УДК 004.056 **Ю.В. Борсуковський, В.Ю. Борсуковська**

ВИЗНАЧЕННЯ СУЧАСНИХ ВИМОГ ЩОДО ПОЛІТИКИ ВИКОРИСТАННЯ ЗАСОБІВ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ

В даній статті проведено детальний аналіз вимог до формування політики інформаційної безпеки щодо використання засобів криптографічного захисту інформації з метою реалізації організаційних та технічних заходів по запобіганню витокам конфіденційної інформації на підприємстві. Сформульовані базові вимоги та рекомендації щодо структури та змісту політики інформаційної безпеки для створення, впровадження та експлуатації превентивних процедур управління захистом інформації із обмеженим доступом. Враховано практичний досвід розробки, впровадження та управління сучасними політиками інформаційної безпеки щодо використання засобів криптографічного захисту конфіденційної інформації на підприємствах різної форми власності.

Ключові слова: криптографічний захист, шифрування, доступ, політика, кібербезпека

Вступ і постановка задачі

Створення та поширення перспективних технологій сприяє появі нових форм кібератак, що піддають інформаційні ресурси підприємств загрозам, до яких вони не готові.

Криптографічний захист конфіденційної інформації дозволяє забезпечити додатковий рівень безпеки даних з обмеженим доступом, шляхом створення додаткового захисту на локальних інформаційних ресурсах, а також в ході їх передачі по відкритим мережам зв’язку. Використання криптографічного захисту, на сьогоднішній день, вважається ІТ-фахівцями найбільш ефективним способом захисту інформації від несанкціонованого доступу.

Із врахуванням чинного ландшафту інформаційних та кібернетичних загроз, криптографічний захист інформації сьогодні доцільно використовувати для роботи із усіма даними, чутливими для бізнесу. Такі дані можуть оброблятися і зберігатися на жорстких дисках, переносних пристроях, в електронних листах, файлах, папках і в інших місцях. Можна сформулювати ряд специфічних ризиків інформаційним ресурсам підприємства, задля своєчасного запобігання яким, доцільно використовувати шифрування конфіденційної інформації [3]:

1. **Крадіжка комп'ютерного обладнання.**

При крадіжці і втраті комп'ютерної техніки конфіденційні дані, що зберігаються на незашифрованих дисках та інших носіях інформації, можуть бути без проблем прочитані зловмисником і продані зацікавленим особам, в тому числі конкурентам. Крім того, в разі раптових перевірок та вилученні комп'ютерного обладнання представниками держорганів інформація конфіденційного характеру може стати відомою стороннім особам.

2. **Промислове шпигунство.**

Інциденти промислового шпигунства, які спостерігаються останнім часом, пов'язані з високим рівнем фінансових ризиків. Зловмисником, може бути будь який, навіть самий «надійний», співробітник підприємства. Він може отримати доступ до ресурсів на яких зберігаються критично важливі для бізнесу дані в незашифрованому вигляді. Крім того, потрібно пам’ятати, що адміністратори систем та додатків мають, апріорі, повний доступ до будь якої інформації що зберігається на комп’ютерах, серверах та різноманітних електронних носіях інформації.

3. **Компромат.**

При фізичному доступі до комп'ютера або сервера зловмисник може розмістити на них будь-яку небажану інформацію і оповістити про це зацікавлених осіб. При цьому, наслідки для бізнесу можуть бути доволі непередбачуваними.

4. **Недбалість співробітників.**

Якщо співробітник раптово залишив робоче місце і забув заблокувати комп'ютер, інформація може стати доступною стороннім особам і може бути використана для заподіяння серйозного збитку власнику інформації. Крім того, співробітник може помилково направити інформацію конфіденційного характеру не довіреному адресату.

Окремою проблемою в кіберпросторі стане реалізація кіберстратегій на рівні державних політик, що явно декларують можливості проведення конкурентної розвідки у інтересах власних виробників, а також подальше розширення технічних можливостей кримінальних структур.

