УДК 004

Я.Білан, магістр гр. КІ-23М
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ВІДДАЛЕНОГО АДМІНІСТРУВАННЯ СЕРВЕРАМИ ЗА ДОПОМОГОЮ KVM-OVER-IP-ПЕРЕМИКАЧІВ

У статті розроблено програмне забезпечення, яке призначено для системи віддаленого адміністрування серверами за допомогою KVM-over-IP-перемикачів. Метою розробки є дослідження та програмна реалізація системи віддаленого адміністрування серверами за допомогою KVM-over-IP-перемикачів.Об'єктом дослідження є процес віддаленого адміністрування серверами за допомогою KVM-over-IP-перемикачів.Предметом дослідження є методи віддаленого адміністрування серверами за допомогою KVM-over-IP-перемикачів.Методи дослідження базуються на методах теорії комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення.Результат роботи – програмна реалізація системи віддаленого адміністрування серверами за допомогою KVM-over-IP-перемикачів.В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

Постановка проблеми. Для рішення завдань керування, економії простору в серверних шафах і рятування від зайвих кабелів багато адміністраторів використовують перемикачі клавіатури, відео й миші (Keyboard, Video, Mouse, KVM). Ці пристрої забезпечують контроль за безліччю серверів і іншим устаткуванням з однієї консолі, причому сервери зовсім не повинні бути однотипними: вони можуть працювати під керуванням самих різних систем – Windows, Unix, Linux.

Щоб ближче познайомитися з можливостями сучасних KVM, їхньою роллю й місцем у керуванні сучасної серверної й IT-інфраструктурою, у роботі розробляється програмне забезпечення, що дозволяє реалізувати потребу в модернізації серверного парку. Використовувані в її ЦОД перемикачі KVM застаріли – зокрема, вони можуть підтримувати тільки обмежене число серверів і не забезпечують віддалений доступ.

Отже, компанія збирається модернізувати свій серверний парк у ЦОД, а заодно обновити й уніфікувати керування серверами. На площадці розміщається 20 стійок з устаткуванням, половину з них займають успадковані різнотипні сервери різних форм-факторів і конфігурацій. Заповнення стійок нерівномірне – від декількох серверів, у тому числі із блейд-системами й UNIX-системами, до 20 і більше. Стійки, що залишилися, планується заповнити однотипними серверами під віртуалізацію (остаточного рішення про вибір моделі ще не прийняте).

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи віддаленого адміністрування серверами за допомогою KVM-over-IP-перемикачів.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи віддаленого адміністрування серверами за допомогою KVM-over-IP-перемикачів.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем віддаленого адміністрування серверами за допомогою KVM-over-IP-перемикачів.

– Дослідження системи віддаленого адміністрування серверами за допомогою KVM-over-IP-перемикачів.

– Програмна реалізація системи віддаленого адміністрування серверами за допомогою KVM-over-IP-перемикачів.

Об'єктом дослідження є процес віддаленого адміністрування серверами за допомогою KVM-over-IP-перемикачів.

Предметом дослідження є методи віддаленого адміністрування серверами за допомогою KVM-over-IP-перемикачів.

Методи дослідження базуються на методах теорії комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Одне з основних питань, що очікуване хвилює замовника, в тому що стосується доступу, особливо віддаленого, до критичного встаткування, – це безпека. Надійність і безпека – от основні критерії, якими необхідно керуватися при виборі рішення для централізованого керування засобами віддаленого доступу. Швидше за все, така стисліть пояснюється тим, що постачальники перемикачів KVM традиційно приділяють підвищену увагу темі захисту й розмежування доступу, тому наявність відповідних розвинених засобів сприймається як щось саме собою що розуміє, не потребуючих подальших пояснень.

Щоб одержувати доступ до конкретних комп'ютерів і управляти ними могли тільки авторизовані користувачі, у перемикачах Aten підтримується дворівневий парольний захист. У перемикачах застосовуються сильні алгоритми шифрування, DES, 3DES, AES; KVM, відео й інформація з віддаленого носія шифруються окремо. Канали можуть шифруватися різними алгоритмами, у тому числі й з довільним вибором на один сеанс. У свою чергу, система централізованого керування на базі CC2000 і перемикачів IP KVM підтримує багаторівневий доступ і дозволяє призначати наступні стандартні ролі: суперадміністратор, адміністратор, користувач, аудитор. При необхідності можна вводити власні ролі, виходячи з маски прав. Можливі зовнішня автентифікація й авторизація RADIUS, TACACS, LDAP, LDAPS, Active Directory.

