інформаційно-аналітичному забезпеченню діяльності правоохоронних органів і прийняттю своєчасних ефективних управлінських рішень.

Такими підрозділами є Ситуаційні центри Національної поліції України (СЦ). При цьому під центром розуміється не лише спеціально обладнане приміщення, але і відповідні інформаційні, телекомунікаційні, програмні та методичні засоби з метою вироблення відповідних управлінських рішень.

Співробітники правоохоронних органів у своїй роботі постійно використовують сучасні технології. І чим більше цих технологій, тим складнішим стає процес їх об'єднання і інтеграції.

Тому рішенням цієї проблеми стає об'єднання існуючих потоків інформації і інструментів управління в єдиний інформаційний візуальний простір на базі геоінформаційних системи (ГІС). Подібні рішення дозволяють повноцінно організувати збір необхідної інформації, її обробку, аналіз і надання доступу до результатів обробки.

Впроваджуючи геоінформаційні системи в роботу ситуаційних центрів, поліція отримує програмну платформу для реалізації ефективного управління та реагування в справі охорони громадського боротьби з правопорушеннями. ГІС з самого початку створювалися для збору, аналізу і відображення даних в найбільш зрозумілому людині вигляді: шляхом нанесення на карту.

Ситуаційні центри надають наступні можливості:

– Оперативний доступ до легкої для розуміння карти з виводом необхідної інформації, з використанням різних каналів передачі даних.

– Збір, зберігання і обробка даних про злочини, правопорушників, підозрюваних, місцях підвищеної небезпеки і будь-яких інших типах об'єктів.

– Надання результатів аналітичної роботи для виявлення залежності між кримінально значущою інформацією і прогнозованими ризиками при плануванні оперативно-розшукових заходів.

– Підвищення ефективності планування і прийняття управлінських рішень.

Ситуаційний центр, перш за все, побудований на аналізі ситуації. За словами начальника Департаменту організаційно-аналітичного забезпечення та оперативного реагування МВС України полковника поліції Сергєєва О.О. у Національній поліції України використовують три види аналізу. Стратегічний (кримінологічний) – аналіз злочинності, її рівня, поширеності, динаміки, структури загалом. Проводиться аналіз стану злочинності в країні, визначається, в яких регіонах складна криміногенна ситуація, і що потрібно робити, щоб стабілізувати обстановку. Другий рівень – тактичний аналіз. Це ситуація впродовж доби, тижня щодо конкретних регіонів, конкретних видів злочинів. Саме цим і займаються ситуаційні аналітики. Третій рівень (один із найскладніших) – практичний. Це оперативний кримінальний аналіз. Це робота щодо кожного конкретного тяжкого та особливо тяжкого злочину.

Одержано 17.04.2018

УДК 342.922

Дмитро Олександрович РУДЕНКО,
Андрій Олександрович ЛАЩЕНКО,
студенти групи КБдср-17-1 ХНУВС
Науковий керівник: завідувач кафедри інформаційних технологій факультету № 4 ХНУВС кандидат технічних наук, доцент Струков В. М.

ВИКОРИСТАННЯ АКТИВНИХ МЕТОДІВ ВТОРГНЕННЯ У КОМП'ЮТЕРНІ МЕРЕЖІ

Серед активних методів виявлення вторгнення у комп'ютерні мережі одним з найбільш широко використовуваних є так звані сніфери.

Аналіза́тор тра́фіку, або сні́фер (від англ. *to sniff* – нюхати) – програма або програмно-апаратний пристрій, призначений для перехоплення і подальшого аналізу, або тільки аналізу мережевого трафіку, призначеного для інших вузлів.

Перехоплення трафіку може здійснюватися:

– звичайним «прослуховуванням» мережевого інтерфейсу (метод ефективний при використанні в сегменті концентраторів (хабів) замість комутаторів (світчей), інакше метод малоефективний, оскільки на сніфер потрапляють лише окремі фрейми);

– підключенням сніфера в розрив каналу;

– відгалуженням (програмним або апаратним) трафіку і спрямуванням його копії на сніфер;

– через аналіз побічних електромагнітних випромінювань і відновлення трафіку, що таким чином прослуховується;

– через атаку на канальному (MAC-spoofing) або мережевому (3) рівні (IP-spoofing), що приводить до перенаправлення трафіку жертви або всього трафіку сегменту на сніфер з подальшим поверненням трафіку в належну адресу.

На початку 1990-х широко застосовувався хакерами для захоплення призначених для користувача логінів і паролів, які у ряді мережевих протоколів передаються в незашифрованому або слабозашифрованому вигляді. Широке розповсюдження хабів дозволяло захоплювати трафік без великих зусиль у великих сегментах локальної мережі практично без ризику бути виявленим.

Сніфери застосовуються як в цілях профілактики та протидії кібератакам, так і в деструктивних цілях.

Аналіз трафіку, що пройшов через сніфер, дозволяє:

Виявити паразитний, вірусний і закільцьований трафік, наявність якого збільшує завантаження мережного устаткування і каналів зв'язку (сніфери тут малоефективні; як правило, для цих цілей використовують збір різноманітної статистики серверами і активним мережним устаткуванням і її подальший аналіз).

