– від розміру ключа залежить кількість раундів шифрування: довжина 128 біт – 10 раундів; довжина 192 біта – 12 раундів; довжина 256 біт – 14 раундів;

– усі раунди, крім останнього, ідентичні.

Для АПК можна обирати деякі симетричні алгоритми шифрування із вищенаведених, в залежності від степені конфіденційності інформації. Але необхідно враховувати, що недоліком симетричного шифрування є те, що секретний ключ повинен бути відомий як відправнику, так і одержувачу. З одного боку, це викликає нову проблему відправки ключів. З іншого боку, одержувач на підставі існування зашифрованого і розшифрованого повідомлення не може довести, що отримав повідомлення від конкретного відправника, оскільки міг згенерувати одне і те ж повідомлення.

ОСНОВНІ ПРАВИЛА ЩОДО КІБЕРБЕЗПЕКИ БУХГАЛТЕРСЬКИХ ДАНИХ НА ПІДПРИЄМСТВАХ

Поливана Л.А., канд. екон. наук, доц.
Луценко О.А., канд. екон. наук, доц.
Державний біотехнологічний університет

Цифрова трансформація змінила правила поведінки бухгалтерів у повсякденному їх житті. Кожне підприємство зіткнулося з реальним світом, в якому технологічний розвиток та поява нових кіберзагроз сунеться швидкими темпами. Зростаюча залежність від технологій та зберігання конфеденційних бухгалтерських даних в цифрових форматах роблять підприємства привабливими цілями для кіберзлочинців. Несанкціонований доступ до цієї інформації може мати серйозні наслідки, включаючи фінансові втрати. Підприємства, які не використовують в своїй дяльності кібербезпеку, зазнають нових вразливостей, які загрожують їх діяльності. Щоб орієнтуватися в цій складній ситуації, бухгалтери повинні збалансовувати використання технологій для зростання та інновацій, одночасно захищаючі свої системи та дані від загроз. В цю епоху бухгалтери повинні залишатися інформованими та приймати надійні міри кібербезпеки для захисту своїх цифрових активів.

Кібербезпеку даних в бухгалтерському обліку розглянуто в працях таких вчених, як Бутинець Ф.Ф., Євдокимов В.В., Івахненко С.В., Палій В.Ф., Пушкар М.С., Шквір В.Д. Однак проблеми кібербезпеки даних бухгалтерського обліку вирішені недостатньо. Саме відсутність глобального керування та введених в дію стандартів кібербезпеки полегшують кіберзлочинцям виявлення та здійснення хакерських атак, тому що кіберзагрози не сповільнилися, а навпаки стали ще більш складними та витонченими.

Законом України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. №2163-VIII визначаються правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у

кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки. Відповідно до цього Закону: кібербезпека - захищеність життєво важливих інтересів людини і громадянина, суспільства та держави при використанны кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [1].

Кожне підприємство України веде бухгалтерський облік, а отже відповідно зберігає цінні фінансові дані та конфіденційну ділову інформацію. Ось чому підприємства повинні приймати запобіжні заходи, щоб захистити себе. Порушення в галузі безпеки ставлять під загрозу дані не тільки підприємства, а і його клієнтів.

Підприємства можуть знизити ризики, підтримуючі суворі протоколи конфеденційності. Отже, на підприємствах має бути обмеженим доступ до інформації співробітникам, підрядникам, та постачальникам послуг, яким необхідний доступ для виконання своїх обов'язків. Підприємства повинні регулярно перевіряти цей доступ. Це можна досягнути завдяки чітким системам забезпечення кібербезпеки.