У перемикачах Raritan здійснюється шифрування AES, авторизація може вироблятися за допомогою як убудованих засобів системи, так і зовнішніх серверів автентифікації LDAP/Radius. Система централізованого керування CommandCenter Secure Gateway забезпечує гнучке й зручне настроювання політик безпеки для окремих користувачів і цілих груп, надаючи «єдину точку входу» зі зручним і інтуїтивно зрозумілим інтерфейсом для доступу до відповідних серверів.

В програмному забезпеченні передбачені механізми поділу прав доступу до об'єктів і ролі кожного користувача (які сервіси йому будуть доступні при роботі із цим ПЗ), підтримується інтеграція з різними службами каталогів, такими як AD, LDAP, TACACS і RADIUS.

Якщо виходити із цих коротких описів, всі рішення оснащені приблизно однаковими функціями безпеки. Зокрема, у мережах Windows буде корисна можливість реєстрації на перемикачі IP KVM з використанням засобів автентифікації Active Directory і наданням різних рівнів доступу до підключених пристроїв на підставі наявних профілів користувачів Active Directory.

При каскадному підключенні один перемикач KVM може управляти декількома пристроями. Звичайно досить лише KVM-консолі KL1516A, але в деяких випадках адміністратори воліють застосовувати матричний KVM-перемикач KM0932/0532, тому що ці пристрої можуть інтегруватися з перемикачами серії KN (з керуванням по мережі) і використовувати єдиний графічний інтерфейс GUI, що набагато зручніше, оскільки відпадає необхідність двічі реєструватися в системі (login) – тим самим досягається краща інтеграція.

Можна використовувати успадковані KVM, якщо об'єднати їх під керуванням централізованої системи ATEN CC2000. Консольні KVM третіх виробників у принципі можуть бути інтегровані за схемою з'єднання порт – консоль, але без інтеграції меню і єдиної

авторизації, у зв'язку із чим рекомендується впроваджувати консолідоване рішення від одного виробника.

Інтеграція вже наявних KVM-перемикачів можлива на рівні інтерфейсу перемикача (наприклад, за допомогою KVM-подовжувача KXII-101-V2), тоді із централізованої системи можна одержати доступ до KVM-перемикача, а через нього – до цільових серверів. Для організації повністю «прозорого» безшовного доступу до цільових серверів (із централізованим керуванням правами користувача) підійдуть перемикачі KVM-over-IP серій KX, консольні сервери SX, гібридні пристрої KSX, а також матричні KVM-перемикачі серії Paragon.

Програмне забезпечення дозволяє додавати в систему пристрою KVM з марками IBM, Fujitsu і Dell (вони виробляються Avocent). Повноцінна інтеграція з іншими виробниками не підтримується.

Сучасні перемикачі KVM здатні підтримувати дозвіл Full HD. Бажаючи забезпечити максимально комфортні умови для роботи системних адміністраторів, замовник вирішив поцікавитися, який канал буде потрібно для передачі зображення з максимальним дозволом. При локальному доступі, коли підключення здійснюється по окремих кабелях, це не представляє проблеми, а при віддаленому – навряд чи хтось захоче виділити такий канал лише для забезпечення зручності віддаленого керування. Якщо ж до питання віддаленого доступу підійти з іншого боку, то при твердих обмеженнях на пропускну здатність, наприклад при доступі по мобільному зв'язку, виявляється досить 128 Кбіт/с і навіть менше.

Для підтримки відео максимально можливої якості в режимі 1600?1200 у випадку перемикачів Aten для кожного підключення буде потрібно канал 50 Мбіт/с. Мінімально ж необхідна для роботи пропускна здатність становить 128 Кбіт/с, причому пристрій може гнучко підбудовуватися під неї, аж до переходу на напівтонове, чорно-біле зображення. Однак для відносно комфортного використання окремих функцій Virtual Media потрібен канал більшої ширини.

