційно-технічного забезпечення університету (далі – ВІТЗ), рекомендації у сфері інформаційної безпеки якого є обов’язковими для виконання всіма працівниками ЛьвДУВС.

1.5. Працівники ВІТЗ забезпечують:

роботу мережевої інфраструктури ЛьвДУВС, структурованих кабельних та безпровідних мереж передачі даних, мережевого обладнання;

встановлення антивірусного програмного забезпечення під час видачі нового комп’ютерного обладнання, заміни жорсткого диска комп’ютера, переустановлення операційної системи;

перевірку корпоративної електронної пошти ЛьвДУВС на наявність шкідливого контенту;

організацію періодичного сканування мережевих систем, ресурсного мережевого та серверного обладнання на наявність вразливостей;

організацію періодичного тестування інформаційно-комунікаційних систем та інформаційних ресурсів ЛьвДУВС на предмет проникнення;

моніторинг службового використання інформаційно-комунікаційних систем;

роботу антивірусного програмного забезпечення та його налаштування відповідно до вимог цього Положення.

1.6. Положення застосовується до всіх електронних інформаційних ресурсів та інформаційно-комунікаційних систем, які використовуються у ЛьвДУВС, і поширюється на користувачів університету.

2. УПРАВЛІННЯ ВІДДАЛЕНИМ ДОСТУПОМ ДО ЕЛЕКТРОННИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ ТА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

2.1. Віддалений доступ до електронних інформаційних ресурсів та інформаційно-комунікаційних систем ЛьвДУВС на рівні адміністрування надається працівникам ВІТЗ з урахуванням їх функціональних обов'язків, індивідуальної ідентифікації та автентифікації.

2.2. Відповідальна особа ВІТЗ, яка здійснює віддалене підключення до електронних інформаційних ресурсів, що використовуються у ЛьвДУВС, зобов'язана:

використовувати віддалений доступ виключно відповідно до своїх функціональних обов'язків;

не допускати витоку інформації з обмеженим доступом.

2.3. Забороняється використання відкритих (не захищених паролем) бездротових комп'ютерних мереж у місцях загального користування для віддаленого підключення до електронних інформаційних ресурсів ЛьвДУВС.

2.4. Порядок використання технічних та програмних засобів для віддаленого доступу передбачає, що:

2.4.1) віддалений доступ до електронних інформаційних ресурсів ЛьвДУВС надається користувачеві шляхом підключення службового персонального комп'ютера працівника ВІТЗ до комп'ютерної мережі університету за допомогою VPN;

2.4.2) у разі використання особистих технічних засобів (пристроїв) для отримання віддаленого доступу до електронних інформаційних ресурсів ЛьвДУВС повинні виконуватися такі умови:

використовуються тільки ліцензійні операційна система та програмне забезпечення;

встановлені всі актуальні оновлення;

пристрій оснащений ліцензійною антивірусною програмою з актуальними антивірусними базами та сигнатурами;

у разі встановлення віддаленого доступу користувач отримує доступ тільки до необхідних електронних інформаційних ресурсів;

2.4.3) при наданні віддаленого доступу використовується багатофакторна автентифікація (за наявної технічної можливості) або застосовується індивідуальний ключ та сертифікат (OpenVPN) користувача;

2.4.4) паролі, що використовуються для віддаленого доступу, повинні містити не менше 12 символів, великі та малі букви латиницею, цифри та спеціальні символи;

2.4.5) віддалене з'єднання після 300 секунд неактивної сесії автоматично вимикається або обривається;

2.4.6) налаштування автоматичного блокування шляхів входу для віддаленого доступу після заданої кількості спроб послідовного введення неправильного пароля є обов'язковим.

2.5. У разі виникнення загрози інформаційній безпеці електронних інформаційних ресурсів ЛьвДУВС системний адміністратор (відповідальна особа з числа працівників ВІТЗ, на яку покладено виконання функцій системного адміністратора) здійснює відключення віддаленої сесії користувача та блокування віддаленого доступу.

3. РЕЗЕРВНЕ КОПІЮВАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ ТА ЕЛЕКТРОННИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

3.1. Резервному копіюванню підлягають усі електронні інформаційні ресурси, які використовуються у ЛьвДУВС, та програмні засоби, що забезпечують їх функціонування:

сервери прикладного програмного забезпечення;

бази даних прикладного програмного забезпечення;

бази даних корпоративної електронної пошти.

3.2. Інформація із службових та персональних комп'ютерів користувачів не підлягає резервному копіюванню. Користувачі зобов'язані самостійно зберігати резервні копії файлів.

3.3. У рамках системи резервного копіювання автоматично ведеться електронний журнал реєстрації подій створення резервних копій (далі – журнал реєстрації подій), який містить актуальну інформацію щодо процесу виконання резервного копіювання.

