УДК 336.72

КОНЦЕПЦІЯ УПРАВЛІННЯ ТА РОЗМЕЖУВАННЯ ДОСТУПУ ДО ІНФОРМАЦІЙНО-ТЕХНІЧНИХ РЕСУРСІВ У СУЧАСНІЙ ІТ-ІНФРАСТРУКТУРІ

Жованик М.О.
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

У статті розглянуто архітектура управління доступом до інформаційних ресурсів у сучасній розподіленій ІТ-інфраструктурі. Наведено базові механізми захисту та управління, що використовуються при розмежуванні доступу в мережі та дозволяють попередити втрату інформації. Визначено поняття менеджменту доступу. Вказано переваги цієї концепції та подальших методик управління доступом. Описано основні принципи введення їх у реальне корпоративне середовище.
Ключові слова: політика безпеки, впровадження, розподілена інфраструктура, менеджмент доступу, протокол віддаленого управління, модель доступу.

Постановка проблеми. При плануванні та побудови сучасної розподіленої ІТ-інфраструктури дуже важливо правильно розробити архітектуру розподілення доступу. В наш час кожен працівник має своє робоче місце, яке є комп'ютеризоване. При правильній організації кожна інфраструктура ділиться на окремі відділи, зони. В кожному відділі працюють окремі працівники. Кожний працівник виконує різні функції і для коректного виконання завдань вони використовують різного типу ресурси. В такому випадку не раціонально зі сторони інформаційної безпеки надавати доступ кожному працівнику до всіх інформаційних ресурсів. Тому потрібно розподілити доступ по працівникам, по відділам і назначити кожній трудовій одиниці окремі доступи. На такому етапі вступає в гру такий сегмент захисту інформації як розмежування доступу. Крім правильного розмежування доступом, потрібно добре спланувати механізм ідентифікації кожної трудової одиниці.

Аналіз останніх досліджень та публікацій. На сьогоднішній день розвиток інформаційної безпеки корпоративного середовища є невід'ємною частиною розвитку бізнес-процесів. Розвиток інформаційних технологій росте з геометричною прогресією. Тому на даний момент обслуговування кожної інфраструктури не обходиться без планування архітектури захисту важливий інформаційних та технічних ресурсів. В наш час ринок кіберзлочинності приносить дохід в 1,5 рази більший, ніж продаж наркотиків. Тому потрібно задуматись, що вигідніше та простіше реалізувати – продаж наркотиків чи хакерські атаки.

Як показали останні тенденції, більшість хакерських атак, що були проведені – це були APT-атаки. Тобто, атаки, які готуються і проводяться за великий проміжок часу. Одна з найбільших атак в Україні була атака Black Energy. Рік почався з кібератаки BlackEnergy на підприємства енергетичного сектора України. Атака стала унікальною за масштабами заподіяної шкоди: хакерам вдалося відключити системи розподілу електроенергії на Західній Україні, запустити в атаковані системи програму Wiper для видалення вмісту заражених комп'ютерів і провести телефонну DDoS-атаку на служби техпідтримки атакованих компаній [1]. Програма BlackEnergy є вкрай динамічною загрозою, і недавні атаки на Україну показали, що її основні цілі – це руйнівні дії і промислове шпигунство, крім того вона прагне скомпрометувати системи промислового управління.

Positive Technologies представила статистику атак на веб-додатки в 2016р, зібрану за результатами проведення пілотних проектів впровадження брандмауера PT Application Firewall. Як розповіли CNews в компанії, особлива увага приділена тому, як зловмисники атакують організації зі сфери інформаційної безпеки – ці тенденції розглядаються на прикладі власних ресурсів Positive Technologies [2].

Найчастіше зловмисники, які атакували вебресурси компанії, намагалися обійти засоби захисту для несанкціонованого доступу до інтерфейсу CMS. При цьому, найчастіше атакуючі не знають, яка CMS використовується на конкретному сайті, і діють навмання – намагаються обійти форму аутентифікації, яка може бути розташована за різними адресами в залежності від CMS.

Близько половини від загального числа атак на ресурси Positive Technologies (45%) припадає на частку атак «Впровадження операторів SQL», що приблизно відповідає показнику для IT-галузі, отриманого в ході пілотних проектів. Чверть від загального числа склали атаки «Підробка міжсайтових запитів», а п'яту частину – «Неконтрольоване перенаправлення». 5% і менше складають такі атаки, як «міжсайтовий виконання сценаріїв», «Відмова в обслуговуванні» і «Віддалене виконання коду і команд ОС». Інші атаки в сумі набирають 1%.