Необхідна величина пропускної здатності каналу передачі даних для сеансу KVM – це завжди компроміс між якістю й швидкістю. Завдяки використанню передових апаратно-програмних рішень для компресії даних, over-IP-перемикачі Dominion KXIII компанії Raritan дозволяють передавати відео FullHD 1080p зі звуком по каналі до 30 Мбіт/с. Але, як правило, на практиці потрібна передача набагато більше скромних обсягів даних – наприклад, при типовій роботі з текстовими документами в інтерфейсі Windows завантаження каналу становить до 100 Кбіт/с. Однак і цей рівень може бути знижений у кілька разів за рахунок більше агресивних настроювань компресії, зменшення глибини кольору й дозволи. Таким чином, прийнятні умови для роботи можна одержати навіть при аварійному доступі через 3G-модем.

Для віддаленої роботи через програмне забезпечення не потрібно значної пропускної здатності – у мінімальному варіанті досить навіть модемного доступу. В програмному забезпеченні є механізм підстроювання під будь-яку швидкість каналу шляхом скорочення розміру вікна або кількості використовуваних квітів.

Що стосується забезпечення можливості віддаленої роботи відразу для декількох операторів, те все залежить від кількості відповідних шин/каналів у конкретного KVM. Наприклад, KVM KN 4124V с керуванням по мережі дозволяє підключити чотири віддалених канали, при цьому зниження якості не відбувається. Віддалений доступ – це так зване цифрове з'єднання, коли сигнали KVM і відео передаються в стислому виді; при локальному ж доступі звичайно використовується аналогове з'єднання, а якість передачі аналогового відео погіршується в міру збільшення відстані.

На відміну від ряду інших рішень, у випадку шлюзу UMG компанії Avocent його підключення до сервера є не аналоговим, а цифровим (TCP). Відповідно, воно краще захищено від перешкод і загасань сигналу з відстанню – для KVM-портів гарантується дальність 100 м від UMG до сервера. Для підключення KVM-портів використовуються спеціальні інтелектуальні кабельні інтерфейси, які й виконують всю оцифровку сигналів з

інтерфейсних портів сервера й забезпечують їхню передачу по звичайному кабелі Категорії 5. Завдяки тому, що процесор, що обробляє всі сигнали, переміщений з KVM в інтерфейсний модуль, стало можливо одночасно відкривати до 40 вікон, що дозволяють працювати з віддаленими серверами, тоді як раніше – не більше 8.

Якщо при звертанні до конкретного перемикача обмеження на кількість одночасно працюючих операторів звичайно досить тверді, то при використанні програмного забезпечення, зокрема CC2000 компанії Aten, кількість серверів, що обслуговуються одночасно, не обмежується. Однак, якщо використовується режим проксі, число серверів, що обслуговуються одночасно, залежить від потужності комп'ютера, на якому встановлено ПЗ, і пропускної здатності мережних інтерфейсів.

Розробка структурної схеми

Розглянемо доцільність застосування KVM при наявності в серверах серверних процесорів HP iLO, IBM RSA, Dell DRAC і ін. Тим більше що вони забезпечують ті ж (і навіть більші) можливості, що й перемикачі, – наприклад, доступ по окремому каналі, керування на рівні BIOS, підключення віртуальних носіїв (Virtual Media) і навіть включення/відключення живлення (у випадку KVM для цього потрібна інтеграція з PDU). Проте постачальники KVM не вважають, що їхньому встаткуванню не залишилося місця в серверні й ЦОД. Більше того, вони як і раніше наполягають на перевагах їхнього застосування. Аргументи наступні.

Перемикачі KVM-over-IP дозволяють одержати повний доступ до цільового сервера на рівні BIOS без необхідності придбання додаткових ліцензій або установки спеціалізованого ПЗ, що принципово відрізняє їх від програмних рішень і засобів доступу на базі сервісних процесорів. Останнім потрібно виділити окрему IP-адресу, що скорочує пул доступних адрес (для великих ЦОД це є актуальною проблемою), не говорячи про необхідність відповідних фізичних підключень. У випадку ж використання KVM досить одного IP-адреси (або двох при необхідності резервування). Крім того, сервісному процесору для роботи потрібні відкриті порти, що створює потенційну уразливість у системі.