3.4. Резервне копіювання виконується в час, коли робоче навантаження на інформаційні системи та електронні інформаційні ресурси мінімальне в неопераційний час (після: 22:00).

3.5. Дані резервуються в копії різних типів для надійного збереження і подальшого відновлення інформації в разі необхідності.

3.6. Перевірку інформації з резервних копій виконує системний адміністратор ВІТЗ.

3.7. Резервні копії зберігаються на технічних засобах (носіях) у віддаленому місці на достатній відстані, щоб уникнути будь-якого пошкодження в разі настання надзвичайних ситуацій в спеціально обладнаному приміщенні. Резервні копії захищаються від модифікації. Носії резервних копій захищаються від несанкціонованого доступу до них.

3.8. Резервне копіювання проводиться щоденно в режимі автономного резервування.

Системний адміністратор ВІТЗ здійснює налаштування системи резервного копіювання, а також перегляд журналів реєстрації подій.

У разі виявлення будь-яких помилок системний адміністратор ВІТЗ виконує необхідні дії для усунення причини проблеми резервного копіювання і перезапускає процес невдалого резервного копіювання.

3.9. Відновлення інформації виконується системним адміністратором ВІТЗ після виявлення критичних похибок чи порушень роботи інформаційних систем ЛьвДУВС.

4. РОЗПОДІЛ ПОВНОВАЖЕНЬ МІЖ КОРИСТУВАЧАМИ ЕЛЕКТРОННИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ ТА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

4.1. У ЛьвДУВС між користувачами здійснюється розподіл повноважень щодо використання та адміністрування, розробки, тестування електронних інформаційних ресурсів та інформаційно-комунікаційних систем.

4.2. З метою розмежування прав доступу користувачів до електронних інформаційних ресурсів та інформаційно-комунікаційних систем, які використовуються у ЛьвДУВС, застосовуються такі правила:

користувач отримує доступ в електронному інформаційному ресурсі тільки до даних, що необхідні йому для виконання функціональних обов'язків;

використовуються стандартні профілі доступу користувачів для типових обов'язків і функцій.

5. ЗАХИСТ КОМП'ЮТЕРНИХ МЕРЕЖ

5.1. Відповідальні працівники ВІТЗ ЛьвДУВС забезпечують:

підтримку достовірної та актуальної схеми топології комп'ютерної мережі ЛьвДУВС у достатній деталізації, щоб забезпечити безперебійну роботу інформаційних систем та ІТ-сервісів, які використовуються у ЛьвДУВС, а також вирішувати проблеми та інциденти, що виникають у комп'ютерній мережі;

документування та маркування всього ресурсного мережевого обладнання із зазначенням відповідального за робочий стан, фізичне розташування тощо;

розробку та впровадження специфікацій та стандартних конфігурацій налаштувань всього мережевого обладнання, що підключається до комп'ютерної мережі, та конфігурацій міжмережевих екранів;

документальне ведення переліку протоколів, портів та стандартів з'єднань, що використовуються в комп'ютерній мережі ЛьвДУВС, документальне ведення переліку всіх каналів зв'язку ЛьвДУВС із зовнішніми мережами, у тому числі телефонними;

перевірку стану систем захисту комп'ютерної мережі ЛьвДУВС та надання рекомендацій на їх основі.

5.2. Для захисту комп'ютерної мережі ЛьвДУВС застосовуються такі вимоги:

будь-які зміни в конфігурації комп'ютерної мережі ЛьвДУВС здійснюють лише працівники ВІТЗ;

на маршрутизаторах та комутаторах всі незадіяні порти мають перебувати в стані «shutdown» (за можливості);

зовнішній доступ до комп'ютерної мережі дозволений тільки з використанням VPN або програмного забезпечення для шифрування сесії;

комп’ютерна мережа налаштовується так, щоб унеможливити проходження трафіка між сегментами в обхід міжмережевого екрану;

комп’ютерна мережа налаштовується так, щоб доступ у мережу Інтернет здійснювався тільки з використанням комплексної системи, що включає в себе міжмережевий екран, антивірус (за можливості операційної системи чи обладнання) та інші існуючі у ЛьвДУВС системи захисту.

5.3. До захисту серверного та мережевого обладнання, яке використовується у ЛьвДУВС, застосовуються такі вимоги:

серверне обладнання розміщується в окремих ізольованих сегментах мережі, згідно з рівнем критичності сервера, рівня довіри (наприклад, шляхом розділення сегментів серверів різних середовищ (роботи, розробки, тестування), серверів моніторингу, адміністрування. Між сегментами налаштовується фільтрація за допомогою міжмережевого екрану;

доступ до інтерфейсів управління маршрутизаторами, міжмережевими екранами та іншим мережевим обладнанням належним чином захищається;

паролі доступу повинні містити (при можливості) не менше 12 символів, великі та малі букви латиницею, цифри та спеціальні символи;

доступ до сегмента мережі користувачів або сегмента мережі адміністрування серверного обладнання дозволений тільки з використанням захищених протоколів (SSH, HTTPS).