Основні джерела атак – Росія (43% атак) і Україна (20% атак). Третє місце займає Великобританія – Сполучене Королівство є джерелом 17% атак. Це пояснюється, з одного боку, присутністю Positive Technologies на європейському ринку ІБ, а з іншого – використанням проксісерверів провайдерів, зареєстрованих на території Королівства. По 6% атак зафіксовано з боку США і Туреччини [2].

Інший цікавий факт – збільшилася частка атак з боку України (40% від загального числа) і Туреччини (12%); активність зловмисників з інших країн, в тому числі Росії, коливалася незначно. Ці факти співвідносяться з попередженнями Федеральної служби безпеки про підготовлювані кібератаки на фінансову систему Росії [2].

Згідно даним дослідженням, такий сектор контролю як менеджмент доступу відіграє не маленьку роль в загальній системі безпеки інформаційних ресурсів. При правильній побудові архітектури системи управління доступом можна знизити ризики проникнення та конфронтації системи безпеки. Правильне управління доступом не забезпечить повністю захищену систему, так як згідно формальному закону – «жодна система не є повністю захищеною», але такий підхід дозволить мінімізувати ризик проникнення несанкціонованого користувача та вбереже від внутрішніх загроз в обличчі не досвідчених користувачів.

Мета статті. Головною метою цієї роботи є дослідження основних принципів захисту та управління доступом до критичних інформаційних ресурсів в корпоративній мережі. Переваги та недоліки впровадження та застосування запропонованої архітектури управління доступом для запобігання витоку корпоративної інформації та захисту від зовнішніх загроз.

Виділення невирішених раніше частин загальної проблеми. Кожну IT-інфраструктуру можна розділити на дві частини – трудові ресурси (штатні працівники, обслуговуючий персонал, інженери і т.д.) та інформаційно-технічні ресурси (безпосередньо різного роду корпоративна інформація, програмне забезпечення, робочі станції користувачів, сервери обслуговування та інше). Відповідно до такого розподілу постає питання побудови системи розмежування доступом та в подальшому управління ними. В багатьох випадках це робиться за допомогою прав доступу. Та в більшості випадків цього не достатньо. Кожен працівник виконує перший перелік функцій і для виконання їх потрібно певний перелік технічний ресурсів. За допомогою розмежування та присвоєння прав на той чи інший ресурс, не завжди можна досягти бажаного результату в даному сегменті захисту та управління інформацією. Тому на такий випадок пропонується інша концепція управління доступом, яка в свою чергу включає надання прав доступу, але крім цього вона включає в себе перелік інших критично важливих функцій.

Виклад основного матеріалу. Для забезпечення виконання політик безпеки стосовно ідентифікації та відповідно розмежування доступом пропонується модель управління цим процесом.

Категоризація трудових та інформаційних ресурсів. Згідно цієї моделі управління доступом відбувається по запропонованому принципу. Кожна інфраструктура має свій набір трудових ресурсів. Але будь-який перелік таких ресурсів можна розподілити на певні групи. В цілому це групи – адміністраторів, цільових користувачів, обслуговуючий персонал, фінанси, інженери різних категорій та технологій, адміністратори безпеки, зовнішні користувачі, аудитори та інші специфічні групи користувачів [3].

Крім поділу на категорії та групи користувачів, відбувається поділ на окремі підгрупи інформаційних ресурсів. Тобто, наприклад інформація по внутрішніх користувачів, база даних фінансової документації, інформація по зовнішніх клієнтів, тестові ресурси, внутрішня документація, технічні ресурси (різного роду програмне забезпечення), окремі серверні та операційні ресурси. Кожна група користувачів відповідає за певні функції, для виконання яких їм потрібні допоміжні інформаційні ресурси. Відповідно до кожної групи трудових ресурсів надається відповідні інформаційні ресурси. Тобто, кожній групі користувачів виділяються відповідні інформаційно-технічні ресурси. Доступ до інших ресурсів, не потрібних для виконання своїх функцій, закривається. Даний розподіл врегульовується внутрішньою політикою безпеки [3].

