ВАСИЛЕНКО МИКОЛА ДМИТРОВИЧ

Національний університет «Одеська юридична академія», професор кафедри кібербезпеки, доктор фізико-математичних наук, доктор юридичних наук, професор, академік Міжнародної академії інформатизації

НОВІКОВ В'ЯЧЕСЛАВ ПАНТЕЛІЙОВИЧ

Національний університет «Одеська юридична академія», доцент кафедри кібербезпеки, кандидат технічних наук, доцент

ЗМЕНШЕННЯ ІМОВІРНОСТІ НЕСАНКЦІОНОВАНОГО ДОСТУПУ В КОМП'ЮТЕРНУ СИСТЕМУ ПРИ ПОСИЛЕННІ ПАРОЛЬНОГО ЗАХИСТУ

Стрімке зростання впливу інформатизації на різні сторони людської діяльності проходить на тлі швидкого становлення «інформаційного суспільства», можливості якого розцінюються як основа подальшого соціально-економічного розвитку сучасних країн за рахунок реалізації ІТ-технологій, зокрема систем штучного інтелекту, здатних створювати суперефективні виробництва. Тим не менш не можна не звертати увагу на деякі негативні, але досить важливі, тенденції загальної інформатизації. Так, наприклад, широкий спектр відомих загроз у сфері формування, збереження та розподілу інформаційних ресурсів та послуг дуже швидко доповнився новими загрозами, пов'язаними з несанкціонованим доступом (НСД) або втручанням різних зловмисників в роботу саме інформаційно-комунікаційних систем (ІКС), що функціонують в різних мережах. І хоча починаючи з 1999 р., в Україні розроблено відповідну нормативно-правову базу щодо захисту інформації, питання забезпечення інформаційної безпеки з багатьох причин все ще залишаються вельми актуальними [1]. Однією з причин такого стану галузі стала недостатня підготовленість, а найчастіше елементарна безвідповідальність, користувачів ІКС, (персоналу фірм та підприємств) в питаннях, пов'язаних з основами інформаційної безпеки ІКС, що призводить до збільшення ймовірності несанкціонованого доступу і проникнення в ІКС. Згідно зі звітом Verison по дослідженню витоку даних за 2016–2019 рр., після серії відомих атак, 63 % підтверджених витоків даних сталися з вини персоналу внаслідок використання ненадійних паролів, вкрадених або встановлених за замовчуванням, а також в порушення вимог експлуатаційної документації [2].

Не викликає сумнівів те, що високий ступінь інформатизації компаній та промислового виробництва вимагає високої кваліфікації працівників при обслуговуванні автоматизованих робочих місць (АРМ), основу яких складають комп'ютери різноманітних модифікацій, включених в різні мережі. На цих АРМ вже зараз створюється значний обсяг продукту, і тому в умовах високотехнологічних виробництв, НСД в такі АРМ вважається неприпустимим. Однак такі АРМ працюють,

як правило, в комп'ютерних мережах, куди при достатньому бажанні можуть проникати зловмисники. У цій ситуації необхідно використовувати ефективні заходи щодо захисту периметра АРМ. Дуже часто захист паролем виступає єдиним ефективним методом забезпечення безпеки таких ІКС. Слід зазначити, що останнім часом з'явилися різні системи захисту типу VPN (скорочення від англ. Virtual Private Network – віртуальна приватна мережа, яка представляє собою узагальнену назву технологій, що дозволяють створювати віртуальні захищені мережі поверх інших мереж із меншим рівнем довіри, а саме вони все частіше стали використовуватися). При цьому робота в умовах віддаленого доступу, яка характерна для нашого часу, накладає додаткові вимоги щодо інформаційної безпеки в таких системах, тому що призводить до додаткових завантажень мереж, що відкриває нові можливості для несанкціонованого доступу зловмисникам (див. [3; 4]). В умовах, що склалися, на думку американських експертів, зняття системи захисту інформації з комп'ютерних систем, призведе до банкрутства приблизно 20 % середніх підприємств протягом декількох годин, а з решти, (60–70) %, розоряться через кілька днів [1]. Тому з метою зниження інформаційних загроз (порушення конфіденційності, цілісності та доступності інформації) на початковому етапі життєвого циклу різних продуктів, велике значення набуває вміло організована робота на захищених програмно-апаратних засобах і системах. Аналіз хакерських атак говорить про те, що для здійснення підступних задумів зловмисникам потрібен контроль над системами доступу для отримання привілеїв вищого рівня [2]. В той же час отримання такого доступу для хакера можливе лише після входу в ІКС, й бажано засобами, що не виявляються засобами захисту даної системи. Найбільш ефективними способами з відповідними засобами захисту інформації від несанкціонованого доступу залишаються ідентифікація та аутентифікація, що засновані на криптографічному перетворенні інформації [5]. Способи аутентифікації в своїй більшості базуються на застосуванні одноразових або багаторазових паролів. А з урахуванням того, що багатофакторні системи аутентифікації ще не стали такими, що використовуються повсюдно, а ті, що вживаються, часто використовують імена користувачів і парольний захист без систем аутентифікації. Вибір ефективних способів встановлення парольного захисту для таких систем принципово впливає на вирішення основного питання щодо їх працездатності протягом цього життєвого циклу. Це передбачає використання таких різновидів способів аутентифікації, які реалізуються: по збереженої копії пароля або його згортку; по деякому перевірочному значенню; без безпосередньої передачі інформації про пароль стороні, що перевіряє; з використанням пароля для передачі криптографічного ключа.