5.4. До міжмережевих екранів, які використовуються у ЛьвДУВС, застосовуються такі вимоги:

міжмережеві екрани ресурсно підтримуються за допомогою регулярних оновлень та інших послуг технічної підтримки;

для захисту мережі від загроз із зовнішніх мереж, у тому числі мережі Інтернет, використовуються міжмережевий екран та належним чином налаштований апаратний чи програмно-апаратний захист;

міжмережевий екран налаштовується так, щоб будь-якому серверу, який повинен приймати тільки вхідні з’єднання (наприклад, VPN сервер), було заборонено посилати вихідні з’єднання;

адміністрування міжмережевих екранів здійснюється тільки системним адміністратором ВІТЗ ЛьвДУВС.

5.5. До маршрутизаторів, які використовуються у ЛьвДУВС, застосовуються такі вимоги:

маршрутизатори повинні ресурсно підтримуватися виробником за допомогою регулярних оновлень та інших послуг технічної підтримки;

заборонено використовувати маршрутизатори з конфігурацією «за замовчуванням»;

обмежується фізичний доступ до маршрутизаторів, за винятком працівників ВІТЗ, які мають право здійснювати їх адміністрування.

5.6. До керованих комутаторів, які використовуються у ЛьвДУВС, застосовуються такі вимоги:

комутатори повинні ресурсно підтримуватися виробником за допомогою регулярних оновлень та інших послуг з технічної підтримки;

заборонено використовувати комутатори з конфігурацією «за замовчуванням».

5.7. До бездротових мереж застосовуються такі вимоги:

точки бездротового доступу до комп'ютерної мережі ЛьвДУВС виділяються в окремий сегмент мережі за допомогою «мережевого екрану»;

точки бездротового доступу розміщуються так, щоб мінімізувати зону радіопокриття мережі за межею контрольованої території ЛьвДУВС;

всі бездротові точки доступу налаштовуються для запобігання віддаленому адмініструванню через бездротову мережу;

обмежується фізичний доступ до бездротових точок доступу, за винятком уповноважених осіб, які мають право здійснювати їх адміністрування;

увесь трафік, що проходить через Wi-Fi мережу, шифрується за допомогою ключа шифрування щонайменше 128 біт із використанням протоколу WPA2;

усі налаштування безпеки бездротових з'єднань за замовчуванням (встановлені виробником) змінюються, включаючи паролі доступу, ключ шифрування протоколів WPA2, WPA3, SSID, пароль адміністратора, протоколу SNMP тощо.

5.8. До мережевого і серверного обладнання, яке використовується у ЛьвДУВС, застосовуються такі вимоги:

щонайменше один раз на місяць перевіряється наявність нових виправлень (патчів) і оновлень програмного забезпечення, що працює на серверному і мережевому обладнанні, і встановлюються ті з них, які вважаються критичними чи необхідними для їх функціонування;

у разі виявлення критичних виправлень (патчів) негайно оновлюється відповідне програмне забезпечення. Перед застосуванням патчів проводиться обов'язкове резервне копіювання конфігурації з метою відновлення працездатності в разі некоректної роботи після оновлення;

до впровадження оновлення, виправлення в робочому середовищі необхідно переконатися, що встановлені оновлення, виправлення не будуть негативно впливати або змінювати інше програмне забезпечення;

створюється резервна копія програмного забезпечення до того, як буде встановлено виправлення (патчі) або оновлення;

створюються резервні копії файлів конфігурації кожен раз, коли вносяться зміни в конфігурацію, щоб забезпечити здатність до відновлення робочої конфігурації за потреби.

5.9. Конфігурації всіх мережевих пристроїв резервуються.

Резервне копіювання конфігурацій мережевих пристроїв здійснюється перед внесенням змін відповідальним працівником ВІТЗ ЛьвДУВС у конфігурацію обладнання.

Передача конфігурацій мережевих пристроїв для резервування проводиться тільки за протоколами SCP, SFTP, SSH, HTTPS.

Файли (резервні копії конфігурацій мережевого обладнання) зберігаються на сервері, доступ до якого обмежений.

Після проведення резервного копіювання архіви файлів (резервні копії) перевіряються на цілісність.

Доступ до файлів (резервних копій конфігурацій мережевого обладнання) надається системному адміністраторові та уповноваженим особам ВІТЗ ЛьвДУВС.

5.10. Для захисту інформації її передавання через загальнодоступні мережі здійснюється за допомогою стійких криптографічних алгоритмів та протоколів, таких як SSL/TLS і IPsec.

