УДК 004.056 **Ю.В. Борсуковський**

ВИЗНАЧЕННЯ СУЧАСНИХ ВИМОГ ДО СТВОРЕННЯ ПОЛІТИКИ УПРАВЛІННЯ ДОСТУПОМ КОРПОРАТИВНИХ КОРИСТУВАЧІВ

В даній статті проведено детальний аналіз вимог до створення політики управління доступом корпоративних користувачів. Сформульовані базові вимоги та рекомендації щодо структури та змісту політики управління доступом корпоративних користувачів з врахуванням останніх інцидентів в області кібербезпеки.

Ключові слова: доступ, політика, стандарти, кібербезпека

Вступ і постановка задачі

Управління доступом до корпоративних інформаційних ресурсів є ключовою функцією забезпечення інформаційної безпеки [3,4,5]. Дана процедура в тому чи іншому вигляді постійно вирішується в кожній інформаційній системі державного та корпоративного сектору.

Завдяки процесу зіставлення облікових записів користувачів і членства в групах з правами, привілеями та дозволами, з ними пов'язаними, операційна система забезпечує захист файлів, додатків та інших ресурсів від несанкціонованого використання [1].

У корпоративної мережі кожної організації зберігається і обробляється інформація з обмеженим доступом, яка є життєво важливою для ведення бізнесу, інформація, яка відноситься законодавством України до комерційної та службової таємниці, персональні дані співробітників та ін.

З метою забезпечення захисту інформаційних ресурсів від їх незаконного використання, розробляється політика доступу до інформаційних ресурсів і встановлюється єдиний для всіх користувачів порядок надання, зміни та скасування доступу до корпоративних IT-ресурсів у відповідності до встановлених вимог безпеки і є обов'язковим для виконання всіма без виключення користувачами.

Управління доступом до корпоративних IT-ресурсів передбачає порядок визначення та зміни прав на використання:

- об'єктів доступу (інформаційні системи, об'єкти IT-інфраструктури, бази даних та інші активи);
- суб'єктів доступу (облікові записи в інформаційних системах, облікові записи в різнорідних ресурсах та активах, включаючи хмарні ідентифікатори).

Формування типових вимог дозволить підвищити ефективність формування політики управління доступом в системах управління інформаційною безпекою державного та корпоративного сектору, уникнути непотрібних ризиків і усунути можливі проблеми з несанкціонованим використанням корпоративних IT-ресурсів.

Для однозначної трактовки термінів їх визначення наведені в таблиці 1.

Таблиця 1

Терміни та визначення

Термін	Визначення
Аутентифікація	Перевірка приналежності суб'єкту доступу пред'явленого їм ідентифікатора; підтвердження автентичності. Найчастіше аутентифікація виконується шляхом набору користувачем свого пароля на клавіатурі комп'ютера або можуть використовуватись сучасні електронні засоби аутентифікації (що є більш прийнятним і надійним).
Ідентифікація	Присвоєння суб'єктам доступу (користувачам, процесам) і об'єктам доступу (інформаційним ресурсів, пристроям) ідентифікатора і (або) порівняння пред'явленого ідентифікатора з переліком присвоєних ідентифікаторів.
Інформаційна система	Сукупність програмного забезпечення і технічних засобів, що використовуються для зберігання, обробки і передачі інформації, з метою вирішення бізнес-завдань організації. У організації можуть використовуються різні типи інформаційних систем для вирішення виробничих, управлінських, облікових та інших бізнес-завдань.
Корпоративний IT-ресурс	Об'єднання інформаційних систем, баз даних, хмарних додатків, комп'ютерного, телекомунікаційного та офісного обладнання всіх підрозділів організації, що управляється, за допомогою їх підключення до єдиної мережі передачі даних організації з використанням різних каналів зв'язку.

Корпоративна мережа	Корпоративна мережа - комунікаційна система, що належить і/або керована єдиною організацією відповідно до правил цієї організації, головним призначенням якої є забезпечення функціонування конкретної організації, що володіє цією мережею.
Критична інформація	Інформація, порушення доступності, цілісності, або конфіденційності якої, може привести до негативного впливу на функціонування підрозділів організації, призвести до заподіяння матеріального чи іншого виду шкоди.
Несанкціонований доступ	Доступ до інформації, що порушує встановлені правила розмежування доступу.
Користувач	Співробітник організації (штатний, тимчасовий, який працює за контрактом і ін.), а також інші особи (підрядники, аудитори тощо), зареєстровані в корпоративній мережі організації в установленому порядку і які отримали права на доступ до корпоративних ІТ-ресурсів відповідно до своїх функціональних обов'язків.
Реєстраційний (обліковий) запис користувача	Сукупність відомостей про користувача, яка включає в себе ім'я користувача і його унікальний цифровий ідентифікатор, однозначно ідентифікує даного користувача в операційній системі (мережі, базі даних, прикладному додатку і т.п.). Реєстраційний запис створюється при реєстрації користувача в операційній системі комп'ютера, в системі управління базами даних, в мережевих доменах, додатках і т.п. Він також може містити такі відомості про користувача, як П.І.Б., назву підрозділу, телефони, e-mail та ін.

