спеціалізованих приладів, розрахованих на специфічні вимоги, другий – застосування універсальних приладів – аналізаторів акумуляторів. Отже й область застосування останніх значно ширше.

Одержано 17.04.2018

УДК 343.982:351.74

Владислав Володимирович ЛАКТІОНОВ,
курсант групи Ф4-102 ХНУВС
Науковий керівник: старший викладач кафедри кібербезпеки факультету № 4 ХНУВС Рвачов О. М.

НОВІТНІ ЗАСОБИ СПЕЦІАЛЬНОЇ ТЕХНІКИ ТА ТЕХНОЛОГІЇ В ДІЯЛЬНОСТІ ПОЛІЦІЇ

У наш час важко уявити ефективну протидію злочинності без використання поліцією спеціальної техніки та сучасних інформаційних технологій.

До популярних технічних засобів, які зараз активно впроваджуються в діяльність поліції багатьох країн світу, у тому числі в Національній поліції України, можна віднести:

1) безпілотні літальні апарати, які в останні роки почали активно використовуватися правоохоронними органами багатьох країн світу для:

– спостереження;

– збирання доказів;

– контролю за натовпом;

– відслідковування біженців;

2) GPS-трекери, які за допомогою супутникової навігації передають через мобільний зв'язок дані на сервер про місцезнаходження певного рухомого об'єкту. За допомогою цього сучасного приладу поліція має змогу:

– відслідковувати злочинців;

– здійснювати моніторинг за правильним виконанням працівниками поліції покладених на них обов'язків;

– координувати та відслідковувати місцезнаходження працівника поліції та їх транспортні засоби в режимі реального часу;

– встановлення місця перебування вкраденого транспорту;

3) системи виявлення вогнепальної зброї, які, використовуючи звукові датчики та відеокамери, надають змогу працівникам поліції швидко виявляти та реагувати на випадки застосування вогнепальної зброї.

В Україні поліцейські для забезпечення публічного порядку під час проведення масових заходів можуть застосовувати сучасний гелікоптер та спеціально обладнані автомобілі, наприклад, їх використовували під час проведення Євробачення-2017 та 9 травня 2017 року. Вони обладнані спеціальною відеоапаратурою, що має можливості фіксації правопорушень та оперативної передачі інформації до Ситуаційних центрів Національної поліції. Спеціально укомплектовані автомобілі розміщувалися неподалік масового скупчення громадян, що дозволило досконало володіти обстановкою та миттєво реагувати на будь-які події.

Україна також не відстає в інтеграції новітніх інформаційних технологій у діяльність правоохоронних органів, у тому числі у діяльність Національної поліції України. У зв'язку з тим, що у діяльності поліції одну з найважливіших ролей відіграє інформація (накопичення банків даних, їх обробка та аналіз), останнім часом в діяльність поліції починають активно впроваджувати хмарні технології обробки інформації. Сучасні інтернет-технології дозволяють швидко надати доступ до центральної системи обробки та зберігання інформації, що знаходиться у «хмарі», з будь-якої частини світу, що у свою чергу дає змогу поліцейському швидко реагувати на надзвичайні події, які виникли і були зафіксовані шляхом відеофіксації, направляти на місця виникнення надзвичайної ситуації відповідні сили і засоби.

Отже, з вище наведеного можна зробити висновок, що застосування новітніх засобів спеціальної техніки та технологій у діяльності правоохоронних органів допомагає забезпечувати безпеку населення на більш вищому рівні та зробити діяльність поліції більш ефективною.

Одержано 17.04.2018

УДК 62-03

Владислав Сергійович ШЕСТОПАЛЮК,
курсант групи Ф4-101 ХНУВС
Науковий керівник: викладач кафедри кібербезпеки факультету № 4 ХНУВС кандидат технічних наук Світличний В. А.

МЕТОДИ ТА ЗАСОБИ ПОШКОДЖЕННЯ ЗАМКІВ

Від того, який тип дверних замків ви віддасте перевагу, буде залежати безпека будинку, офісу, квартири, кабінету, сейфу, сховища і т. і. Розглянемо три типи установки замків, а саме: навісні замки; накладні замки; та врізані замки.

Незважаючи на те, що серед навісних замків є екземпляри з різними типами замикаючих механізмів з різними класом надійності, вони можуть бути просто вирвані монтуванням. Тому навісні замки частіше застосовують для замикання сараїв, підвалів, в яких не зберігаються цінні речі.

Звичайно на відміну від навісних замків краще – накладний, але в цьому є свої мінуси, тому що якщо їх накладають або встановлюють в середину дверей і це призводить до того що приходиться посилювати внутрішню частину дверей, а це призводить до того, що вони стають занадто тяжкими і частіше ламаються та ремонт обходиться дорожче.

Але зауважимо, що потрібно надати більшу перевагу врізаним замкам, тому що головна особливість замку цього типу – це кріплення його всередині дверного полотна, що робить його більш естетичним зсередини і, на відміну від навісних замків, більш надійним від в злому.