На інтерфейсах, підключених до провайдерів зв'язку, налаштовуються базові списки доступів, які забезпечують базовий захист від атак з мереж провайдера зв'язку.

Списки доступів на маршрутизаторах виконують первинну фільтрацію трафіку. Для контролю доступів користувачів до інформаційних систем використовується міжмережевий екран.

Міжмережеві екрани використовуються для обмеження доступу користувачів до додатків інформаційних ресурсів, а також сегментації мережі на зони безпеки з метою виключення несанкціонованого доступу.

Забороняються будь-які з'єднання, які виходять від недовірених мереж і вузлів, за винятком протоколів, необхідних для функціонування інформаційних систем.

Перегляд конфігурації міжмережевого екрану на предмет відповідності стандартам безпеки, а також на предмет актуальності проводиться щоквартально.

Усі порти керованих комутаторів, які не використовуються, блокуються з метою запобігання спробам несанкціонованого підключення, а також атакам канального рівня; керовані комутатори локальних обчислювальних мереж містять опції Port Security, VMPS, 802.IX

5.11. Працівникам ЛьвДУВС забороняється самостійно підключати до комп'ютерних мереж університету будь-які технічні пристрої (персональні комп'ютери, друкуючі пристрої, мультимедійне та відеообладнання, мережеві комутатори та маршрутизатори, точки доступу Wi-Fi тощо). Самостійне підключення пристроїв допускається лише до безпровідних мереж Wi-Fi університету.

Категорично заборонено підключати до комп'ютерних мереж ЛьвДУВС обладнання, на якому здійснюється обробка інформації з обмеженим доступом.

5.12. ВІТЗ ЛьвДУВС ініціює та забезпечує організацію проведення тестування комп'ютерних мереж на предмет проникнення та сканування на предмет вразливостей.

5.13. До тестування на проникнення застосовуються такі вимоги:

тестування на проникнення проводяться не рідше одного разу на рік;

тестування на проникнення проводяться позапланово після будь-яких істотних змін у конфігурації мережі, введення в експлуатацію або виведення з експлуатації продукту (процесу), обладнання, що суттєво впливає на топологію мережі ЛьвДУВС.

5.14. Внутрішнє сканування мережі ЛьвДУВС на предмет вразливостей проводиться постійно, зовнішнє сканування на предмет вразливостей проводиться один раз у квартал.

5.15. Сканування на предмет вразливостей перевіряє правильність конфігурації, встановлені виправлення (патчі) та/або відомі вразливості для:

операційних систем;

WEB-серверів;

серверів прикладного програмного забезпечення;

серверів баз даних;

серверів електронної пошти;

міжмережевих екранів;

маршрутизаторів;

керованих комутаторів;

точок бездротового поступу;

мережевих служб, таких як FTP, DNS та SMTP тощо.

5.16. Заходи щодо усунення виявлених вразливостей або вторгнень в інформаційні системи, які використовуються у ЛьвДУВС, та/або мережу ЛьвДУВС починаються негайно після виявлення.

5.17. Рекомендується застосовувати мережеві сніфери або системи аналізу та протидії атакам IPS (пристрої або програмне забезпечення для перехоплення аналізу мережевого трафіку).

5.18. Дата і час проведення сканування визначаються ВІТЗ ЛьвДУВС з урахуванням мінімального навантаження на інформаційні системи та можливого суттєвого падіння їх потужностей.

5.19. До синхронізації часу застосовуються такі вимоги:

на всіх серверах, комп’ютерах, мережевому та іншому обладнанні ЛьвДУВС ведеться регулярна синхронізація часу;

синхронізація часу на серверному, мережевому обладнанні та на комп’ютерах проводиться не менше одного разу на добу;

синхронізація часу проводиться за протоколом NTP;

самочинна зміна користувачами часу, джерел синхронізації часу, часових поясів забороняється.

5.20. Синхронізація часу ведеться:

із зовнішніх джерел, базованих на Міжнародному атомному часі (Intematoinal Atomic Time) або Всесвітньому координованому часі (UTC);

із джерел, розташованих у внутрішньому сегменті мережі, які централізовано синхронізуються із зовнішніми джерелами, базованими на Міжнародному атомному часі (Intematoinal Atomic Time) або Всесвітньому координованому часі (UTC).

6. АНТИВІРУСНИЙ ЗАХИСТ ІНФОРМАЦІЙНИХ СИСТЕМ

6.1. В інформаційних ресурсах і системах ЛьвДУВС використовується сучасне антивірусне програмне забезпечення для виявлення та блокування зловмисного коду як превентивний захід безпеки, що забезпечує перевірку:

будь-яких файлів на змінному носії та файлів, одержаних через мережу, на предмет наявності зловмисного коду до їх (його) запуску або відкриття користувачем;

поведінкового аналізу на предмет виявлення нетипової активності на комп’ютерах та серверах;

приєднаних до електронної пошти та завантажених з мережі файлів на предмет наявності зловмисного коду до відкриття або запуску;

вебсторінок на шкідливий вміст.