Виклад основного матеріалу дослідження

Зважаючи на ріст рівня кіберзагроз для державного та корпоративного сектору, варто виокремити декілька основних тверджень.

Твердження 1.

Політика управління доступом корпоративних користувачів до інформаційних, хмарних та технічних ІТ-ресурсів (надалі корпоративних ІТ-ресурсів) корпоративної мережі повинна включати в себе, але не обмежуватися наступним змістом:

- порядком надання користувачам прав доступу до корпоративних ІТ-ресурсів, включаючи мережеві сервіси (сервіс друку, електронна пошта, веб-сервери і т.д.), розподілені мережеві ресурси (файли, каталоги, диски, робочі станції, периферія), бази даних, хмарні додатки і т.п.;
- порядком надання віддаленим користувачам прав доступу до корпоративних ІТ-ресурсів через мережі загального доступу;
- порядком скасування прав доступу звільнених співробітників до корпоративних ІТ-ресурсів;
- порядком зміни прав доступу при переході на іншу посаду, зміні посадових обов’язків і т.п.;
- вимогами, що пред’являються до користувачів у зв’язку з наданням їм доступу до корпоративних ІТ-ресурсів;
- порядком здійснення контролю за положеннями політики, що регламентує порядок доступу до корпоративних ІТ-ресурсів;
- відповідальністю користувачів за порушення вимог політики доступу до корпоративних ІТ-ресурсів.

Твердження 2.

Вимоги політики управління доступом повинні поширюватися на всіх користувачів, яким надано доступ до корпоративних ІТ-ресурсів, без виключення. В цей перелік включаються всі користувачі корпоративної мережі (штатні співробітники, тимчасові, що працюють за контрактом і ін.), а також інші особи (підрядники, аудитори і т.п.), зареєстровані як користувачі в корпоративній мережі в порядку, що встановлюється політикою управління доступом.

Твердження 3.

Доступ до корпоративних ІТ-ресурсів повинен здійснюватися зареєстрованими користувачами при пред’явленні доказів їх справжності (аутентифікації). Використовувана схема аутентифікації повинна бути стійка до несанкціонованого прослуховування каналів зв’язку.

Твердження 4.

Для надання користувачам прав доступу до корпоративних ІТ-ресурсів повинна здійснюватися процедура їх реєстрації в корпоративній мережі з визначенням профілю користувача (роль та права доступу) [2]. Внаслідок виконання процедури реєстрації для

кожного співробітника створюється в корпоративній мережі реєстраційний запис, що в подальшому використовується для отримання доступу до корпоративних ІТ-ресурсів відповідно до заданому профілю та функціональних обов'язків. Для привілейованих користувачів допускається створення додаткових привілейованих реєстраційних записів, які можуть використовуватись ними як сеансові на період виконання привілейованих операцій в корпоративній мережі.

Твердження 5.

Реєстраційний запис користувача повинен бути унікальним та самодостатніми для однозначної ідентифікації користувача і визначення його профілю з метою надання користувачу відповідних прав доступу до корпоративних ІТ-ресурсів і забезпечення можливостей здійснення оперативного контролю над діями користувача зі сторони служб ІТ та інформаційної безпеки, а також аудиторських служб.

Твердження 6.

Всі запити на надання або зміну прав доступу користувача повинні реєструватися в журналі або в системі типу HelpDesk (при наявності) і підкріплюватися оригіналами заявок встановленого зразка.