Величина загроз по відношенню до конфіденційної інформації підприємств з кожним роком тільки збільшується. По даним останнього дослідження компанії Fortinet кількість атак, що приходиться на одну організацію збільшилось за останній квартал 2017 на 82% [5]. Після публікації WikiLeaks документів і файлів із закритої мережі Центру радіотехнічної і електронної розвідки ЦРУ в Ленглі - по суті елементів кіберзброї - через дуже короткий термін засоби і наробки державного органу було ефективно використано в кримінальних цілях [4].

Основні переваги використання засобів криптографічного захисту конфіденційної інформації на підприємстві:

- надійний захист конфіденційної інформації, що регулярно використовується в електронному вигляді у бізнес-діяльності підприємства;
- можливість захисту від несанкціонованого доступу баз даних, корпоративної пошти та іншої інформації з обмеженим доступом;
- надання доступу до конфіденційних даних тільки довіреним співробітникам;
- наявність засобів екстреного блокування доступу до конфіденційних даних;
- захист від несанкціонованого копіювання конфіденційних даних нелояльним або підкупленим співробітником, який може мати фізичний доступ до комп'ютерного та серверного обладнання.
- зниження ризиків прямих і непрямих фінансових втрат внаслідок несанкціонованого витоку критичної для бізнесу інформації;
- підвищення рівня довіри клієнтів і партнерів;
- підвищення рівня корпоративної бізнес-етики при зовнішньому і внутрішньому інформаційному обміні електронними повідомленнями;
- забезпечення впевненості у надійному захисті конфіденційної інформації.

Таким чином, впровадження засобів криптографічного захисту конфіденційної інформації дозволить знизити ризики витоку інформації із обмеженим доступом і підвищити конкурентоздатність підприємства. Очевидно, що впровадження засобів криптографічного захисту конфіденційної інформації потребує розробки відповідної політики підприємства і це вимагає формалізації основних її складових з метою створення відповідних процедур та інструкцій для розгортання, впровадження, експлуатації і ефективного управління засобами криптографічного захисту конфіденційної інформації.

Терміни та визначення

Для однозначного трактування термінів і їх визначень відповідні роз’яснення наведені в таблиці 1.

Таблиця 1. Терміни та визначення

Термін		**Визначення**
Відкритий ключ		ключ, який доступний всім на кожному з етапів його життєвого циклу
Дешифрування інформації		відновлення відкритого тексту з шифротексту за відомими ключами.
ДІТ		департамент інформаційних технологій
Життєвий цикл ключа		послідовність стадій, які проходить ключ від моменту встановлення до наступної заміни
Засіб		програмний, апаратно-програмний, апаратний або інший засіб,

криптографічного захисту інформації (ЗсКЗІ)		призначений для криптографічного захисту інформації
ІзОД		інформація з обмеженим доступом
КК		керуюча компанія
Компрометація		факт чи підозра на доступ сторонньої особи до інформації, що захищається
Компрометація особистого ключа		втрата довіри до того, що сторонні особи не мають або не мали в минулому доступ до використовуваних секретним ключам. До подій, пов'язаних з компрометацією ключа, відносяться (включаючи, але не обмежуючись) наступні події: • порушення цілісності корпусу носія; • втрата ключових носіїв; • втрата ключових носіїв з подальшим виявленням; • звільнення співробітників, що мали доступ до ключових носіїв; • виникнення підозр на витік інформації або її спотворення в ЗсКЗІ; • порушення цілісності печаток на сейфах з ключовими носіями, якщо використовується процедура опечатування; • втрата ключів від сейфів (приміщень) в момент знаходження в них ключових носіїв; • втрата ключів від сейфів (приміщень) в момент знаходження в них ключових носіїв з подальшим виявленням; • доступ сторонніх осіб до ключової інформації; • випадки, коли не можна достовірно встановити причину виходу з ладу ключових носіїв (в тому числі, коли спростована можливість того, що даний факт стався в результаті несанкціонованих дій зловмисника)
Криптографічний захист (КЗ)		вид захисту інформації, який забезпечує конфіденційність і автентичність інформації шляхом перетворення інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її істинності, цілісності, авторства тощо
Криптографічні ключі		приватні та публічні ключі призначені для накладання / перевірки електронного цифрового підпису, шифрування / дешифрування електронних документів
Носій ключової інформації (НКІ)		носій інформації (флешка, eToken, і т.п.), що містить один або кілька криптографічних ключів
Секретний (особистий) ключ		ключ, який повинен зберігатися в секреті і не повинен бути доступним стороннім особам на кожному з етапів його життєвого циклу
СлІБ		служба інформаційної безпеки
Управління ключами		створення (генерація) ключів, їх зберігання, поширення, видалення (знищення), облік і застосування, а також видача та відкликання сертифікатів ключів підписів відповідно до політики безпеки застосування ЗсКЗІ
Шифротекст		результат операції шифрування
Шифрування інформації		перетворення відкритого тексту в шифротекст