Комп’ютерне обладнання без установленого антивірусного програмного забезпечення не вводиться в експлуатацію. У разі виявлення обладнання без установлених засобів антивірусного захисту уповноважені особи негайно їх встановлюють і проводять повне сканування на предмет наявності зловмисного коду.

У разі виявлення будь-якої інформації, яка може становити загрозу для ЛьвДУВС, включаючи, але не обмежуючись даними, повідомленнями, вкладеннями вхідної та вихідної корпоративної електронної пошти та мережевим трафіком, така інформація автоматично блокується, ізолюється або видаляється.

6.2. Для забезпечення ефективного захисту інформації та засобів обробки інформації ЛьвДУВС від шкідливого коду використовується антивірусне програмне забезпечення.

Антивірусне програмне забезпечення повинно мати такі функціональні можливості:

пошук та ідентифікація зловмисного коду;

видалення зловмисного коду;

видалення або ізоляція інфікованих файлів, якщо їх очищення від зловмисного коду в цей момент неможливе;

оповіщення користувача та адміністратора про виявлені загрози;

автоматична реєстрація подій;

поведінковий аналіз;

евристичний аналіз, а також аналіз на основі моделі поведінки програмного забезпечення;

захист від зміни конфігурації чи видалення антивірусного програмного забезпечення.

6.3. Антивірусне програмне забезпечення налаштовується на захист від усіх відомих загроз, які включають, серед іншого, віруси, шпигунські програми і клавіатурні шпигуни.

Антивірусне програмне забезпечення налаштовується на блокування, видалення виявленого зловмисного коду або на його ізоляцію (карантин), якщо автоматичне видалення неможливе або недоцільне. Також антивірусне програмне забезпечення налаштовується на автоматичне лікування зараженого файлу (наприклад, видалення шкідливого коду), карантин або заборону доступу до інфікованого файлу, якщо автоматичне лікування неможливе.

Забороняється зупиняти роботу антивірусного програмного забезпечення. У разі необхідності для усунення помилки чи встановлення авторизованого програмного забезпечення дозволяється коротка (протягом усунення такої помилки чи перебігу інсталяції) зупинка роботи антивірусного програмного забезпечення. Інтерресурсний захист знову включається відразу ж після

завершення установки, а повне сканування проводиться до моменту підключення до комп'ютерної мережі апарату ЛьвДУВС.

Право здійснювати короткочасну зупинку роботи антивірусного програмного забезпечення мають виключно відповідальні працівники ВІТЗ.

6.4. Антивірусне програмне забезпечення встановлюється та налаштовується на такому обладнанні:

комп'ютери користувачів;

сервери (за наявності актуального програмного забезпечення для цієї платформи);

портативне комп'ютерне обладнання (ноутбуки), що має доступ до комп'ютерної мережі ЛьвДУВС;

мережеве обладнання (за технічної можливості) з власною вбудованою операційною системою (маршрутизатори, комутатори тощо).

Антивірусне програмне забезпечення налаштовується для забезпечення автоматичного сканування обладнання. Конфігурація антивірусного програмного забезпечення налаштовується згідно з рекомендаціями виробника.

Антивірусне програмне забезпечення знаходиться постійно в оперативній пам'яті та перевіряє на наявність шкідливих програм усі об'єкти, до яких звертається користувач.

6.5. Усі події, що пов'язані з роботою антивірусного програмного забезпечення, автоматично реєструються в журналі подій (захисту).

Антивірусне програмне забезпечення автоматично сповіщає користувача чи системного адміністратора у випадках:

виявлення зловмисного коду;

виявлення спроб мережевих атак;

помилки оновлення антивірусних баз;

помилки ініціалізації модулів захисту.

6.6. Бази антивірусного програмного забезпечення постійно підтримуються в актуальному стані, оновлюються автоматично одразу після надання виробником відповідних оновлень.

7. ВИКОРИСТАННЯ КОРПОРАТИВНОЇ ЕЛЕКТРОННОЇ ПОШТИ

7.1. Корпоративна електронна пошта ЛьвДУВС та електронне листування, що створюється та зберігається на службових персональних комп'ютерах працівників, є власністю ЛьвДУВС.

7.2. Первинний доступ користувачам до електронної пошти надається відповідно до структури та штатного розпису ЛьвДУВС.

7.3. У разі доступу до електронної пошти ЛьвДУВС з використанням веббраузера рекомендується використовувати приватний режим браузера.