Виходячи із вище сформульованих тверджень в політику управління порядком доступу користувачів до корпоративних ІТ-ресурсів доцільно включити наступні ключові вимоги:

Щодо порядку надання користувачам загальних прав доступу до корпоративних ІТ-ресурсів:

- доступ до корпоративних ІТ-ресурсів надається користувачеві на підставі письмової або цифрової заявки встановленої форми, яка подається в службу ІТ з підписом (цифровим підписом) керівника структурного підрозділу, в якому працює користувач;
- у заявці має бути зазначені ідентифікаційні дані користувача, термін дії необхідних прав доступу, перелік ресурсів і рівень повноважень, необхідних даному користувачеві (профіль користувача);у разі, якщо профіль користувача включає в себе ресурси інших підрозділів, то ініціатор заявки в обов'язковому порядку надає необхідні погоджуючі підписи (цифрові підписи) керівників підрозділів, що володіють цими ресурсами;
- заявка на надання (внесення змін) прав доступу до корпоративних ІТ-ресурсів узгоджується керівниками служб ІТ та інформаційної безпеки;
- доступ до корпоративних ІТ-ресурсів надається користувачеві у відповідності до його профілю на час і в обсязі, необхідному для виконання ним своїх посадових обов'язків;
- початковий доступ до корпоративних ІТ-ресурсів надається користувачеві тільки після вивчення документів, що регламентують правила доступу та правила використання корпоративних ІТ-ресурсів. Факт проведення такого навчання повинен реєструватися в окремому журналі служби інформаційної безпеки з фіксацією дати проведення навчання, переліку вивчених документів та оригіналу підпису користувача про ознайомлення з відповідними документами;
- форма заявки на створення (зміну) реєстраційного запису користувача розробляється та зберігається в службі ІТ;
- на основі затвердженої заявки служба ІТ зобов'язана створити (внести зміни) реєстраційний запис користувача і надати йому права доступу до корпоративних ІТ-ресурсів у відповідності до його профілю та посадових обов'язків.

Щодо порядку надання віддаленим користувачам прав доступу до корпоративних ІТ-ресурсів при використанні мереж загального користування:

- віддалений доступ до корпоративних ІТ-ресурсів надається користувачеві з обов'язковим виконанням всіх вимог до звичайного доступу;
- віддалений доступ до корпоративних ІТ-ресурсів надається користувачеві з використанням VPN-каналу та засобів апаратної аутентифікації (при наявності);

- віддалений доступ до корпоративних ІТ-ресурсів надається користувачеві з використанням з використанням засобів шифрування;
- віддалений доступ до корпоративних ІТ-ресурсів надається користувачеві з використанням засобів управління мобільними додатками, що забезпечують відповідний порядок захисту конфіденційної інформації;
- при надані віддаленого доступу до корпоративних ІТ-ресурсів повинна бути передбачена процедура та можливості визначення місцеположення, блокування та знищення конфіденційної інформації у разі втрати обладнання або засобів, що використовувалось для віддаленого доступу до корпоративних ІТ-ресурсів;
- процедура надання віддаленого доступу до корпоративних ІТ-ресурсів регламентується окремим документом.

Щодо порядку скасування користувачам, що звільняються, прав доступу до корпоративних ІТ-ресурсів

- в день подачі користувачем заяви про звільнення або закінчення терміну роботи користувача його керівник (незалежно він є прямий чи опосередкований (при виконанні робіт сторонніми особами/організаціями)) зобов'язаний направити в службу ІТ заявку про скасування або встановлення користувачеві тимчасових прав доступу до корпоративних ІТ-ресурсів (на період проходження процедури звільнення) та проконтролювати, в найкоротший термін, її отримання уповноваженою особою в службі ІТ;
- служба ІТ зобов'язана негайно сповістити уповноважену особу в службі інформаційної безпеки щодо ініційованих змін у повноваженнях користувача, що звільняється;
- кадрова служба зобов'язана повідомити уповноважену особу в службі ІТ про звільнення співробітника негайно після підписання наказу про звільнення користувача;
- після отримання заявки керівника підрозділу або сповіщення кадрової служби про підписання наказу про звільнення користувача служба ІТ повинна провести блокування всіх реєстраційних записів користувача, що звільняється, на термін визначений процедурою внутрішньої міграції даних (проведення змін у правах доступу для подальшого використання іншим користувачем) у структурних підрозділах;
- у разі наявності прав доступу до корпоративних систем та сервісів, що не вимагають наявності облікового запису користувача, такі права доступу повинні бути заблоковані;
- після закінчення терміну внутрішньої міграції служба ІТ сповіщає керівника відповідного структурного підрозділу та видаляє обліковий запис користувача.

Щодо порядку зміни користувачам загальних прав доступу до корпоративних ІТ-ресурсів:

- у разі зміни посадових обов'язків користувача або прав доступу, переведення на іншу посаду, в інший підрозділ його керівник зобов'язаний подати уповноваженому співробітнику в службі ІТ заявку с повідомленням про зміну профілю, посадових обов'язків та прав доступу користувача;
- керівник підрозділу, який залишає користувач, у разі зміни посадових обов'язків, зобов'язаний подати уповноваженому співробітнику в службі ІТ заявку з повідомленням про скасування відповідних прав доступу у даному структурному підрозділі;
- форма заявки розробляється та зберігається в службі ІТ;
- зміна прав доступу користувача здійснюється у відповідності до порядку надання користувачам загальних прав доступу до корпоративних ІТ-ресурсів.