Щоб побачити, що відбувається в момент помилки сервера, адміністраторові прийде перевірити сервер через локальну консоль: «KVM використовується для централізованого керування, для спільного використання клавіатури/миші/монітора, в остаточному підсумку – для економії сил/грошей/місця, а також як альтернативне підключення до клієнтських серверів». До того ж у такому «зоопарку», тобто при наявності серверів різних вендорів, погоджене використання IPMI навряд чи можливо – у цьому випадку однозначно потрібні перемикачі KVM. Крім того, за допомогою перемикачів KVM серії KN можна реєструвати все, що відбувається з підключеними серверами, – для цього потрібно окремо встановити ПЗ.

Крім обґрунтування доцільності використання KVM поряд із серверними процесорами, замовника цікавила можливість контролю й за іншим установленим у стійках устаткуванням. А саме – що додатково буде потрібно для інтеграції з послідовними консолями для забезпечення керування комутаторами, маршрутизаторами й іншим устаткуванням, не оснащеним портами KVM?

Керування послідовними консолями (комутаторами, маршрутизаторами й іншим устаткуванням без портів KVM) здійснюється декількома способами, і вибір оптимального залежить від конфігурації/розподілу відповідних пристроїв по стійках. Але можна назвати три основних способи доступу:

- over-IP-перемикач KX з модулями CIM для послідовних портів;
- сервер консолей SX з підтримкою до 48 послідовних портів;
- комбінований пристрій KSX з портами KVM і послідовними портами.

Пропонується наступний варіант – придбати консольні сервери для керування послідовними пристроями. Консольний сервер забезпечує як дистанційний, так і внутримережний доступ одночасно до 48 серверів або послідовних пристроїв (у наявності є також моделі з 1, 8, 16 і 32 портами). KVM-перемикачі серії KN оснащені портами RS232, до яких можна підключити відповідне IT-устаткування, або для підключення до KVM

консольного порту ІТ-пристрою можна скористатися модулем KA7140, що спеціально для цього призначений.

Ще один важливий момент, що замовник випустив з уваги, це перезавантаження «завислих» серверів, що KVM самі по собі не забезпечують. Для цього в сучасних моделях перемикачів передбачається інтеграція із блоками розеток (Power Distribution Union, PDU). Система пропонує й ряд додаткових можливостей, зокрема по інтеграції із системами розподілу й керування електроживленням. Управляючи інтелектуальним пристроєм розподілу електроживлення (iPDU) на рівні окремої розетки, можна примусово включати, виключати або перезавантажувати різне встаткування. Найчастіше, при збої ПЗ, перезавантаження по живленню є єдиним реальним способом повернути працездатність тому або іншому встаткуванню.

У процесі розширення інфраструктури ІТ-департамент зіштовхується з необхідністю централізованого контролю за безліччю пристроїв. При ближчому розгляді з'ясовується, що потрібно організувати не тільки моніторинг наявного встаткування, але й керування ім. Обидві завдання рідко виникають окремо одна від інший, і вирішувати їх необхідно паралельно.

Як правило, на первісному етапі найбільш актуальн і пророблені є завдання керування серверами. Для повсякденної роботи (установки сервера, настроювання ПЗ й т.п.) потрібен локальний доступ, тобто KVM-консоль, що через комутатор KVM підключають відразу до декількох серверів. Для невеликих інфраструктур така схема буде прийнятної й корисної по наступних причинах:

– KVM-консоль дозволяє працювати з усіма серверами;

– поряд з функцією локального керування й перемикання між серверами, більшість KVM мають функцію віддаленого доступу – усувати збої можна з будь-якої точки миру через Інтернет;

– для роботи з подібним устаткуванням (KVM-консолі й перемикачі) не потрібні особливі знання по його установці, настроюванню й використанню.

Проте даний підхід не позбавлений істотних недоліків:

– KVM-консолі й перемикачі можна використовувати тільки при включеному й справному сервері;

– через таке підключення не можна перезавантажити завислий сервер;

– при неприступності сервера неможливо діагностувати несправність – чи поломка це самого сервера або, наприклад, проста відсутність живлення.