7.4. Паролі доступу користувачів електронної пошти ЛьвДУВС повинні містити не менше 8 символів, великі та малі букви латиницею, цифри;

7.5. До використання мобільного пристрою для організації віддаленого доступу до електронної пошти ЛьвДУВС застосовуються такі вимоги:

доступ до мобільного пристрою обмежено засобами захисту (паролем, біометричним засобом автентифікації тощо). За наявності технічної можливості рекомендується шифрування пам’яті та змінних носіїв пристрою;

у разі втрати мобільного пристрою, на якому налаштовано доступ для віддаленого підключення до корпоративної електронної пошти ЛьвДУВС, необхідно в найкоротший термін звернутися до відповідальних працівників ВІТЗ для віддаленого видалення інформації та зміни пароля.

7.6. Під час використання корпоративної електронної пошти ЛьвДУВС працівникам забороняється:

використання корпоративної електронної пошти ЛьвДУВС з нересурсним (відключеним) антивірусним програмним забезпеченням;

зберігання в доступному місці логінів та паролів доступу до електронної пошти ЛьвДУВС;

використання корпоративної електронної пошти ЛьвДУВС для реєстрації на сайтах, форумах, інформаційних системах, інших ресурсах, що не пов’язані з виконанням функціональних обов’язків;

налаштовування переадресації повідомлень електронної пошти ЛьвДУВС на особисту електронну пошту.

Службове листування працівниками ЛьвДУВС здійснюється виключно за використанням корпоративної електронної пошти ЛьвДУВС.

8. ВИКОРИСТАННЯ РЕСУРСІВ МЕРЕЖІ ІНТЕРНЕТ

8.1. Доступ користувачам ЛьвДУВС до ресурсів мережі Інтернет надається відповідальними працівниками ВІТЗ ЛьвДУВС.

8.2. Працівники ЛьвДУВС зобов’язані використовувати доступ до ресурсів мережі Інтернет виключно для виконання функціональних обов’язків.

8.3. Працівникам ЛьвДУВС забороняється:

використання ресурсів мережі Інтернет для виконання завдань, не пов’язаних зі службовою діяльністю;

вивантаження на інші ресурси мережі інтернет, інформації з обмеженим доступом або інформації, що є власністю ЛьвДУВС або його партнерів, чи контрагентів, та підлягає захисту відповідно до укладених угод та зобов’язань сторін;

публікація, завантаження та поширення інформації та матеріалів, що містять вірусне та шкідливе програмне забезпечення, комп’ютерні коди, файли, програми, що застосовуються для порушення, знищення або обмеження функціональності будь-якого комп’ютерного або комутаційного обладнання або програмного забезпечення для здійснення несанкціонованого доступу, а також серійні номери до комерційних продуктів та програмного забезпечення для їх генерування, логіни, паролі та інші засоби для отримання несанкціонованого доступу до платних ресурсів у мережі Інтернет, розміщення посилань на вищезазначену інформацію;

змінення налаштування програмних продуктів щодо доступу до ресурсів мережі Інтернет;

використання доступу до ресурсів мережі Інтернет з нересурсним (відключеним) антивірусним програмним забезпеченням;

завантаження та запускання файлів (архівів) без попередньої перевірки за допомогою встановленого антивірусного програмного забезпечення, що здійснюється в автоматичному порядку;

використання ресурсів мережі Інтернет для перегляду або завантаження інформації розважального та порнографічного характеру;

використання зі службовою метою електронних поштових скриньок на сторонніх (не службових) поштових серверах мережі Інтернет (gmail.com, ukr.net, i.ua тощо), крім випадків, погоджених з керівництвом ЛьвДУВС;

для службового листування чи передачі будь-якої службової інформації, у тому числі документів, створених під час службової діяльності, використання месенджерів, крім тих, які погоджені у відповідному порядку для виконання працівником функціональних обов'язків;

створення та виконання на службовому персональному комп'ютері технічної підтримки вебсерверів, персональних вебсторінок, у тому числі сторінок у соціальних мережах (Facebook, Twitter, Instagram тощо), не пов'язаних з виконанням функціональних обов'язків;

здійснення на службовому персональному комп'ютері підписки на інтернет-розсилання, не пов'язаних із виконанням функціональних обов'язків;

використання анонімних проксі-серверів, сторонніх VPN-сервісів, інших технічних та програмних засобів та заходів для прихованого доступу до ресурсів мережі Інтернет.

8.4. У ЛьвДУВС можуть здійснюватися обмеження доступу до ресурсів мережі Інтернет, зміст яких не стосується виконання функціональних обов'язків, а також до ресурсів, заборонених законодавством, включаючи інформацію, що принижує честь та гідність осіб, пропагує культ насильства і жорстокості, расової, національної чи релігійної нетерпимості та дискримінації, порнографічного характеру, у тому числі такі, що роз'яснюють порядок застосування вибухових речовин та іншої зброї тощо, або в разі виникнення підозри щодо загрози інформаційній безпеці ЛьвДУВС.