Щодо порядку зміни віддаленим користувачам прав доступу до корпоративних ІТ-ресурсів при використанні мереж загального користування:

- порядок зміни віддаленим користувачам прав доступу до корпоративних ІТ-ресурсів при використанні мереж загального користування аналогічний порядку зміни загальних прав доступу користувача до корпоративних ІТ-ресурсів.

Щодо порядку контролю прав доступу користувачів до корпоративних ІТ-ресурсів:

- контроль прав доступу користувачів до корпоративних ІТ-ресурсів здійснюється шляхом регулярного проведення аудиту прав доступу користувачів до корпоративних ІТ-ресурсів;
- контроль (аудит) прав доступу може здійснюватися спеціалістами служб ІТ, інформаційної безпеки або відповідних аудиторських компаній;
- співробітники служби ІТ повинні здійснювати регулярний аналіз журналів реєстрації подій, що мають відношення до спроб обходу механізмів захисту корпоративних ІТ-ресурсів та спроб отримання несанкціонованого доступу до корпоративних ІТ-ресурсів;
- у разі виявлення вищевказаних інцидентів повинна бути негайно проінформована служба інформаційної безпеки та вжиті заходи щодо припинення спроб несанкціонованого доступу;
- за всіма фактами, пов'язаними з порушенням порядку та вимог, щодо доступу до корпоративних ІТ-ресурсів повинно бути проведене службове розслідування з складання протоколу щодо результатів розслідування та прийнятих заходів;
- результати розслідування доводяться до відома власника корпоративних ІТ-ресурсів;
- контроль прав доступу користувачів до корпоративних ІТ-ресурсів здійснюється по мірі необхідності, але не рідше чим один раз на рік;

Щодо відповідальності за здійснення контролю за правами доступу користувачів до корпоративних ІТ-ресурсів:

- відповідальність щодо дотримання вимог політики управління правами доступу до корпоративних ІТ-ресурсів несе керівник ІТ;
- відповідальність за здійснення контролю щодо виконання вимог політики управління правами доступу до корпоративних ІТ-ресурсів несе керівник інформаційної безпеки;
- користувачі, що порушують вимоги політики управління правами доступу до корпоративних ІТ-ресурсів можуть піддані дисциплінарним стягненням, відповідно до діючого Трудового кодексу України.

Висновок

Питання організації безпеки корпоративних ІТ-ресурсів, а зокрема управління правами доступу до них, на даний час досить гостро стоять у державному та корпоративному секторах. Проаналізовані і сформовані рекомендації та вимоги щодо створення політик управління доступом до корпоративних ІТ-ресурсів організацій різних форм власності, можуть допомогти суттєво зменшити ризики пов'язані з несанкціонованим доступом до інформації, втратою інформації з обмеженим доступом, компрометації організацій і т.п. Подальші дослідження варто зосередити на створенні та впровадженні типової політики управління правами доступу та навчанні персоналу.

Література:

1. Управління доступом. TechNet - Microsoft (https://technet.microsoft.com/ru- ru/library/cc770749 *(v=ws.11).aspx)*

2. Рольове управління доступом для IBM Systems Director Console (http://www.ibm.com /support/knowledgecenter/ru/ssw_aix_71/com.ibm.aix.sysdircon/rbac_main.htm)

3. Борсуковський Ю.В., Бурячок В.Л., Складанний П.М. Аналіз сучасних вимог до створення парольних політик корпоративних користувачів. / Сучасний захист інформації №3, 2016, с.72-76

4. Бурячок В.Л. Політика інформаційної безпеки: підручник. / В.Л.Бурячок, Р.В.Грищук, В.О.Хорошко / За заг. ред. докт. техн. наук, проф. В.О. Хорошка. – К.: ПВП «Задруга», 2014. – 222 с.

5. Бурячок В.Л. Політика інформаційної безпеки: навчальний посібник. / В.Л.Бурячок, Р.В. Грищук, В.О.Хорошко / За заг. ред. докт. техн. наук, проф. В.О. Хорошка. – К.: ПВП «Задруга», 2014. – 134 с.

Надійшла 22.11.2016 р. Рецензент: к.т.н., доц. Гулак Г.М.