МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ДНІПРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

НАКАЗ

01.10.2024 м. Дніпро № 646

Про затвердження Положення про систему контролю доступу та відеоспостереження в Дніпровському державному університеті внутрішніх справ

Відповідно до статті 307 Цивільного кодексу України, статей 6, 7 Закону України «Про захист персональних даних», статей 2, 6, 7, 11 Закону України «Про інформацію», підпункту 2 пункту 4, підпункту 7 пункту 5 Положення про Міністерство внутрішніх справ України, затвердженого постановою Кабінету Міністрів України від 28 жовтня 2015 року № 878, з метою врегулювання порядку організації та використання системи контролю доступу та відеоспостереження в Дніпровському державному університеті внутрішніх справ

НАКАЗУЮ:

1. Затвердити Положення про систему контролю доступу та відеоспостереження в Дніпровському державному університеті внутрішніх справ (додаток 1).
2. Ознайомити з Положенням про систему контролю доступу та відеоспостереження постійний та перемінний особовий склад університету.

Контроль за виконанням цього наказу покласти на проректора підполковника поліції Ігоря КОВАЛЬОВА.

Ректор
полковник поліції **Олександр МОРГУНОВ**

Додаток 1
до наказу ДДУВС
від 11.11.2024 № 616

Положення
Про систему контролю доступу та відеоспостереження на території Дніпровського державного університету внутрішніх справ

І. Загальні положення

1. Це положення визначає мету, структуру, суб'єктів, порядок організації та використання системи контролю доступу та відеоспостереження (далі – Система) на території Дніпровського державного університету внутрішніх справ (далі – університет) та території, прилеглій до його периметральної огорожі, в адміністративних будівлях ДДУВС та контрольно-пропускних пунктах університету за адресою: пр. Науки 26, м. Дніпро.

2. У цьому Положенні терміни вживаються в таких значеннях:

автоматизоване робоче місце користувача інформації в Системі – робоче місце, обладнане комп'ютерною технікою, що підключена до електронної комунікаційної мережі і призначене для автоматизації службової діяльності, реалізації повноважень з обробки інформації, наданих розпорядником Системи;

віртуальний центр – апаратно-програмний комплекс, який складається із серверів, призначений для виконання функції комутації та маршрутизації потоків інформації в Системі;

комутаційний центр – апаратно-програмний комплекс, призначений для виконання функції комутації та маршрутизації потоків інформації в Системі;

система гарантованого електроживлення – комплекс організаційних заходів і технічної складової – електричного обладнання, що забезпечує безперебійну подачу електроенергії у складові системи контролю доступу та відеоспостереження в разі збою або відмови в роботі зовнішньої мережі, електроживлення та складається із джерела безперебійного живлення, що живить центральний програмно-технічний комплекс і джерела безперебійного живлення, що живить усю Систему в цілому;

система контролю доступу та відеоспостереження – сукупність технічних засобів та програмного забезпечення, призначених для обробки інформації, що утворюється у процесі контролю та управління доступом, відеоспостереження на території університету;

центральне сховище даних – програмно-технічний комплекс, який складається із серверів, систем керування базами даних, та іншої програмної продукції, призначених для безперервного виконання операцій, записування, зберігання, знищення, зберігання системних журналів аудиту роботи, користувачів інформації в Системі та системних журналів реєстрації роботи програмного забезпечення;

центральний програмно-технічний комплекс – сукупність технічних засобів і програмного забезпечення, призначених для обробки інформації, який забезпечує розподіл прав проходу через точки контролю доступу, розмежування прав доступу користувачів інформації Системи, введення, записування, формування, зберігання та видалення інформації в Системі, моніторинг стану інформаційного обміну між

складовими Системи, а також системних журналів аудиту роботи користувачів інформації Системи, технічних засобів і програмного забезпечення, ведення відеоспостереження на території університету та ведення запису до центрального сховища даних з камер відеоспостереження.

Інші терміни в цьому Положенні вживаються у значеннях, наведених у Законах України «Про електронні комунікації», «Про захист персональних даних», «Про інформацію», «Про захист інформації в інформаційно-комунікаційних системах», «Про технічні регламенти та оцінку відповідальності», Порядку організації та забезпечення режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, затвердженого постановою Кабінету Міністрів України від 18 грудня 2013 року №939/ДСК, та інших нормативно-правових актах України у сфері захисту інформації та охорони державної таємниці.