9. ПРАВИЛА КОРИСТУВАННЯ СЛУЖБОВИМИ ПЕРСОНАЛЬНИМИ КОМП'ЮТЕРАМИ

9.1. Відповідальні працівники ВІТЗ встановлюють службові персональні комп'ютери та периферійні пристрої на робочому місці працівників ЛьвДУВС і підключають до комп'ютерної мережі.

9.2. Відповідальні працівники ВІТЗ мають право обмежити доступ працівників ЛьвДУВС до користування службовими персональними комп'ютерами шляхом їх блокування, якщо це не пов'язано з виконанням функціональних обов'язків, а також якщо працівник ЛьвДУВС за допомогою вищезазначеного обладнання збирає, зберігає та поширює інформацію, заборонену законодавством, відомчими розпорядчими документами ЛьвДУВС та МВС, включаючи інформацію, що принижує честь та гідність інших осіб, а

також матеріали, що спонукають до розпалу національної, релігійної ворожнечі чи розбрату, закликають до протиправної діяльності, у тому числі такі, що роз'яснюють порядок застосування вибухових речовин та іншої зброї тощо.

9.3. Працівники ЛьвДУВС зобов'язані:

використовувати службові персональні комп'ютери та мережеві ресурси виключно для виконання функціональних обов'язків;

у разі виникнення будь-яких несправностей комп'ютера або периферійного обладнання повідомляти ВІТЗ у встановленому порядку,

не перешкоджати автоматичній перевірці за допомогою встановленого антивірусного програмного забезпеченням дискових носіїв та пристроїв, що підключаються до службового персонального комп'ютера (флеш-накопичувачі тощо);

після закінчення роботи коректно завершувати сеанс роботи з операційною системою та вимикати комп'ютер (якщо інше не обумовлено технологічними вимогами);

встановлювати останні оновлення операційних систем на службових персональних комп'ютерах, якщо того вимагає система відповідним сповіщенням.

9.4. Працівникам ЛьвДУВС забороняється:

самостійно встановлювати та/або використовувати будь-які програмні засоби на службовому персональному комп'ютері, крім випадків, коли таке програмне забезпечення погоджено у відповідному порядку з ВІТЗ для виконання функціональних обов'язків;

самостійно змінювати налаштування апаратного та/або програмного забезпечення службового персонального комп'ютера, мережеві налаштування тощо;

зберігати на службових персональних комп'ютерах інформацію (програмне забезпечення, музичні, відео-, фотофайли, ігрові програми тощо), не пов'язані з виконанням функціональних обов'язків;

використовувати для доступу до службового персонального комп'ютера облікові записи (логіни та паролі) інших працівників, крім випадків, коли працівник відсутній через відрядження, хворобу, відпустку або інші обставини, що перешкоджають його фізичній присутності на робочому місці, і з дозволу керівника структурного підрозділу;

самовільно розширювати свої права доступу;

зберігати в доступному місці ідентифікаційні дані для доступу до службового персонального комп'ютера, мережевих дисків чи каталогів;

надавати доступ до свого комп'ютера іншим працівникам ЛьвДУВС без відповідного дозволу керівника структурного підрозділу, крім випадків з технічного обслуговування працівниками ВІТЗ та проведення відповідних перевірок;

примусово відключати антивірусне програмне забезпечення, встановлене на службовому персональному комп'ютері;

використовувати особисті комп’ютери для здійснення повсякденної службової діяльності, крім випадків, погоджених з керівництвом ЛьвДУВС та ВІТЗ, та в межах виконання службових повноважень дистанційно.

10. ПОЛІТИКА УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ

10.1. В університеті оцінка вразливостей електронних інформаційних ресурсів здійснюється самостійно працівниками ВІТЗ, або залученням третіх сторін (дослідників) згідно із нормами законодавства України.

10.2. Оцінка вразливостей інформаційних ресурсів ЛьвДУВС включає наступні етапи:

10.2.1. Ідентифікація вразливостей інформаційних ресурсів:

сканування інформаційних ресурсів ЛьвДУВС автоматизованими сканерами безпеки (Nessus, OpenVAS, Qualys тощо);

аналіз логів і подій безпеки (SIEM-системи, журнали подій ОС, IDS/IPS тощо);

проведення тестувань на проникнення (penetration testing, Pentest тощо);

оцінка звітів про нові вразливості (CVE, NVD, експертні джерела тощо);

ручний аналіз конфігурацій систем і коду (code review, security audits тощо).

10.2.2. Класифікація вразливостей інформаційних ресурсів:

визначення рівня критичності (низький, середній, високий, критичний);

використання стандартів класифікації (CVSS – Common Vulnerability Scoring System);

аналіз впливу на конфіденційність, цілісність і доступність інформації (CIA-тріада);

визначення джерел загроз (зовнішні, внутрішні, випадкові, навмисні).