Нарешті, цей підхід застосуємо тільки для серверів, а на роботу ІТ-систем прямо впливає й інше встаткування – комутатори, системи зберігання даних і т.д., які залишаються «за бортом» подібного «централізованого» керування.

Таким чином, за допомогою перемикачів KVM можна вирішувати деяке обмежене коло щоденних завдань, а також діагностувати невеликий перелік несправностей інфраструктури. Але до повноцінної системи контролю й керування це рішення «не дотягає».

У цьому зв'язку напрошується аналогія. Представимо, що ми намагаємося вирішити завдання віддаленого контролю автомобіля (читай – ІТ-інфраструктури). KVM – це робот, що може вести машину й стежити за індикацією на панелі приладів.

Але він не зможе підкачати спущене колесо або, наприклад, зрозуміти, що автомобіль не заводиться через згорілий запобіжник.

Для повноцінного рішення всього спектра завдань контролю й керування серверною інфраструктурою виробники серверів розробили так звані убудовані модулі керування (Integrated Management Module, IMM), які сьогодні є майже в будь-якому сервері. IMM є окремим міні-комп'ютером, не залежить від самого сервера й тому дозволяє вирішувати наступні завдання:

– відслідковувати стан сервера, наявні несправності, історію дій і т.п.;

– управляти сервером на рівні «заліза» – включати/виключати й перезавантажувати навіть «завислий» сервер;

– одержувати доступ, як з KVM-консолі.

І при цьому всі подібні модулі забезпечують можливість роботи через браузер, тобто підходять для 99% всіх завдань, що виникають при роботі із сервером, – хіба що комутаційні шнури самі не підключають. Але IMM не надає єдиного інструмента – це окремі пристрої для кожного сервера. І оскільки загальних стандартів на IMM ні, те й централізовано до них підключитися теж не вийде. Проте цей необхідний засіб.

Першим кроком до централізації повинна стати система моніторингу. Вибір програмних продуктів величезний – від промислових систем, наприклад HP OpenView, до продуктів з відкритим вихідним кодом начебто Zabbix або Nagios. Ці утиліти підходять не тільки для серверного встаткування, але й для будь-якого пристрою, що «уміє» інформувати про свої несправності за допомогою переривань SNMP, тобто для всієї IT-інфраструктури. При їхньому використанні адміністратор, побачивши, що сервер чомусь недоступний, уже зможе з'ясувати причину неприступності: відсутність живлення, несправність блока живлення сервера, поломка мережної карти, комутатора або системи зберігання, на якій розміщається ОС сервера, і т.п.

Повернемося до запропонованої аналогії: наш робот навчився виходити з автомобіля, перевіряти стан коліс, заглядати під капот, щоб проконтролювати рівень масла, стан запобіжників і т.п. Але для кожного вузла автомобіля (частин IT-інфраструктури: серверів, комутаторів, СЗД і т.д.) усе ще потрібні окремі ящики з інструментами.

Насправді всі ці ящики з інструментами можуть бути складені в загальне сховище – у своєрідний багажник, фізичною аналогією якого є виділена мережа керування. До неї підключаються всі IMM серверів і порти керування іншого встаткування – SAN- і Ethernet-комутаторів, СЗД і іншого встаткування. Зібрати всі ці інструменти в один загальний ящик цілком можливо, для цього існують промислові системи керування розробки BMC, HP, EMC і т.д. При інсталяції прийде багато попрацювати, зате потім життя стане набагато легше.

Ефективність використання окремих систем керування досягається лише тоді, коли за допомогою даних систем виконуються чітко певні, налагоджені комплексні процеси керування, бажано в автоматичному режимі. Для автоматизації комплексних процесів керування використовуються системи класу Orchestrator – вони дозволяють об'єднати завдання керування, виконувані окремими системами, у чіткі технологічні процеси зі строго певною послідовністю виконуваних дій.

