Витяг з протоколу № 17
засідання виїзної розширеної колегії Державного агентства лісових ресурсів України, що відбудеться на базі державних лісогосподарських підприємств, що координуються Волинським обласним управлінням лісового та мисливського господарства, та Шацького національного природного парку
18 – 19 серпня 2022 року

6. Нова політика безпеки для мереж камер спостереження за пожежною ситуацією в лісовому фонді.

Колегія розглянула питання про запобігання несанкціонованого доступу до елементів систем відео нагляду за пожежами (СВНп) та витоку інформації службового характеру і з метою запобігання несанкціонованого доступу до елементів систем відео нагляду за пожежами (СВНп) та витоку інформації службового характеру рекомендує наступне:

При налаштуванні всіх елементів СВНп з типами доступу «без доступу до мережі інтернет» дотримуватися наступних політик:

- Встановити на всіх активних елементах СВНп мережі IP-адресу шлюзу за замовчуванням, яка була б відмінною від основної і резервної IP-адреси каналів інтернету.
- Заборонити використання стандартних параметрів користувача та пароля для авторизації на обладнанні (наприклад admin) та встановити довжину пароля мінімум з 10 символів (цифри, літери, символи).
- Вимкнути додаткові сервіси адміністрування обладнання такі як SSH, Telnet, SNMP якщо вони не знаходяться у активному використанні.
- На всіх шлюзах, які використовуються на підприємстві заборонити доступ до мережі інтернет всьому активному обладнанню СВНп з вище зазначеним типом доступу.

При налаштуванні всіх елементів СВНп з типами доступу «обладнання зі спеціальним доступом до мережі інтернет» дотримуватися наступних політик:

- Встановити на всіх активних елементах СВНп мережі IP-адресу шлюзу, який дозволяє забезпечити безпечний віддалений доступ.
- Для організації шлюзів інтернет віддавати перевагу спеціалізованим пристроям з потужним фаерволом і системою фільтрації трафіку.
- Заборонити використання стандартних параметрів користувача та пароля для авторизації на обладнанні (наприклад admin) та встановити довжину пароля мінімум з 10 символів (цифри, літери, символи).
- Переналаштувати систему таким чином, щоб IP камери СВНп не мали прямого доступу до мережі інтернет. Віддалений доступ до СВНп здійснювати через проміжне обладнання (відеореєстратор), які мають значно вищий рівень захисту і керування віддаленим доступом.
- Для організації каналів передачі даних віддаленого доступу віддавати перевагу шифрованим тунельним з'єднанням (наприклад L2TP IPsec, Open VPN та інш.), а також комбінаціями цих з'єднань з елементами пасивного захисту (наприклад PortKnock, або СМС авторизація).

- Рекомендується виокремлювати трафік всього активного обладнання СВНп в окрему підмережу за допомогою vlan.

Проведення вказаних заходів і застосування всіх рекомендацій по налаштуванню СВНп на практиці дуже сильно знизить ризик витоку службової інформації та несанкціонованого доступу до обладнання. Ризик зламу системи оцінюється в 1-2%, через людський фактор.

КОЛЕГІЯ ВИРІШИЛА:

1. Керівникам територіальних управлінь забезпечити виконання керівниками підприємств, установ та організацій, що координуються обласними управліннями:

1.1. З'ясування у виробників систем відеонагляду за пожежами (СВНп) з якими зовнішніми сервісами взаємодіють їхні програмні та апаратні складові СВНп через мережу інтернет. Результат у вигляді довідки (довільної форми) надати до Державного агентства лісових ресурсів України. Термін – до 31.08.2022.

1.2. Проведення аудиту встановленого обладнання, що входить до СВНп, а саме:

- Визначити перелік всього активного обладнання СВНп (IP камери, відеореєстратори, сервери,керовані свічі і т.д.).
- Визначити схему інтеграції СВНп у локальну мережу підприємства.
- Провести аудит налаштувань активного обладнання СВНп.
- Умовно розділити обладнання за типами доступу на обладнання «без доступу до мережі інтернет» та «обладнання зі спеціальним доступом до мережі інтернет».
- Визначити сервіси СВНп, які безпосередньо взаємодіють з мережою інтернет та до яких надано віддалений доступ користувачам у межах своїх службових обов'язків.
- Проінформувати Держлісагентство щодо результатів проведення аудиту встановленого обладнання. Термін - до 31.08.2022.

1.3. Проведення переналаштування у відповідності до інструкції із Протоколу засідання колегії Державного агентства лісових ресурсів України від 18-19 серпня 2022 року щодо «Нової політики безпеки для мереж камер спостереження за пожежною ситуацією в лісовому фонді» всього активного обладнання СВНп та локальної мережі для запобігання витоку інформації службового характеру до мережі Інтернет. За результатами проведення робіт надіслати звіт щодо переналаштування всього активного обладнання СВНп та локальної мережі. Термін - до 19.09.2022.

Голова колегії **Юрій БОЛОХОВЕЦЬ**

Згідно:

Секретар колегії **Алла СВЯТЕЦЬКА**