10.2.3. Оцінка ризиків:

визначення ймовірності експлуатації вразливості;

аналіз потенційних наслідків (втрата інформації, репутаційні ризики, збої у роботі тощо);

визначення необхідності та терміновості усунення;

використання матриці ризиків для прийняття рішень.

10.2.4. Усунення вразливостей:

встановлення оновлень (патчів) безпеки від розробників;

конфігураційні зміни (обмеження прав доступу, посилення аутентифікації);

впровадження заходів зниження ризиків (мікросегментація, додаткові механізми контролю);

тимчасові заходи (наприклад, відключення вразливих сервісів, якщо немає патчів).

10.2.5. Моніторинг і контроль:

періодичне повторне сканування систем на наявність вразливостей;

впровадження та оновлення політик безпеки;

налаштування систем виявлення вторгнень (IDS/IPS);

аналіз інцидентів і коригування заходів безпеки;

підвищення обізнаності працівників щодо актуальних загроз.

11. ПОРЯДОК РЕАГУВАННЯ НА ІНЦИДЕНТИ

11.1. У разі виявлення працівниками ЛьвДУВС чи адміністраторами систем підозрілої активності на персональних комп'ютерах або ознак несанкціонованого доступу до інформаційних ресурсів, вони зобов'язані негайно проінформувати про це ВІТЗ.

11.2. Працівники ВІТЗ ЛьвДУВС здійснюють перевірку обладнання чи інформаційних ресурсів на наявність несанкціонованого втручання в їх роботу, а при підтвердженні факту кіберінциденту, відключають їх від комп'ютерної мережі та інформують про подію проректора за напрямом роботи та ректора університету.

11.3. Про виявлені факти підозрілої активності або ознаки втручання в інформаційні системи одразу інформується Департамент інформатизації МВС, Департамент кіберполіції Національної поліції України або НКЦК, Команду реагування CERT-UA або Ситуаційний центр забезпечення кібербезпеки СБУ.

11.4. Працівники ВІТЗ ЛьвДУВС самостійно або з фахівцями кіберполіції Національної поліції України здійснюють:

виявлення джерел інциденту та його класифікацію за типом, критичністю та обсягами впливу;

аналіз і оцінку загрози;

ізоляцію загрози, ліквідацію вразливостей та відновлення нормальної роботи інформаційних ресурсів;

аналіз та вдосконалення заходів безпеки.

11.5 Про результати проведеної роботи інформується проректора за напрямом роботи та ректора університету, звіт щодо кіберінциденту надсилається в Департамент інформатизації МВС та Команду реагування CERT-UA.

11.6. Інформацію щодо кіберзагрози доводиться працівникам ЛьвДУВС.

12. ПІДВИЩЕННЯ ОБІЗНАНОСТІ З ПИТАНЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА КІБЕРБЕЗПЕКИ

12.1. Підвищення обізнаності осіб з числа постійного та перемінного складу ЛьвДУВС з питань інформаційної та кібербезпеки проводиться щорічно та додатково, у разі необхідності.

12.2. Підвищення обізнаності осіб з числа постійного та перемінного складу ЛьвДУВС з питань інформаційної та кібербезпеки покладається на ВІТЗ та профільні кафедри університету в межах програм навчання.

12.3. Основними напрямами підвищення обізнаності осіб з числа постійного та перемінного складу ЛьвДУВС є:

основи кібергігієни;

організація інформаційної безпеки ЛьвДУВС;

джерела загроз інформаційній безпеці та об'єкти захисту;

принципи, методи захисту інформації та заходи щодо протидії загрозам безпеки;

нормативно-правові акти та відомчі розпорядчі документи з питань інформаційної безпеки і кібербезпеки;

процедура реагування на інциденти інформаційної безпеки та кібербезпеки.

12.4. Формами підвищення обізнаності осіб з числа постійного та перемінного складу ЛьвДУВС з питань інформаційної безпеки та кібербезпеки є:

навчання в межах освітнього процесу;

факультативні заняття;

тренінги;

інформування;

практичні заняття з налаштування захисту персональних пристроїв;

проведення бінарних занять запрошених експертів з кіберполіції;

перевірки дотримання правил інформаційної безпеки та кібербезпеки;

періодичне оцінювання рівня знань;

моніторинг дотримання інформаційної безпеки;

аналіз інцидентів та розбір типових помилок;

спільні наради;

електронне навчання.

12.5. Підвищення обізнаності осіб з числа постійного та перемінного складу ЛьвДУВС з питань інформаційної безпеки та кібербезпеки здійснюється з використанням презентацій, плакатів, слайдів, відеозаписів, роздаткового матеріалу, веб-технологій, повідомлень на корпоративну електронну пошту тощо.