Виклад основного матеріалу дослідження

Зважаючи на ріст рівня інформаційних та кібернетичних загроз для підприємств різної форми власності, варто виокремити декілька основних тверджень щодо підходу до формування політики криптографічного захисту інформації з обмеженим доступом. Для наочності і, як приклад, розглянемо основні складові сучасних вимог щодо формування політики використання засобів криптографічного захисту інформації на підприємстві (в нашому випадку - керуючій компанії).

Твердження 1. Загальні положення

З метою забезпечення у керуючій компанії (далі КК) захисту інформації від несанкціонованого доступу, витоку, умисного або необережного порушення цілісності, або доступності та інших загроз інформаційній безпеці, політика інформаційної безпеки встановлює вимоги до використання засобів криптографічного захисту інформації.

Засоби криптографічного захисту інформації повинні забезпечувати шифрування дисків робочих станцій, інформації на знімних носіях, електронної пошти, папок і файлів в корпоративній мережі КК, а також забезпечувати можливість роботи із зашифрованою електронною поштою на мобільних пристроях.

Твердження 2. Призначення

Чинна політика встановлюється для використання ЗсКЗІ з метою захисту конфіденційності, автентичності та цілісності ІзОД, а також підтримки інформаційної безпеки при зберіганні та обміні інформацією з обмеженим доступом як всередині КК, так і з зовнішніми кореспондентами.

Чинна політика визначає:

- основні положення при роботі з ЗсКЗІ;
- вимоги інформаційної безпеки до ЗсКЗІ;
- відповідальність при роботі з ЗсКЗІ.

Твердження 3. Сфера дії

Політика поширюється на всіх співробітників КК, а також третіх осіб, які беруть участь у електронному документообігу КК, і є обов'язковою для виконання всіма співробітниками, без виключення.

Всі виключення із чинних вимог політики повинні бути погоджені службою інформаційної безпеки КК.

Твердження 4. Основні вимоги до використання ЗсКЗІ

ЗсКЗІ повинні використовуватися відповідно до вимог КК, викладеними в даній політиці.

Перелік, дозволених для використання ЗсКЗІ, визначає СлІБ керуючої компанії.

При розробці, впровадженні та використанні елементів ЗсКЗІ в обов'язковому порядку враховуються і реалізуються вимоги даної політики.

ЗсКЗІ повинні застосовуватися для:

- шифрування інформації, що зберігається і передається;
- забезпечення цілісності та / або автентичності;
- забезпечення неможливості відмови від вчинених дій шляхом застосування криптографічних методів отримання доказів появи, відсутності події або дії.

При використанні шифрованих файлових папок загального доступу додатково повинні бути розмежовані права доступу користувачів на системному рівні і надаватися тільки співробітникам, які мають відповідні дозволи на доступ до цих папок [1, 2].

Всі локальні і знімні диски на комп'ютерах співробітників (користувачів) повинні шифруватися.

Для завантаження операційних систем комп'ютерів із зашифрованими дисками повинна використовуватися процедура додаткової передзавантажувальної аутентифікації.

Для змінних носіїв повинна застосовуватися процедура примусового шифрування інформації при записі на них будь-якої інформації, за виключенням пристроїв які включені в

перелік і на які може записуватись інформація у відкритому вигляді. Чинний перелік таких пристроїв затверджує СлІБ за письмовим поданням керівника організаційного підрозділу.

До отриманих або згенерованих криптографічних ключів повинні застосовуватися заходи захисту від їх втрати, зміни або руйнування. Закриті ключі повинні захищатися від несанкціонованого доступу і розкриття.