Злодіям для відкривання замків потрібні відмички різних видів, які допомагають відкрити різні класів та типи замків. Звичайно 1 та 2 клас замку злодій відкриє занадто швидко, тому такі замки потрібно встановити на міжкімнатні двері, а на вхідні краще всього підійде 3 та 4 клас, який навіть самий досвідчений фахівець не зможе справитися менш ніж за 30 хвилин.

Для того щоб протидіяти в злому вашого майна, потрібно всього на всього збільшити точність виготовлення механізму секретності та встановити секретність зі складним профілем замкової шпарини, та системою автентичності ключа.

Крім відмичок існують інші способи відкривання замків, наприклад руйнація замкової щілини шляхом хімічної руйнації пружин. Щоб нейтралізувати загрози цієї проблеми необхідно застосувати:

а) захист накладок, які механічно перекривають доступ до замкової шпарини циліндрового механізму;

б) встановити циліндр, у якому сумарна довжина штифтової пари перевищує глибину камори в корпусі циліндрового механізму;

в) використання циліндрових механізмів, в яких серцевина блокується обертання стопорними елементами різного типу.

Один з методів силового деблокування відноситься ствердіння корпусу (фрезування), при якому створюються умови з нейтралізації окремих деталей, що блокують від обертання серцевини.

Також потрібно спостерігати за візуалізацією коду ключа, ще краще всього мати з собою ключ дублікат, який врятує вас від зламу чи пропажі ключа, також по можливості міняти свою серцевину замка кожних пів року.

Якщо встановити захисні накладки, які закривають доступ до торцевої частини механізму секретності, його вибиття суттєво ускладниться.

Виходячи зі специфіки розглянутих вище методів запобігання в злому механізму дверей та замків секретності та акцентування уваги на необхідність системного підходу до питання захисту приміщення, при якому оцінка стійкості від злому має враховувати показники кожного елементу: механізму секретності, замка, дверей тощо. Рекомендується проводити постійний моніторинг ситуації з означеним питанням безпеки.

Одержано 17.04.2018

УДК 004.9

Данило Олексійович КУЛІКОВ,
курсант групи Ф4-202 ХНУВС
Науковий керівник: викладач кафедри кібербезпеки факультету № 4 ХНУВС кандидат технічних наук Світличний В. А.

ПЕНТЕСТ ЯК ПРІОРИТЕТНИЙ НАПРЯМОК В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

У ситуації, що склалася в наш час, популярним стає пентест, іншими ж словами тестування на проникнення.

Пентест – це новий метод оцінки безпеки комп'ютерних систем або мереж засобами моделювання атаки зловмисника. Сам процес включає в себе активний аналіз системи на наявність потенційних вразливостей, які можуть спровокувати некоректну роботу цільової системи, або ж в результаті повну відмову в обслуговуванні. Важливо виділити мету самого пентеста – це оцінка можливості його здійснення і прогноз економічних втрат в результаті успішного здійснення атаки. Результатом є звіт, який містить в собі всі знайдені вразливості системи безпеки, а також може містити рекомендації щодо їх усунення. Тобто, можна зробити висновок, що випробування на проникнення є частиною аудиту безпеки.

Слід виділити кілька різних методик випробувань на проникнення. Основними відмінностями є наявність інформації про досліджувану систему. Існує чотири вида систем: відкриті, закриті, напівзакриті та цільові.

При перевірці закритої системи атакуючий не має гадки відомостей про пристрій, що атакується. Завданням такого виду перевірки є збір необхідної інформації про розташування цільової системи, її інфраструктури.

У відкритих системах доступна повна інформація про цільовій системі, а в напівзакритих системах доступна часткова інформація. Розглянемо цільові системи, до них відносяться комп'ютерні системи з доступом з мережі Інтернет. Випробування на проникнення повинно проводитися до запуску цільової системи в масове використання. Це дає певний рівень гарантії, що будь-який атакуючий не зможе завдати шкоди, прямої або непрямої, роботі досліджуваної системи.

Тест на проникнення дозволяє досить швидко оцінити реальну захищеність обраних інформаційних активів від несанкціонованого доступу, моделюючи найбільш поширені атаки. Основною відмінною особливістю тесту на проникнення в порівнянні з традиційним аудитом інформаційної безпеки є:

– велика деталізація знайдених вразливостей;

– більш точна оцінка ризиків ІБ (грунтується на результатах реалізації знайдених вразливостей);

– оцінка більшої кількості процесів ІБ, ніж при інструментальному аудиті, включаючи оцінку процесів (наприклад, управління інцидентами, моніторинг і т.д.), об'єктивна оцінка яких не може бути отримана іншими засобами (інструментальний аудит, анкетування і інтерв'ювання і т.д.);

– детальне опрацювання знайдених вразливостей, що дозволяє отримати більш об'єктивну оцінку процесів забезпечення інформаційної безпеки організації.