При організації доступу використаємо таку схему. Перший крок – це проведення процедури створення єдиної точки доступу до інформаційно-технічний ресурсів. Це означає використання єдиної консоль входу та доступу до будь-яких інформаційних ресурсів. Без використання цієї точки входу, не можна буде отримати підключення до якихось інформаційних ресурсів. Тобто, виключається можливість отримання доступу за допомогою інших способів комунікації до інформаційно-технічних ресурсів. Це мінімізує ризик отримання доступу до ресурсів не авторизованим користувачам, що в свою чергу зменшить

ризик компрометації системи захисту в цілому. Крім єдиної точки входу дана система управління доступом передбачає дві функції, що будуть відповідати за такі можливості системи, як збереження інформації про користувачів, дотримання політик розмежування доступом та технічна організація каналів зв'язку для всіх авторизованих користувачів [4].

Доступ до інформаційних ресурсів можливий лише через консоль входу. Кожний користувач для отримання доступу повинен пройти авторизацію в консолі входу. Для авторизації використовується механізм двух-факторної авторизації. Перший етап авторизації – це обліковий запис, що складається з логіну і паролю користувача. На пароль відповідно до даної схеми, накладається певні умови – більше 8 символів, обов'язкове використання спеціальних символів, великих, маленьких букв, зміна паролю кожні 60 днів. Далі відповідно до введених облікових даних, відбувається авторизація з допомогою доменного контролеру Active Directory [4]. Після проходження даного етапу авторизації користувачеві потрібно пройти другий етап авторизації за допомогою Radius-серверу. Цей етап включає введення унікального для кожного користувача ключа, що передається на Radius-сервер для проходження другого етапу авторизації. Далі облікові дані перевіряються на цьому сервері і якщо сервер присилає відповідь – Successful, то користувач отримує доступ до своїх ресурсів.

Адміністратор безпеки, який має права – Full Control, має список всіх доступних ресурсів. Для кожного користувача відображається в списку лише той список ресурсів, до яких він має доступ по політиці безпеки.

За даною моделлю підключення до ресурсів відбувається за допомогою технології «віддаленого управління робочим столом». Дана технологія передбачає віддалене підключення до інформаційних ресурсів за допомогою основних протоколів віддаленого підключення – RDP та SSH. Дана модель передбачає не лише підтримку протоколів RDP та SSH, а також підтримку протоколів віддаленого підключення до інших операційних систем [5].

Типова схема роботи даної моделі виглядає наступним чином:

1. Користувач проходить процедури ідентифікації/аутентифікації на точці єдиного входу, створює запит на з'єднання з потрібним ресурсом.

2. Після узгодження запиту на з'єднання модуль, що відповідає за канал зв'язку отримує дані для підтвердження аутентифікації.

3. Після аутентифікації проходить процес з'єднання користувача безпосередньо з обраними ресурсами за допомогою деякого визначеного протоколу.

4. Під час сесії користувача ведеться безперервна запис дій, виконуваних на керованих пристроях. Запис ведеться в відео-форматі (для графічних сеансів) і в текстовому форматі (для сеансів командного рядка). Записи зберігаються в деякому сховищі даних і доступні аудиторам і фахівцям з інформаційної безпеки для перегляду та аналізу.

5. Можлива відправка подій безпеки в системи моніторингу.

Окремою функціональною можливістю даної моделі є адаптивне управління доступом. Дана можливість включає в себе підтримку не лише віддаленого підключення до операційних систем, а й управління доступом до різних додатків. Це означає, що можна встановлювати політики розмежування доступом до різного роду додатків, таких як наприклад офісного програмного забезпечення (Word, Excel, Power Point та інше), клієнтів управління різного роду базами даних (SQL Management Studio, PLSQL for Oracle та багато інших). Основна і головна перевага адаптивності в даній моделі є те, що вона передбачає організацію доступу до нових додатків, ОС та інших процесів, що не передбачені в загальній політиці безпеки. Можна контролювати доступ до кожних нових ресурсів та нових клієнтів за допомогою яких здійснюється цей доступ. Дана можливість реалізується створенням нових підключень до нових додатків та ресурсів. Це реалізується за допомогою, того що кожне підключення до інформаційних ресурсів здійснюється на базі визначеного протоколу підключення. З'єднання по своїй суті це процес, який здійснює підключення до ресурсів. Цей процес проводить спробу запуску додатку до якого він здійснює доступ. Це можливо, так як кожний додаток має свій файл виконання і в цей процес можна з інтегрувати будь який новий файл і таким чином отримати доступ до нових або не підтримуваних додатків. Результатом цього є адаптація до нових чи не підтримуваних додатків за допомогою яких відбувається доступ до ресурсів [6].