Виявити в мережі шкідливе і несанкціоноване ПЗ, наприклад, мережеві сканери, флудери, троянські програми, клієнти пірінгових мереж та інші (це зазвичай роблять за допомогою спеціалізованих сніферів – моніторів мережної активності).

Перехопити будь-який незашифрований (а деколи і зашифрований) призначений для користувача трафік з метою отримання паролів і іншої інформації.

Локалізувати несправність мережі або помилку конфігурації мережних агентів (для цієї мети сніфери часто застосовуються системними адміністраторами)

Оскільки в «класичному» сніфері аналіз трафіку відбувається вручну, із застосуванням лише простих засобів автоматизації (аналіз протоколів, відновлення TCP -потоку), то він підходить для аналізу лише невеликих його обсягів.

Одержано 17.04.2018

УДК 004.056.53

Євгенія Юріївна СПОРИШ,
студент групи Ф-6-3Ідср-14-1 ХНУВС
Науковий керівник: доцент кафедри інформаційних технологій факультету № 4 ХНУВС кандидат технічних наук, доцент Тулупов В. В.

ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ ВІДЕОСПОСТЕРЕЖЕННЯ

Актуальність обраної теми полягає в тому, що в сучасних умовах основна частина атак зловмисників здійснюється через комп'ютерні мережі, постійно ускладнюється їх структура, швидко збільшується кількість комп'ютерів та мережевого обладнання у тому числи систем відеоспостереження.

Захист інформації є складовою частиною забезпечення національної безпеки будь-якої держави і забезпечується правовими, організаційними, програмними та інженерно-технічними заходами.

На державному та регіональних рівнях впроваджуються різні програми та заходи безпеки. Так, наприклад у березні 2018 року на сесії Харківської обласної ради була прийнята «Програма забезпечення публічної безпеки і порядку та протидії злочинності на території Харківської області на 2018–2019 роки», відповідно до якої будуть придбатися системи відеоспостереження, стаціонарні переговорні пристрої для термінового виклику спецслужб, електронні планшети, відеореєстратори, відеотехніка та сучасні засоби зв'язку для груп швидкого реагування та правоохоронців.

Серед завдань програми є:

– удосконалення науково-методичного, матеріально-технічного та інформаційного забезпечення правоохоронних та інших органів, що беруть участь у забезпеченні публічної безпеки та порядку;

– безперервний моніторинг криміногенної ситуації в області, в т.ч. за рахунок соціологічних технологій та забезпечення своєчасного реагування на негативні зміни;

– здійснення посиленого контролю за ситуацією у публічних місцях, передусім при проведення заходів за участю значної кількості громадян;

– запобігання правопорушенням, що вчиняються з використанням телекомунікаційних мереж та мережі Інтернет.

На теперішній час у системі Міністерства внутрішніх справ впроваджено низку аналітичних систем з можливістю проведення глибокого аналізу великих масивів інформації, включаючи відкриті джерела де на першому рівні є система відеомоніторингу наприклад – єдиний аналітичний сервісний центр (UASC) поліції, створений за прикладом системи безпеки Абу-Дабі при ГУНП в Донецькій області.

Метою даної роботи є дослідження можливості побудови безпечної мережі відеоспостереження за об'єктами.

Відповідно до поставленої мети визначимо наступні завдання:

– охарактеризувати стан проблем існуючих систем відеоспостереження та їх використання суб'єктами господарювання;

– дослідити канали витоку інформації та сучасні методи й засоби захисту мереж відеоспостереження;

– проаналізувати технічні завдання на проектування мереж відеоспостереження та існуючи системи на сучасному ринку готового обладнання.

Одержано 17.04.2018

УДК 004.728:519.87

Павло Сергійович ВЄЛЬКІН,
студент групи КІТз-72м Національного технічного університету «Харківський політехнічний інститут»
Науковий керівник: професор кафедри інформаційних технологій факультету № 4 ХНУВС доктор технічних наук, професор Можаєв О. О.

МОДЕЛЮВАННЯ ПЕРЕДАЧІ МУЛЬТИМЕДІЙНОЇ ІНФОРМАЦІЇ В ГЕТЕРОГЕННИХ КОМП'ЮТЕРНИХ МЕРЕЖАХ

При проектуванні, реалізації та обслуговуванні інформаційних телекомунікаційних систем і мереж зв'язку часто зустрічаються випадки, коли аналітичне рішення задачі практично неможливо в силу значних математичних труднощів, а проведення експериментальних досліджень та натурних випробувань вимагає досить великих витрат часу і коштів. Питання моделювання інформаційних процесів, систем і мереж розглядаються в даній роботі.

В результаті аналізу традиційних методів та моделей опису мережевого трафіку та визначення характеристик мережевого трафіку були наведені вимоги до якості обслуговування мережі, к яким відносяться – прозорість, доступність і надана пропускна здатність мережі. Детально розглянуті види мережевого трафіку та оцінки параметрів мережі.