Короткий аналіз цих способів показує, що перший спосіб передбачає наявність певної бази даних у обох чи кількох імен користувачів для збереження пароля, куди може проникнути зловмисник. Очевидно, що найбільш ефективний третій спосіб. Для виключення можливості несанкціонованого доступу у всіх інструкціях по експлуатації ІКС

рекомендується встановлювати не менше 6–8 букво-цифрових знаків, але зазвичай їх встановлюють менше. Це дозволяє з використанням програм типу Active Password Channger, без особливих зусиль, зламати або стерти паролі користувачів і безперешкодно дістатися до бази даних користувачів і паролів в ОС Windows, які зберігаються в SAM-файлі директорії С. Зазвичай на персональному комп'ютері встановлено 2–3 ОС. І в цьому випадку вибір для хакера відповідного SAM-файлу не представляє великих труднощів.

Не зупиняючись на математичному дослідженні стійкості парольних систем захисту документів і архівів, надамо лише посилання на покрокову інструкцію з установки паролю як одного з найвідповідальніших моментів в роботі: після моменту включення персонального комп'ютера [6]. Сама інструкція складається з семи кроків, дотримуватись які обов'язково з разі розуміння важливості збереження конфіденційності, а саме, мова йдеться про запобігання несанкціонованого доступу в комп'ютерну систему. Зазначимо лише те, що процес установки пароля може незначно відрізнятися від одного системного блоку до іншого, але його загальний сенс залишається незмінним.

Отже, установка надійного паролю різко знижує ймовірності злому парольного захисту навіть при використанні методів інтелектуального злому, словникових атак, а також систем автоматичного підбору всіяких комбінацій знаків.

Список використаної літератури:

1. Емельянов С. Л. Основы информационной безопасности : конспект лекций по спецкурсу / С. Л. Емельянов. – Одесса : ОНЮА., 2003. – 197 с.
2. Диогенес Ю., Озкайя Э. Кибербезопасность: стратегии атак и обороны / Ю. Диогенес, Э. Озкайя, пер. с анг. Д. А. Беликова. – Москва : ДМК Пресс, 2020. – 326 с.
3. Василенко М. Д., Новіков В. П., Рачук В. О. Безпека та виклики сучасності: ризики та кібербезпека в період пандемії / М. Д. Василенко, В. П. Новіков, В. О. Рачук // Безпека в сучасному світі : матеріали II Всеукраїнської науково-практ. конф. (м. Одеса, 20 листоп. 2020 р.) / за ред. О. В. Дикого. Одеса : Видавничий дім «Гельветика», 2020. – С. 93–98.
4. Василенко М. Д., Новіков В. П., Рачук В. О., Слатвинська В. М. Кібербезпека в проявах ризиків у період пандемії: стан та ґенеза / М. Д. Василенко, В. П. Новіков, В. О. Рачук, В. М. Слатвинська // Вісник Черкаського державного технологічного університету: технічні науки. – 2020. – № 3. – С. 51–60.
5. Никифоров С. Н. Методы защиты информации. Пароли, скрытие, шифрование / С. Н. Никифоров. – С.-Пб : Издат. центр «ИНТЕРМЕДИЯ» Лань, 2019. – 124 с.
6. Баркалов С. А., Барсуков О. М., Белоусов В. Е., Славнов К. Е. Информационная безопасность при управлении техническими системами: учеб. пособие / С. А. Баркалов, О. М. Барсуков, В.Е Белоусов., К.Е.Славнов. – С.-Пб : Издат. центр «ИНТЕРМЕДИЯ», 2016. – 498 с.

Ключові слова: інформація, інформатизація, персональні комп'ютери, інформаційно-комунікаційні системи, автоматизовані робочі місця, ідентифікація, аутентифікація, несанкціонований доступ, паролі.

Ключевые слова: информация, информатизация, персональные компьютеры, информационно-коммуникационные системы, автоматизированные рабочие места, идентификация, аутентификация, несанкционированный доступ, пароли.

Key words: information, informatization, personal computers, information and communication systems, automated workstations, identification, authentication, unauthorized access, passwords.

БАКУНИНА ЕЛЕНА ВАЛЕРЬЕВНА

Национальный университет «Одесская юридическая академия»,
доцент кафедры кибербезопасности,
кандидат физико-математических наук, доцент

О СУЩЕСТВОВАНИИ КЛАССА S-БЛОКОВ, УДОВЛЕТВОРЯЮЩИХ КОРРЕЛЯЦИОННОМУ ИММУНИТЕТУ КОМПОНЕНТНЫХ БУЛЕВЫХ ФУНКЦИЙ И 4-ФУНКЦИЙ

Одно из важнейших мест в любой комплексной системе защиты информации занимает криптографическая подсистема. При этом, со времен открытия К. Шенноном математически строго обоснованной теории секретной связи, теория криптографической стойкости получила свое существенное развитие во многом благодаря введению и описанию критериев криптографического качества компонентных булевых функций, с помощью которых могут быть представлены конструкции криптографического алгоритма [1; 2].

Тем не менее, дальнейшее развитие методов криптографии и криптоанализа, а также разработка новых методов криптоаналитических атак, основанных на функциях многозначной логики, актуализирует переход к последующему этапу развития криптографии, основанному на использовании преимуществ функций многозначной логики.

Переход к новому этапу означает разработку криптографических примитивов, в первую очередь S-блоков, для которых выполняются не только критерии криптографического качества компонентных булевых функции, но и новые критерии криптографического качества функций многозначной логики, с помощью которых могут быть описаны конструкции практически всех современных криптографических алгоритмов [3].

При этом важнейшим критерием, характеризующим способность S-блока, а значит, и всего криптопреобразования в котором он используется, противостоять атакам корреляционного криптоанализа, является критерий корреляционного иммунитета его компонентных функций.