Модель контролю доступу поєднує в собі багато функціональних можливостей та являється єдиною точкою доступу-входу до ресурсів IT-інфраструктури. Також являє собою комплекс механізмів контролю, організованих у сукупність механізмів управління повним «життєвим циклом» будь-яких облікових даних. Даний комплекс механізмів призначений для керування обліковими даними до будь-яких інформаційно-технічних ресурсів і дозволяє забезпечити надання доступу до критично важливої інформації, управління обліковими даними і контролювати активність користувачів. Дана модель передбачає та реалізує комплекс механізмів управління доступом, що в свою чергу виступають як єдина система [6]:

· Реєстрація дій адміністраторів під час їх віддаленого підключення до критичних систем та ресурсів;

· Чітка ідентифікація адміністраторів, включаючи тих, що використовують загальні облікові записи;

· Надання механізмів розслідування по фактам виходу зі строю або втручання в роботу критичних ресурсів;

· Управління автентифікацією додатків та розмежування доступу між додатками;

· Повний та постійний моніторинг користувацької активності;

· Ізоляція активів та ресурсів.

Всі ці механізми входять в єдину архітектуру управління та розмежування доступу та працюють як єдине ціле. В основу даної моделі входить принцип, що один механізм без іншого працювати не буде. Кожний окремий механізм взаємопов'язаний з іншими.

Реєстрація дій користувачів. Даний механізм реалізує потужний функціонал моніторингу облікових записів. Кожна віддалена сесія записується в відео форматі та зберігається в спеціалізованому сховищі. Даний механізм використовується для аудиторського контролю та для розслідування інцидентів безпеки. Передбачається запис всіх введених консольних команд в текстовому форматі з ціллю реєстрації всіх дій користувачів. При відтворенні записаних сесій передбачається механізм швидкого пошуку по запису. Даний механізм дозволяє здійснювати пошук дій по введених команд, наприклад ping, ifconfig, cmd.exe, sudo su і таке інше [7].

Чітка ідентифікація адміністраторів та користувачів. Кожний користувач, адміністратор або інша трудова одиниця має обліковий запис в Active Directory. За допомогою цього облікового запису даний користувач виконує всі дії та функції в IT-інфраструктурі. Дана модель розмежування та управління доступом передбачає, що авторизація та ідентифікація при спробі отримання доступу в консолі входу здійснюється за допомогою цього облікового запису. Таким чином, мінімізується процес обману чи виконання дій під іншим обліковим записом. Всі дії, що здійсненні з під певного облікового запису будуть реєструватись та фіксуватись з під якого користувача чи облікового запису виконано ті чи інші дії.

Повний контроль доступу та ізоляція активів. Даний підхід забезпечує повну ізоляцію ресурсів, тим що не авторизований користувач чи користувач, що не має відповідного доступу не зможе отримати чи підключитись до тих чи інших інформаційних ресурсів. Дана модель передбачає строгий розподіл ресурсів для кожного користувача та за допомогою «парольних політик» повний контроль за виконанням розмежування доступу [7].

Управління та надання привілегій. Кожному користувачеві доступ до ресурсів надається на основі політик. В політиці вказується список ресурсів, які дозволяються для доступу тому чи іншому користувачеві. Вказується режим запису та подальше відтворення сесії.

Повний та постійний моніторинг користувацької активності та механізми розслідування інцидентів. Кожна сесія будь-якого користувача записується як у відео форматі, так і в текстовому форматі. Для кожної записаної сесії передбачається механізм пошуку, той чи іншої події, введеної команди чи внесених змін. Для сесій також передбачено потужний механізм постійного моніторингу користувацької активності – моніторинг користувацьких сесій в режимі реального часу. Це означає, що є можливість контролю та аудиту користувацьких сесій навіть протягом того, коли користувач чи інша трудова одиниця працює. Такий підхід разом з механізмом протидії в режимі онлайн надає оперативну можливість протидіяти злоякісним навмисним чи ненавмисним діям різних категорій користувачів.