Криптографічні ключі користувачів повинні мати певний строк дії і бути доступні всім учасникам інформаційного обміну.

Підтвердження дійсності криптографічних ключів користувачів має відбуватися автоматично кожні 14 (чотирнадцять) днів.

У випадки неактивності криптографічного ключа користувача протягом 90 (дев'яноста) днів ключ повинен автоматично блокуватися для пошуку в ЗсКЗІ.

Парольна фраза (за необхідності використання) повинна відповідати вимогам "Політики забезпечення інформаційної безпеки при використанні парольного захисту" та значенню рівному 100% в параметрі оцінки якості паролю, як правило, вбудованого в засіб криптографічного захисту інформації (при наявності). Рекомендована мінімальна довжина парольної фрази не менше 24 (двадцяти чотирьох) символів. Використання прогалин в парольній фразі не рекомендується.

При звільненні співробітника, закриті ключі повинні бути збережені (при наявності такої можливості в ЗсКЗІ) у архівне сховище ключів СлІБ і анульовані.

При компрометації секретних ключів та / або ключової інформації співробітники СлІБ повинні вжити заходів для припинення будь-яких операцій з використанням цих ключів і ключової інформації, а також виконати заходи щодо заміни ключів шифрування і ключової інформації.

При компрометації засобів криптографічного захисту співробітники СлІБ повинні вжити заходів для припинення будь-яких операцій з використанням ЗсКЗІ, а також провести заходи по заміні засобів криптографічного захисту інформації.

Всі дії з управління криптографічними ключами повинні реєструватися системою управління ключами, а якщо така функціональність недоступна - у паперовому вигляді.

Процеси управління засобами криптографічного захисту здійснюються відповідно до експлуатаційної та технічної документації, правил користування (встановленими процедурами і регламентами).

Порядок функціонування ЗсКЗІ, обов'язки співробітників, які забезпечують її працездатність, правила роботи співробітників, що використовують ЗсКЗІ, повинні бути регламентовані відповідними посадовими інструкціями, процедурами і регламентами.

Твердження 5. Вимоги щодо криптографічного захисту інформації з обмеженим доступом

Передача і зберігання документів, які містять ІзОД, допускається при обов'язковому застосуванні засобів криптографічного захисту інформації (електронні документи повинні шифруватися в обов'язковому порядку).

Співробітникам, які використовують ЗсКЗІ, категорично забороняється:

- передавати будь-кому свій секретний криптографічний ключ;
- розголошувати пароль доступу (пін-код) до свого секретного криптографічного ключа, в тому числі своєму безпосередньому керівництву;
- повідомляти будь-кому, що він є власником секретного криптографічного ключа;
- використовувати секретний криптографічний ключ на явно несправному пристрої зчитування, несправному персональному комп'ютері, ноутбуці, планшеті, мобільному пристрої, сервері і т.п.;
- порушувати вимоги документів, що регламентують правила отримання / зберігання / роботи із засобом криптографічного захисту інформації.