Побудова й використання таких процесів ефективно як при рішенні стандартних рутинних завдань технічної підтримки, коли потрібно виявити несправність і відновити компоненти IT-інфраструктури, так і при автоматизації критичних для бізнесу завдань, де неприйнятні затримки й помилки ручного керування. Такий підхід дозволяє використовувати готові, що найбільше часто зустрічаються процеси керування – наприклад, рекомендації ITIL або класичні завдання адміністрування. Крім того, система автоматизації комплексних процесів керування дозволяє розробляти власні процеси й інтегрувати в них широкий набір IT-систем.

Головний вивід, якому можна зробити з нашої спроби змоделювати завдання заміни застарілих KVM у досить великої серверної, полягає в тім, що при поточній розмаїтості засобів віддаленого доступу, до яких ставляться фізичні (KVM-перемикачі) і програмні (RDP, VNC, SSH, Telnet) інструменти, а також різні сервісні процесори (IPMI, iLO, DRAC), потрібна система централізованого контролю, що підтримувала б всі перераховані інструменти й дозволяла управляти як фізичними, так і віртуальними ресурсами.

За допомогою традиційних систем KVM системний адміністратор може управляти встаткуванням, що перебуває на відстані до 300 м. Технологія KVM over IP (IP KVM) забезпечує доступ до клавіатури, монітору й миші комп'ютера з будь-якого місця через локальну, глобальну мережу або Інтернет. У результаті стали доступними керування й діагностика серверів і мережних пристроїв на віддалених площадках, у тому числі керування серверами на рівні BIOS (навіть при відмові системи), інсталяція ПЗ за допомогою емуляції

CD-ROM (функція Virtual Media), відключення й включення живлення серверів за допомогою блоку керованих розеток.

Рисунок 1 – Структурна схема системи

Завдяки цьому при обмеженому бюджеті й невеликому штаті фахівців вдається відстежити стан віддалених комп'ютерів, швидко усунути неполадки, а крім того, скоротити загальну вартість володіння (TCO). Virtual Media дозволяє імітувати на підключеному комп'ютері зовнішній диск (наприклад, привод DVD/CD, пристрій зберігання USB, накопичувачі на жорстких дисках і образи ISO), що дає можливість установлювати операційну систему, інсталювати й обновляти програмне забезпечення, запускати діагностичні тести й т.п. відразу на декількох комп'ютерах.

Використовуючи встаткування KVM, можна перемикатися між керованими системами, не витрачаючи часу на переміщення, заощадити на придбанні моніторів, ефективніше використовувати простір на робочому столі, визволити місце в ЦОД, знизити вимоги до тепловідводу й електроживлення, підвищити ефективність керування. Технологія KVM добре вписала в тенденцію централізації адміністрування інфраструктури у великих і розподілених компаніях.

Єдиний інтерфейс IP KVM надає системним адміністраторам широкі можливості керування розподіленою інфраструктурою IT, які практично не уступають локальним методам, хоча через обмеженість пропускної здатності каналів у таких рішеннях звичайно застосовуються програмне й/або апаратний стиск потоку даних, що знижує якість відео. До того ж для роботи IP KVM потрібна функціонуюча мережа, адже несправність шлюзу або помилкова конфігурація мережного встаткування можуть утруднити доступ ззовні.

Підтримка додаткового каналу зв'язку (наприклад, модемного з'єднання) дозволяє управляти віддаленим пристроєм навіть при відмові мережі. При керуванні по додатковому каналі (Out-of-Band) – через провідні або бездротові модеми – сигнали передаються з невисокою якістю, але цього досить для аварійного доступу до віддаленого комп'ютера.

Перемикачі IP KVM, що становлять зараз більше половини світового ринку KVM, істотно розрізняються по функціональності й класу – випускаються як прості й економічні рішення для SMB/SOHO, так і системи корпоративного рівня з більше широким

функціоналом і потужні каскадуємі рішення, що дозволяють управляти тисячами серверів у ЦОД.

IP KVM відрізняються від традиційних KVM своєю функціональністю, рівнем безпеки, підтримуваним якістю відео, інтерфейсами, методами доступу (мідні й оптичні лінії, резервування за допомогою модемного з'єднання), числом керованих пристроїв, користувачів і консолей. Та й вартість цих пристроїв вище. Для рішення локальних завдань керування IP KVM – дорогий й менш зручний варіант. При необхідності ж віддаленого доступу через KVM, рішення на базі IP буде гарним вибором, незважаючи на неминучий компроміс у питаннях якості сигналу, зручності роботи, безпеки й т.п. У деяких ситуаціях можна застосовувати пристрою обох типів, з вигодою сполучаючи переваги високої якості відео й безпека подовжувачів KVM з універсальністю/ масштабованістю IP KVM.