Рис. 1. Функціональна модель управління доступом

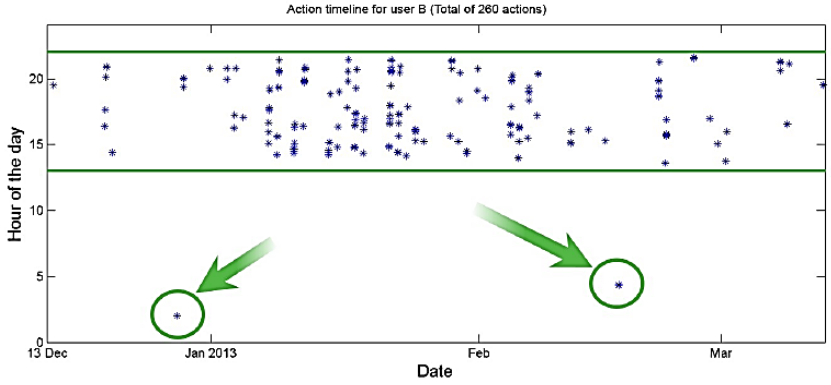

Рис. 2. Поведінковий аналіз дій користувача

Автентифікація додатків. Механізм для управління додатків та скріптів, мандати і ключі шифрування, призначена для організації взаємодії між інформаційної системами. Цей механізм виключає необхідність зберігання реквізитів в додатках, скриптах і файлах конфігурація, і дозволяє зберігати, управляти і проводити аудит дій з вкрай «чутливим» паролями [7].

Окремим розділом в даній моделі є механізм моніторингу та протидії за діями користувача в режимі онлайн. Цей механізм виділено в окремий параграф, бо функціональність даного механізму відрізняється від звичайного. Цей механізм реалізовує забезпечення цілеспрямованих, швидко здійсненних оповіщень про загрози шляхом виявлення аномалій в діях привілейованого користувача і облікової діяльності. Реагування здійснюється на основі зібраних даних з різних джерел по всій IT-інфраструктурі. Цей механізм співпрацює з загальними

механізмами моніторингу, збирає сам дані. З цим багатим і цільовим набором даних, може швидко визначити аномальні заходи, які можуть вказувати на атаку. В результаті команди реагування на інциденти можуть категоризувати пріоритети, які пов'язані з привілейованими обліковими записами, що дозволить їм зупинити руйнівні атаки, перш ніж вони стануться.

Даний механізм працює на основі певних вироблених шаблонів поведінки кожного користувача та алгоритмів машинного навчання, для аналізу та корекції поведінкової бази користувачів. Наприклад, на малюнку показано як відбувається виявлення аномальних дій, що пов'язані з отриманням доступу користувачів:

Згідно з цим прикладом, користувач В протягом 3 місяців здійснював спроби отримати доступ до ресурсів в другій половині дня. Але було два аномальних випадку, коли даний облікових запис здійснив спроби доступу в першій половині дня. Дані аномалії мають середній пріоритет і сповіщають адміністраторів безпеки, що дана активність є небезпечною і не нормальною.

Даний механізм дозволяє нам досягти таких результатів:

· Радикально скоротити час виявлення атаки зловмисника і зменшити шкоду, зосередивши виявлення загроз на привілейовані облікові записи;

· Швидко виявлення атак з аналітикою на основі вбудованих алгоритмів, що постійно оновлюються і пристосовуються до нових атак;

· Спрощення отримання та дослідження інформації про інциденти безпеки, що пов'язані чи були здійснені з допомогою облікових записів користувачів.

Схема роботи – користувач проходить авторизацію та отримує доступ до певних ресурсів. Паралельно окремий модуль співпрацюючи з іншими джерелами інформації в мережі, збирає інформацію та створює поведінкову фігуру для кожного користувача. Після встановлення сесії відбувається моніторинг в реальному часі всіх дій, що здійснює користувач. Аналіз дій відбувається відповідно до поведінкових шаблонів та встановлених політик, та паралельно алгоритми машинного навчання аналізують дані в мережі та будуть новий шаблон чи визначають зловмисні дії цього користувача. Наприклад, користувач, що відповідає за генерування звітів по кількості випитої кави в офісі, починає сканувати мережу (наприклад, arp -a, ping і так далі), то система видасть адміністраторам безпеки повідомлення про ці дії, назве обліковий запис, час, джерело та іншу допоміжну інформацію.