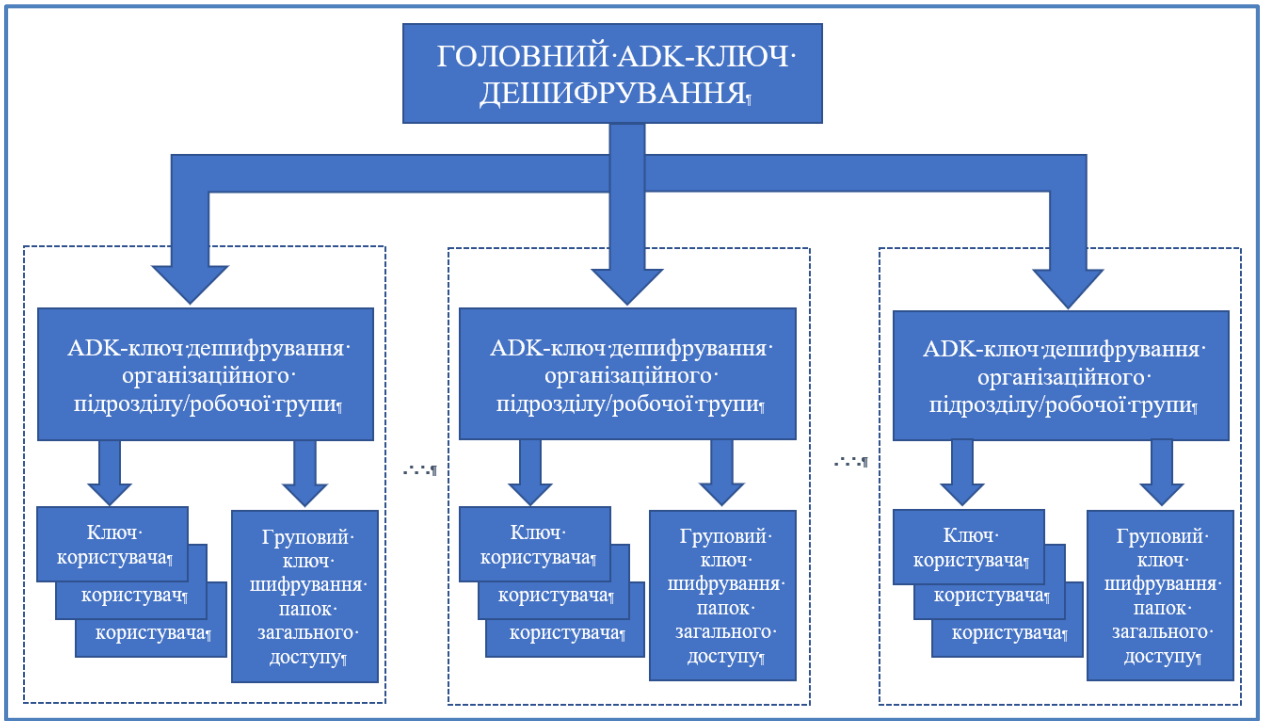

Рис. 1. Ієрархія ключів шифрування / дешифрування

де:

Головний ADK-ключ дешифрування - ключ, який додається до кожного процес шифрування, який відбувається в межах підпорядкованості КК (Рис. 1).

ADK-ключ дешифрування організаційного підрозділу - ключ, який додається до кожного процесу шифрування, який відбувається в межах організаційного підрозділу та / або робочої групи (див. Рис. 1).

Ключ користувача (співробітника) - персональний ключ, який застосовується співробітником для шифрування / дешифрування інформації, що знаходиться в його розпорядженні при виконанні службових обов'язків (Рис. 1).

Груповий ключ шифрування папок загального доступу - ключ, який використовується групою користувачів організаційного підрозділу та / або робочою групою для шифрування загальних папок і подальшого доступу до зашифрованої в них інформації (Рис. 1).

Організаційний підрозділ - група користувачів, яка створюється на підставі належності співробітників до певних структурних об'єднань та / або робочих груп (департамент, відділ, сектор, робоча група).

Твердження 7. Вимоги щодо встановленої ієрархії криптографічних ключів

З метою забезпечення конфіденційності і автентичності інформації, запобігання витокам, умисного або необережного порушення цілісності, доступності, а також інших загроз інформаційній безпеці в КК повинні бути визначені та затверджені вимоги щодо ієрархії криптографічних ключів.

Дані вимоги встановлюють чинну ієрархію ключів шифрування і додаткових ключів дешифрування з метою підтримки інформаційної безпеки при зберіганні та обмін інформацією в КК.

Ці вимоги визначають:

- ієрархію додаткових ключів дешифрування (ADK-ключ) КК;
- вимоги до найменування ADK ключів;
- відповідальність при роботі с ADK ключами.

Твердження 8. Сфера дії ієрархії криптографічних ключів

Ієрархія ключів шифрування і додаткових ключів дешифрування поширюється на ключі всіх співробітників КК, які мають відповідні права для отримання / зберігання / роботи з криптографічними ключами.

Всі виключення з даних вимог щодо чинної ієрархії криптографічних ключів повинні бути узгоджені зі службою інформаційної безпеки КК.

Твердження 9. Вимоги щодо структури ADK-ключів

У КК повинна бути встановлена дворівнева структура додаткових ключів дешифрування, які забезпечують аварійну можливість доступу до зашифрованої інформації у спеціальних випадках, що встановлюються КК (Рис. 1).