3. Система є автономною і працює без підключення до інших інформаційно-комунікаційних систем та мереж передачі даних, у тому числі до мережі «Інтернет». Будь-яке віддалене втручання в роботу Системи заборонено.

4. Дія цього Положення в частині контролю доступу поширюється на осіб, яким видана магнітна перепустка відповідно до вимог Правил пропускного режиму на території університету, затверджених наказом ДДУВС від 03 липня 2024 року №414/ДСК, та Правил внутрішньооб'єктового режиму у ДДУВС, затверджених наказом ДДУВС від 21 березня 2024 №189/ДСК, а в частині відеоспостереження – на всіх осіб, які перебувають на території університету

5. Метою обробки персональних даних у Системі є забезпечення реалізації державної політики у сфері охорони державної таємниці в частині виконання вимог пропускного та внутрішньооб'єктового режимів на території університету відповідно до вимог Закону України Про державну таємницю та Порядку організації та забезпечення режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, затвердженого постановою Кабінету Міністрів України від 18 грудня 2013 року №939/ДСК.

6. Контроль доступу та відеоспостереження на території університету здійснюється відкрито.

7. Система забезпечує контроль доступу та відеоспостереження.

Контроль доступу здійснюється з метою:

- регулювання доступу на території ДДУВС.
- моніторингу переміщення осіб на територію університету.
- запобігання несанкціонованому доступу до університету та проникненню до режимних територій, зон і приміщень університету.
- зберігання інформації про переміщення особи на території університету, де здійснюється контроль доступу.

Відеоспостереження здійснюється з метою:

- забезпечення режиму безпеки на території університету.
- спостереження відвідувань об'єктів університету.
- виявлення нетипових ситуацій у зоні здійснення відеоспостереження.

- відеофіксація подій для об'єктивної їх оцінки та вжиття заходів реагування в разі виникнення нетипових ситуацій.

II. Режим (умови) контролю доступу та відеоспостереження

1. Особи ідентифікуються в Системі за магнітними перепустками. Магнітна перепустка є складовою контролю доступу на територію університету та являє собою пластикову картку, на якій міститься інформація про особу, якій вона видана. Запис інформації щодо використання особою магнітної перепустки під час пересування на об'єктах університету здійснюється в постійному режимі.

Відділ організації служби університету видає магнітні перепуски всім працівникам та здобувачам освіти відповідно до їх фактичної кількості під підпис. Після підписання наказу про прийом на роботу працівника університету та прийом на навчання здобувача освіти відділ кадрового забезпечення університету не пізніше одного робочого дня подає заявку на видачу магнітної перепустки до відділу організації служби.

Відділ організації служби повідомляє кожному працівнику університету (здобувачу освіти), для яких оформлюється магнітна перепустка, про потребу внесення в базу даних Системи фотокартки працівника (здобувача освіти). Працівник (здобувач освіти) повинен сфотографуватися чи принести свою фотокартку на електронному носії. Після звільнення працівник (здобувач освіти) забов`язаний здати перепустку до відділу організації служби.

Відділ кадрового забезпечення після підписання наказу про звільнення працівників (здобувачів освіти) не пізніше одного робочого дня подає до відділу організації служби перелік звільнених працівників (здобувачів освіти).

Відповідальний за зберігання та облік магнітних перепусток працівник (далі – Відповідальний працівник) проводить перевірку наявності та стану магнітних перепусток.

Виявлені непридатні до використання магнітні перепустки та перепустки звільнених працівників (здобувачів освіти) заносяться до відповідного акту списання.

Акт списання магнітних перепусток затверджується начальником відділу організації служби.

Знищення магнітних перепусток проводиться шляхом подріблення або спалювання у присутності комісії, до складу якої входять щонайменше три особи, включаючи Відповідального працівника. За результатами знищення магнітних перепусток складається акт знищення, який підписується всіма членами комісії.

Акти знищення магнітних перепусток зберігаються у відділі організації служби протягом трьох років.

Строк зберігання даних в Системі становить 1 рік після звільнення працівника (здобувача освіти).