Висновок і пропозиції. В загальному, можна зробити висновок, що при сучасному розвитку інформаційних технологій та широким спектром використання інформаційних та технічних ресурсів, дане рішення надає широкий пакет можливостей по управлінню та розмежування доступом, що використовується у корпоративній діяльності. Зокрема, вони дозволяють керувати доступом до різного роду пристроїв, синхронізувати передачу та отримання даних, обмежити доступ до інформації, функцій та додатків, а також передбачають використання політик та завдань, що дозволяє не виконувати щоразу рутинну роботу для налаштування кожного пристрою окремо. Але з іншого боку, перш ніж почати впровадження даної концепції в корпоративну мережу, треба чітко зрозуміти від яких нових загроз доведеться захищатися та оцінити чи не буде впровадження цих технологій для захисту інформаційних ресурсів коштувати дорожче власне самих ресурсів. Це одне із головних питань при прийнятті рішення про впровадження даної моделі керування доступом в корпоративну мережу. Тому на даний час, дана концепція – це досить молоде рішення, дослідження в даній галузі будуть актуальні ще не одне десятиліття. Вирішення питання менеджменту доступу буде знаходитись на одному рівні з темпами виникнення нових технологій. В загальному, це просте та ефективне рішення, що стосуються питань доступу та управління безпекою інформаційних ресурсів в корпоративній мережі, що будуть актуальні ще не один рік.

Список літератури:

1. Kaspersky Security Bulletin 2016. Развитие угроз и статистика [Електронний ресурс] – Режим доступу: https://securelist.ru/analysis/ksb/29828/kaspersky-security-bulletin-2016-review/
2. Статистика атак на веб-приложения в 2016 году [Електронний ресурс] – Режим доступу: http://safe.cnews.ru/news/line/2017-01-30_positive_technologies_opublikovala_statistiku
3. Классификация информационных ресурсов [Електронний ресурс] – Режим доступу: http://be5.biz/pravo/iyno/04.htm
4. Системы управления доступом к информационным ресурсам [Електронний ресурс] – Режим доступу: http://www.author.kiev.ua/resheniya/sistemy-upravleniya-dostupom.html
5. Технологии построения эффективной системы управления доступом к информационным ресурсам [Електронний ресурс] – Режим доступу: https://cctv-pro.com.ua/article/6132/tehnologii-postroeniya-effektivnoy-sistemy-upravleniya-dostupom-k-informacionnym-resursam/
6. Управление доступом к информационным ресурсам [Електронний ресурс] – Режим доступу: http://window.edu.ru/catalog/pdf2txt/758/72758/50485
7. Управление доступом к корпоративной сети [Електронний ресурс] – Режим доступу: http://cisco-lan.ru/network_and_information_security/controlling_access_to_information_resources_on_the_corporate_network.php

Жованик М.А.
Национальный технический университет Украины
«Киевский политехнический институт имени Игоря Сикорского»

КОНЦЕПЦИЯ УПРАВЛЕНИЯ И РАЗГРАНИЧЕНИЯ ДОСТУПА К ИНФОРМАЦИОННО-ТЕХНИЧЕСКИМ РЕСУРСАМ В СОВРЕМЕННОЙ ИТ-ИНФРАСТРУКТУРЕ

Аннотация
В статье рассмотрены архитектура и модель управления доступом к информационным ресурсам у современной распределенной ИТ-инфраструктуре. Приведены базовые механизмы защиты и управления, которые используются при разграничении доступа в сети, позволяющие предупредить потерю информации. Определено понятие менеджмента доступа. Указано преимущества этой концепции и дальнейших методик управления доступом. Описаны основные принципы введения их в реальную корпоративную среду.
Ключевые слова: политика безопасности, внедрение, распределенная инфраструктура, менеджмент доступа, протокол удаленного управления, модель доступа.

Zhovanik M.O.
National Technical University of Ukraine
«Kyiv Igor Sikorsky Polytechnic Institute»

THE CONCEPT OF INFORMATION TECHNOLOGY RESOURCES ACCESS CONTROL AND ISOLATION IN THE MODERN IT INFRASTRUCTURE

Summary
The article examines the architecture and model of access control to information resources in a modern distributed IT infrastructure. Basic protection and control mechanisms are provided, which are used to differentiate access to the network, thus preventing the loss of information. The concept of access management is defined. The advantages of this concept and the further methods of access control are indicated. The main principles of introducing them into the real corporate environment are described.
Keywords: security policy, implementation, distributed infrastructure, access management, remote control protocol, access model.