УДК 621.3

Дацюк А. О., магістрант, гр. ЗІСТм-21-1
Науковий керівник: Дубина О. Ф., канд. техн. наук., доцент,
доцент кафедри БІ та Т
Державний університет «Житомирська політехніка»

ІНФОРМАЦІЙНА БЕЗПЕКА В СИСТЕМАХ ОХОРОННОГО ВІДЕОСПОСТЕРЕЖЕННЯ

На теперішній час замовник системи відеоспостереження бажає отримати систему безпеки, яка справно функціонує, виконує поставлені завдання в рамках заданих параметрів. З одного боку відеоспостереження – це по суті технологічна система, яка рідко коли задіється в рамках основної виробничої діяльності замовника, а відповідно і ІТ-шників. З іншого боку – сьогодні IP-відеоспостереження – це класична ІТ-інфраструктура як з усіма її перевагами, так і недоліками – такими як загрози інформаційної безпеки, в якій господарники, а часом і служ-ба охорони, просто не мають необхідних компетенцій.

В результаті складається ситуація, коли рідкісний замовник замислюється про інформаційну безпеку проектів відеоспостереження, але саме він в першу чергу і страждає від проблем в інформаційному за-хисті. Методи захисту і рекомендації в області інформаційної безпеки є у виробників, але ні проектувальник, ні інсталятор за своєю ініціативою навряд чи будуть вивчати цю інформацію.

Вихід з цієї ситуації може бути в залученні експертів ІТ-департаменту, або зовнішніх експертів в області інформаційної безпеки до написання ТЗ на систему відеоспостереження. Саме експерт повинен скласти модель загроз і сформулювати вимоги до рівня інфор-маційної безпеки відповідно до передбачуваних загроз, відомих на поточний момент. Експерт допоможе проконтролювати проектні рішення і вказівки для інсталятора на відповідність сформульованим вимогам, проконтролювати і прийняти роботу інсталятора в частині реалізації заходів забезпечення інформаційної безпеки, проводити періодичний аудит системи захисту.

В відеоспостереженні потрібно захищати:

– Відеоархіви і бази даних (псування записів, втрата файлів відеоархіву, підміна файлів відеоархіву, несанкціонований перегляд відео-архіву).
– Канали зв'язку, що використовуються в системі відеоспостереження (перехоплення даних, псування, зміна, умисні перешкоди при передачі, нестабільна передача даних не пов'язана безпосередньо з зловмисним втручанням).
– Пристрої: камери, комутатори, сервери, і інші розумні пристрої (вразливі місця: конфігурація (програмні налаштування обладнання), несанкціонований доступ до зображення і управління).

Від чого потрібно захищати відеоспостереження.

Людський фактор.

Цю «групу загроз» варто розділити на дві категорії. Перша – зловмисники. Це люди, які не ріжуть дроти і не мажуть фарбою об'єктиви – їхні методи акуратні і непомітні. Можливо, саме тому відстежити такого роду загрози дуже важко. Саме ж в результаті може бути завдано наступний збиток:

– знищення або підміна записів архівів;
– зміна налаштувань і режимів роботи системи;
– несанкціонований доступ до спостереження і перегляду архівів;
– використання системи для власних завдань хакера.

Друга група – це некваліфікований персонал. На відміну від попередньої категорії загроз, тут відсутній злий умисел. Однак результати неграмотного або неакуратного користування можуть бути рівно такі ж, як і в разі наявності умислу.

«Перешкоди» від стороннього обладнання.

Цей тип загроз зустрічається, якщо система IP-відеоспостереження не є закритою і використовує мережі зв'язку спільно з іншими системами підприємства (IP-телефонія, ERP-системи і т.п.). Якщо проектувальник або інсталятор не звернув уваги на їх наявність і роботу – високий шанс зіткнутися з якимись програмними конфліктами, що заважають нормальній роботі. У підсумку: нестабільна роботи системи.

Шкідливе ПЗ. Всім відомі «віруси», «троянці», «шифрувальники» ... Як не дивно, незважаючи на широку популярність, дуже на багатьох об'єктах досі взагалі немає ніякого захисту від цього типу загроз.

Методи забезпечення інформаційної безпеки.

– вбудований захист ПЗ відеоспостереження.
– захист на рівні комутаційного обладнання.
– власний захист обладнання відеоспостереження.

Таким чином, у залежності від типу інформації (конфіденційна, для службового користування і т.д), яка циркулює на об'єкті, що охороняється, необхідно приймати відповідні заходи щодо захисту самої системи охорони.