2. При оформленні магнітної перепустки інформація про особу вноситься до програмного забезпечення контролю доступу. Особі, яка отримала магнітну перепустку роз'яснюються правила та обов`язки щодо її зберігання та використання.

3. Особи, які потрапляють до зони видимості камер відеоспостереження, інформуються про ведення відео фіксації шляхом розміщення спеціальних повідомлень.

4. Запис із камер відеоспостереження здійснюється до центрального сховища даних центрального програмно-технічного комплексу Системи. За допомогою програмного забезпечення, встановленого на автоматизованих робочих місцях користувачів інформації в Системі, зображення виводиться на монітор.

5. Запис із камер відеоспостереження здійснюється в постійному режимі або внаслідок детекції руху, що потрапляє до зони виявлення руху відеокамер залежно від їх технічних можливостей.

6. Строк зберігання відеозапису в центральному сховищі даних становить 14 днів.

7. Відеозаписи після закінчення строку їх зберігання автоматично видаляються з носіїв інформації центрального сховища даних шляхом перезапису.

8. Користувачі інформації в Системі ознайомлюються з вимогами законодавства щодо захисту персональних даних і забезпечують захист персональних даних, що містяться в Системі, від випадкових втрат, знищення, незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних.

9. Обробка та зберігання даних, отриманих у результаті функціонування Системи, здійснюються відповідно до вимог законодавства у сфері захисту інформації.

10. Місце розміщення та перелік встановлених зчитувачів магнітних карток та камер відеоспостереження визначаються планами їх розміщення на території університету та затверджуються ректором університету.

III. Суб'єкти Системи

1. Суб'єктами Системи є: власник, розпорядник, володілець інформації в Системі, користувачі інформації в Системі, адміністратор.

2. Власником і розпорядником Системи є держава в особі Дніпровського державного університету внутрішніх справ. Власник системи вживає заходів з організації матеріально-технічного забезпечення, необхідного для ефективного функціонування Системи.

3. Володільцем інформації в системі є Дніпровський державний університет внутрішніх справ.

4. Користувачем інформації в Системі є:

- ректор, проректора, директор Ліцею.
- посадові особи режимно-секретного відділу університету, які уповноважені використовувати інформаційні ресурси Системи.
- посадови особи відділу організації служби університету, які забезпечують пропускний режим та цілодобову охорону території університету.
- посадові особи відділу інформаційно-технічного забезпечення.

5. Адміністратором Системи є відділ інформаційно-технічного забезпечення.

Адміністратор Системи забезпечує:

- реалізацію заходів з інформаційного, технічного і програмно-технологічного функціонування Системи.
- надання, обмеження, припинення доступу користувачам інформації в Системі до Системи.
- збереження та захист інформації, що міститься в Системі.
- впровадження та вдосконалення програмно-апаратних засобів Системи.
- визначення правил управління інформаційною безпекою, політики управління ризиками.
- здійснення заходів із створення, підтримки та технічного адміністрування інформаційно-комунікаційних засобів, програмних та апаратних компонентів, що використовуються для забезпечення функціонування Системи.
- автоматизацію реєстраційних та облікових процесів Системи

IV. Структура Системи.

1. Складовими Системи є:
- центральний програмно-технічний комплекс.
- електронна комунікаційна мережа.
- система гарантованого електроживлення.
- комплексна система захисту інформації.
2. До складу центрального програмно-технічного комплексу входять:
- комутаційний центр.
- центральне сховище даних.
3. Центральний програмно-технічний комплекс Системи розміщується в окремій кімнаті на території університету.

V. Захист інформації в Системі

1. Захист інформації в Системі забезпечується створенням у ній комплексної системи захисту інформації.

Користувачі інформації в Системі отримують доступ до даних, що містяться в Системі, відповідно до наданого їм власником системи рівня доступу.

Для забезпечення доступу до Системи застосовується ідентифікація користувачів інформації в Системі.

2. Власник Системи створює умови та вживає заходів для забезпечення зберігання, запобігання несанкціонованому доступу та поширенню інформації з інформаційних ресурсів Системи.

Начальник
відділу організації служби
підполковник поліції **Андрій АНДРЕЄВ**