Додаткові ключі дешифрування повинні бути включені в усі криптографічні ключі, які застосовуються в КК.

Твердження 10. Вимоги щодо найменування ключів дешифрування

Довжина найменування організаційного підрозділу в ADK-ключі не повинна перевищувати 30-ти символів.

Повинні бути задані шаблони найменування ключів дешифрування для їх створення і подальшого використання.

1. Шаблон найменування головного ADK-ключа дешифрування КК.

Приклад: Головний ключ дешифрування керуючої компанії «Bi3S»:

ADK.Bi3S.Ukraine-керуюча_компанія

2. Шаблон найменування ADK-ключів дешифрування для підпорядкованих бізнесів КК.

Приклад: Шаблон додаткових ключів дешифрування організаційних підрозділів керуючої компанії «Bi3S» у місті Києві:

ADK.Bi3S.KievUA-найменування_організаційного_підрозділу

Твердження 11. Відповідальність за виконання вимог чинної політики

Відповідальність за установку, налаштування, працездатність і підтримку в актуальному стані засобів криптографічного захисту інформації несе ДІТ.

Відповідальність за управління криптографічними ключами покладається на СлІБ.

Відповідальність за дотримання співробітниками (користувачами) КК вимог чинної політики інформаційної безпеки, а також здійснення контролю за фізичною цілісністю носіїв ключової інформації (секретні ключі, сертифікати тощо) користувачів (співробітників) покладається на їх безпосередніх керівників.

Відповідальність за підтримання чинної політики в актуальному стані несе СлІБ.

До співробітників, які порушують вимоги цієї політики, можуть бути застосовані заходи дисциплінарного впливу, включаючи догану і звільнення з роботи за грубе порушення вимог інформаційної безпеки КК.

Твердження 12. Історія змін чинної політики

Всі зміни і доповнення щодо чинної політики повинні протоколюватися в даному розділі із вказанням дати, причин та відповідального за внесення відповідних змін та доповнень.

Висновок

Масштабні кібератаки, масові випадки шахрайства з даниими та/або їх крадіжки призводять до значної економічної шкоди, спричиняють геополітичну напруженість і втрату довіри до Інтернету. Головною передумовою таких чинників у 2017-2018 роках стало, перш за все, зростання зацікавленості урядових структур в отриманні інформації, яка може бути використана супротивними сторонами в світовій конкурентній і політичній боротьбі.

Питання ефективної організації захисту інформації з обмеженим доступом переходить сьогодні в розряд найактуальніших питань у цілому світі. Особливо це актуально для підприємств, що відносяться до об’єктів критично-важливої інфраструктури.

Проаналізовані сучасні вимоги і сформовані рекомендації щодо базових елементів при формуванні політики криптографічного захисту підприємства дають можливість зменшити ризики, що пов'язані з несанкціонованим доступом до конфіденційної інформації, втратою та компрометацією конфіденційних інформаційних ресурсів підприємства і т.п.

Подальші дослідження варто зосередити на створенні та впровадженні типових процедур, регламентів та інструкцій щодо розгортання базових криптографічних засобів захисту інформації з обмеженим доступом та їх експлуатації (як комерційних, так і, враховуючи нинішню ситуацію, OpenSource), тренінгам персоналу правилам та практикам ефективного використання систем криптографічного захисту інформації.

Список використаної літератури

1. Управління доступом. Інтернет-ресурс. Режим доступу: TechNet - Microsoft (https://technet.microsoft.com/ru-ru/library/cc770749(v=ws.11).aspx)
2. Рольове управління доступом для IBM Systems Director Console. Інтернет-ресурс. Режим доступу: http://www.ibm.com/support/knowledgecenter/ru/ssw_aix_71/com.ibm.aix.sysdircon/rbac_main.htm
3. Шифрование данных. Інтернет-ресурс. Режим доступу: http://itprotect.ru/solutions/encryption/
4. WikiLeaks (@wikileaks). Інтернет ресурс. Березень 7, 2017
5. Fortinet. Інтернет-ресурс. Режим доступу: https://www.itweek.ru/security/news-company/detail.php?ID=199637

Надійшла: 10.02.2018 Рецензент: к.т.н. Довбешко С.В.