Нами запропоновано узагальнення наступних правил кібербезпеки, дотримання яких буде гарантовано захищати бухгалтерські дані:

– правильне налаштування мережі: необхідно налагодити правильну конфігурацію в архітектурі мережі підприємства, також треба відслідкувати, щоб не постраждала оперативність передавання даних. Це можна зробити шляхом встановлення фаерволів нового покоління та постійного моніторингу онлайн-активності, відслідковуючі спроби кібервторгнення;

– управління ідентифікацією та доступом (IAM): бухгалтери можуть використовувати рішення для управління ідентифікацією та доступом до аутентифікації, авторизації до систем бухгалтерського обліку. Рішення з управління ідентицікацією та доступом можуть включати в себе інструменти для надання прав доступу та відслідковування спроб входу в систему та активність доступу;

– резервне копіювання: необхідно забезпечити резервне копіювання інформації, додатків та операційних систем, зберігати дані в хмарному середовищі. Треба завести правило, регулярно зберігати дані, з якими постійно працює підприємство. Зберігати копії треба окремо від систем, щоб запобігти їх шифруванню програмами-зчитувачами;

– застосовування політики зберігання даних: важливо вказати терміни зберігання конфіденційної інформації, а також правильні процедури знищення даних. Це допоможе мінімізувати ризик несанкціонованого доступу до застарілих даних;

– розробка та встановлення парольної політики: потрібно наполягати на тому, щоб співробітники не використовували однакові, прості та скромпометовані паролі для доступу до різних сервісів, також використовувати менеджери паролів, двофакторну аутентифікацію там де це можливо;

– застосовувати політику конфіденційності, яка пояснює як підприємство може управляти інформацією про клієнтів: регулярно проводити інструктажі, освітні програми в галузі інформаційної безпеки, які знижують вплив людського фактору, допомагають співробітникам розпізнавати та протидіяти можливому фішінгу;

– проводити моніторинг активності в мережі для виявлення слідів злому;

– впроваджувати програми реагування на інциденти: у з'вязку з оновленням законодавства та регулярними атаками необхідно розробляти програми політики, план, стандартні форми атестації, а також визначати відповідальних;

– оновлювати програмне забезпечення: треба постійно слідкувати за його оновленням, в тому числі і антивірусних програм. Розуміється, що використовувати треба тільки ліцензійне програмне забезпечення, яке має сертифікати безпеки;

– забезпечити безпеку систем електронної пошти: блокувати IP, час та місцезнаходження для доступу до електронної пошти. Треба налагодити аутентифікацію за допомогою єдиного входу до електронної пошти на підприємстві. Відключити протоколи поштових скриньок, такі як SMTP, POP, IMAP. Зобов'язати співробітників мати надійні паролі до електронних пошт. Обмежити права доступу тільки необхідними користувачами.

Досліджуючі питання кібербезпеки щодо бухгалтерської інформації ми дійшли розуміння, що підприємствам треба бути завжди пильними. Отже, нами запропоновано розширити Наказ про облікову політику ще одним додатком, який може мати назву «Політика інформаційної безпеки». Цей документ буде містити вказівки про те «що можна», а що «під забороною». В ньому повинно бути зазначене очікуване використання доступів до паролів та логінів у робочому середовищі, також можливий доступ до додатків або мереж, що використовує підприємство, правильне використання електронної пошти та доступ до неї, правила використання та зберігання виданої на роботі електронної техніки. Також пропонуємо оформлювати такі документи як «Згода про доступ до даних третіми особами», «План реагування на виток даних». Тому що наявність необхідної документації про відповідність потребам є важливою частиною управління бухгалтерськими даними.

Отже, цифрова трансформація призвела до революції в бухгалтерській галузі, а також зробила кібербезпеку главним пріоритетом. Щоб не потрапити в пастку, підприємствам пропонуємо підвищувати рівень інформованості в галузі кібербезпеки. Так це може бути просте тестування співробітників, або моделювання хакерських атак на бізнес. Беручі до уваги наші розробки та пропозиції, спеціалісти з бухгалтерського обліку зможуть забезпечити безпеку своїх систем та бухгалтерських даних при постійно зростаючих кіберризиках.

Інформаційні джерела:

1. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017р. №2163-VIII. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.