Надійний доступ до найважливіших ресурсів IT залишається ключовою характеристикою платформи IP KVM. Обиране рішення повинне забезпечувати оперативний доступ до керованого встаткування з будь-якої точки локальної або глобальної мережі й при цьому бути сумісним з використовуваними в компанії операційними системами, серверними платформами й мережними пристроями. Крім того, необхідно, щоб кількість портів відповідала числу комп'ютерів або серверів в організації, а рішення мало необхідну масштабованість. Важливими параметрами є максимальний дозвіл відео, алгоритми стиску відеосигналу для зниження вимог до пропускної здатності, конструктивні особливості, максимальне число одночасних сеансів. Інтеграція IP KVM з Intelligent Platform Management Interface (IPMI) дозволяє додати різні функції IPMI, наприклад віддалене керування блоками живлення сервера й моніторинг його стану.

Деякі моделі IP KVM мають порти для підключення пристроїв керування електроживленням, с допомогою яких можна не тільки включати й виключати живлення, але й програмувати режим включення/відключення за графіком. Перемикачі KVM у комбінації з інтелектуальними пристроями розподілу й керування електроживленням (Power Distribution Unit, PDU) розширюють можливості керування аж до окремої розетки. Інтерфейс інтелектуального керування платформами IPM дозволяє збирати інформацію з датчиків про температуру/вологість, швидкості обертання вентиляторів, споживану потужність або напругу в електромережі. Керуючись цими даними, можна віддаленно включати й виключати встаткування й перезапускати систему. Керування PDU здійснюється через захищені з'єднання (наприклад, Telnet, SSH або SNMP). Адміністратор може запрограмувати систему на автоматичне відключення некритичних серверів при аварії в електромережі або знеструмлювати розетки, у яких енергоспоживання виходить за встановлене граничне значення.

Доступ з будь-якого місця відкриває нові можливості використання KVM, однак ускладнює завдання забезпечення інформаційної безпеки при централізованому керуванні інфраструктурою IT, адже IP KVM надає поглиблений контроль розподілених ресурсів і може стати "слабкою ланкою" у системі ІБ. Разом з тим IP KVM дозволяє протоколювати всі дії, передбачає розвинені засоби шифрування й контролю доступу. Крім того, рівень фізичної безпеки можна значно підвищити, розмістивши сервери в закритих приміщеннях або в захищених ЦОД, що обслуговуються дистанційно, без присутності персоналу на об'єкті.

У сучасних рішеннях застосовуються різні підходи до безпеки. У перемикачі KVM може, наприклад, підтримуватися прийнята в компанії технологія (або власні методи) перевірки дійсності. Інтерфейс адміністрування із шифруванням всіх сигналів між KVM і керованими пристроями у відповідності зі стандартами AES, DES, 3DES або 128-розрядним SSL не дозволить перехопити сигнал від віддаленого комп'ютера й побачити зображення на моніторі.

IP KVM часто підтримують централізовану багатоступінчасту автентифікацію з однократною реєстрацією на основі LDAP і Active Directory, тим самим надаючи можливість для використання звичних методів автентифікації без створення нових облікових записів.

Іноді для протидії потенційним погрозам передбачається автоматичне відправлення повідомлень про невдалу спробу автентифікації.

Основні переваги розробленої системи:

– керування через IP;

– інтегрована підтримка послідовного інтерфейсу (serial devices), можливість організації доступу в термінальному режимі до мережного й будь-якого іншого аналогічного встаткування;

– віддалене перезавантаження живлення підключеного встаткування (с допомогою додаткової опції Power Management);

– високорозвинене програмне забезпечення з убудованими функціями адміністрування й безпеки, інтеграція з LDAP, AD, RADIUS, NT Domain, TACACS;

– звичний Web інтерфейс користувача;

– убудована можливість модернізації ПЗ KVM-перемикача по мережі;

– підключення пристроїв кабелем 5-й категорії, використання технології інтелектуального кабельного інтерфейсу (Smart Cable Interface), що дозволяє значно скоротити кількість необхідного кабелю;

– легкість масштабування;

– підтримка різних серверних платформ;

– функція Virtual Media – можливість передачі файлів на віддалений сервер і завантаження з віддаленого носія.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів віддаленого адміністрування серверами за допомогою KVM-over-IP-перемикачів.

Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем віддаленого адміністрування серверами за допомогою KVM-over-IP-перемикачів.

– Досліджена система віддаленого адміністрування серверами за допомогою KVM-over-IP-перемикачів.

– На основі отриманих результатів досліджень створена програмна реалізація системи віддаленого адміністрування серверами за допомогою KVM-over-IP-перемикачів.

Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання віддаленого адміністрування серверами за допомогою KVM-over-IP-перемикачів. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». Advanced Information Systems, 2023, 7(2), pp. 49-56.
2. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchev, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». CEUR Workshop Proceedings, Volume 3530, 2023, pp. 256-265.
3. Smirnov, O., Odarchenko, R., Smirnova, T., Bondar, S., Volosheniuk, D. «Optimal Structure Construction of Private 5G Network for the Needs of Enterprises». Lecture Notes on Data Engineering and Communications Technologies, 2023, 178, pp. 208–223.
4. Smirnova, T., Gnatyuk, S., Yudin, O., Sydorenko, V., Polozhentsev, A., «The Model for Calculating the Quantitative Criteria for Assessing the Security Level of Information and Telecommunication Systems». CEUR Workshop Proceedings Volume 3156, 2022, Pages 390-399.
5. Smirnova T., Gnatyuk S., Berdibayev R., Avkurova Zh., Iavich M. «Cloud-Based Cyber Incidents Response System and Software Tools». Communications in Computer and Information Science, 2021, vol 1486. Springer, Cham. pp 169-184.
6. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.

7. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». Journal of theoretical and applied information technology Vol.98. No 21, 2020, P. 3334-3346.
8. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 172-177.
9. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. 2021. pp 557-587.
10. Smirnov, O., Markovets, O. Vovk, N., Turchyn, Y., «Model of informational support for social network administrators' content creation». CEUR Workshop Proceedings Volume 2616, 2020, Pages 125-136.
11. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». CEUR Workshop Proceedings Volume 2616, 2020, Pages 366-379.
12. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645.
13. Smirnov O. Kuznetsov A., Zaicenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties». International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019; Odessa; Ukraine; 9-13 September 2019. P.22-28.
14. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407.
15. Smirnov, O., Kuznetsov, A., Reshetniak, O., Ivko, N., Katkova, T., Kuznetsova, T., «Generators of Pseudorandom Sequence with Multilevel Function of Correlation». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019 . P.517-522.
16. Smirnov, O., Odarchenko, R., Abakumova, A., Usik, P., Kundyz, M., «QoE optimization technique for media delivery in 5G networks». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019. P.597-601.
17. Smirnov, O., Krasnobayev, V., Yanko, A., Kuznetsova, T. «Methods of nulling numbers in the system of residual classes». CEUR Workshop Proceedings, Vol 2588, P. 90-106, 2019.
18. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Averchev, A., Pastukhov, M., Kuznetsova, K., «Formation of Pseudorandom Sequences with Special Correlation Properties», 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT -2019/ Lviv, Ukraine, 2-6 July, 2019, P. 395-399.
19. Smirnov, O., Kuznetsov, A., Kiian, A., Zamula, A., Rudenko, S., Hryhorenko, V., «Variance Analysis of Networks Traffic for Intrusion Detection in Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 353-358.
20. Smirnov, O., Kuznetsov, A., Kavun, S., Babenko, B., Nakisko, O., Kuznetsova, K., «Malware Correlation Monitoring in Computer Networks of Promising Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 347-352.
21. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Pastukhov, M., Kuznetsova, K., Prokopovych-Tkachenko, D., «Discrete Signals with Special Correlation Properties», CEUR Workshop Proceedings Volume 2353, CEUR Workshop Proceedings 2019, Pages 618-629.