Література

1. General Data Protection Regulation. URL: https://gdpr-info.eu/.

2. DIRECTIVE (EU) 2016/680 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, in vestigation, detection or prosecution of criminal of fences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN.

3. DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of securityof network and information system sacross the Union. URL:https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN.

4. Дрейс Ю., Лозова І., Педченко Є. Оцінювання негативних наслідків від витоку персональних даних. ITSec-2019 : матеріали IX міжнар. наук.-техніч. конф., м. Київ, 22-27 березня 2019 року. Київ, 2019. С. 41-42.

5. Дрейс Ю.О., Лозова І.Л. Розробка GDPR-моделі параметрів оцінювання наслідків витоку персональних даних. Комп'ютерні технології: інновації, проблеми, рішення: матеріали II Всеукр. наук.-техніч.конф., м. Житомир, 14-15 листопада 2019 р. Житомир: Житомирська політехніка, 2019.С. 78-79.

6. Y. Dreis, I. Lozova, A. Biskupskyi, Y. Pedchenko, Y. Ivanchenko.GDPR-model of parameters for estimating losses from loss of personal data. Przetwarzanie, transmisja i bezpieczeńs two informacji: Monografia. Tom2. AkademiaTechniczno-Humanistyczna w Bielsku-Bialej, 2019. pp.127 - 138.

УДК 004.056.53

АНАЛИЗ СОВРЕМЕННЫХ СИСТЕМ АУТЕНТИФИКАЦИИ

Журов Ю.С.
магистрант
кафедры безопасности информационных технологий,
Национальный авиационный университет
iurii.zhurov@gmail.com

Аннотация: Целью данного анализа является исследование современных методов и инструментов цифровой аутентификации, их сильных и слабых сторон, эффективности их использования. Также рассматривается современные направления развития цифровой аутентификации.

Актуальность предмета анализа обусловленна развитием информационных технологий. Их быстрое развитие привело к формализации контроля доступа объектов/субъектов систем с ограничением доступа на следующие составляющие:

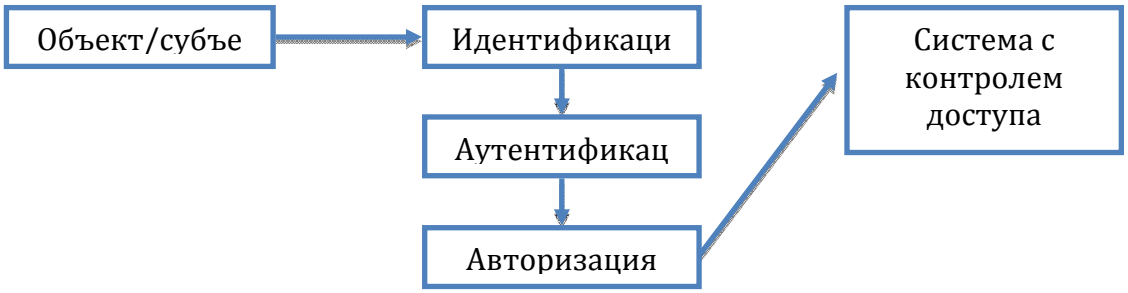

Рис.1 Составляющие контроля доступа объектов/субъектов систем с ограничением доступа

Как мы видим на Рис.1 – ввиду последовательности процессов, аутентификация является связующим процессом, подтверждая идентификацию объектов/субъектов и давая разрешение на начало процесса авторизации. Таким образом, можно сделать вывод, что процесс аутентификации крайне важен для безопасности информационных технологий.

В процессе цифровой аутентификации выделяют цифровые аутентификаторы и методы аутентификации.Лаборатория информационных технологий при Национальном институте стандартов и технологий США (ITLattheNIST, USA) предлагает федеральным агентствам США, внедряющим цифровую аутентификацию, NIST Special Publication 800-63B, Digital Identity Guidelines, Authentication and Lifecycl eManagement. В данной публикации[1] выделены уровни аутентификации, аутентификаторы, а также ранжирование аутентификаторов по “гарантированию” (Authenticator Assurance Levels). Перечень аутентификаторы и подходов к внедрению цифровой аутентификации предлагаемые ITLNISTне является исключительным, однако как документ описывающий современное представление и использование цифровой аутентификации NIST.SP.800-63b вполне приемлем для целей данного анализа, такую же структуру предлагает і стандарт ISO/IEC 29115:2013[2].

Для анализа предлагаются следующие типы аутентификаторов: пароль/PIN, секретные вопросы, внеполосные устройства (OutOfBand, OOB), однофакторные OTP(OneTimePassword, одноразовый пароль) устройства (1Ф OTP устройства), многофакторные OTP устройства (МФ OTP устройства), однофакторное криптографическое ПО (1Ф криптографическое ПО), однофакторное криптографическое устройство (1Ф криптографическое устройство), многофакторное криптографическое ПО (МФ криптографическое ПО), многофакторное криптографическое устройство (МФ криптографическое устройство); и следующие виды факторов: знание (пароль, PIN, личные данные, последовательности), владение (устройство), свойство (биометрия).

В таблице 1 проанализированы аутентификаторы с ранжированием по критериям стоимости внедрения/владения системой цифровой аутентификации с каждым из видом аутентификаторов, стойкости к компрометации и быстроты/удобства использования.

Таблица 1

	Стоимость			Стойкость к компрометации	Быстрота/удобство использования
	Стоимость внедрения	Стоимость владения	Итого		
Пароль/PIN	1	5	6	1	10
Секретные вопросы	2	2	4	2	7
Внеполосные устройства	2	2	4	3	5
1Ф OTP устройства	8	2	10	4	4
МФ OTP устройства	8	2	10	6	3
1Ф криптографическое ПО	7	3	10	6	5
1Ф криптографическое устройство	9	4	13	9	3
МФ криптографическое ПО	7	4	11	8	5
МФ криптографическое устройство	10	5	15	10	3

(где 1 – минимально, 10 – максимально)

Также хочется отметить, что критерий простоты/удобства использования субъектом цифровой аутентификации очень важен, так как это значительно влияет на человеческий фактор в работе информационной системы и его игнорирование способно нивелировать все предпринятые меры по улучшению информационной безопасности[3].

Основным инструментом цифровой аутентификации являются факторы, следует обратить внимание на возможности подверженности факторов зловредным действиям. Фактор знания: может быть подобран, угадан, подсмотрен, разглашен, получен незаконным путем. Фактор владения – может быть потерян, сломан, украден, скопирован. Фактор свойства – может быть подделан.

Далее следует обратить внимание на методы цифровой аутентификации: однофакторная, многофакторная, двухфакторная и многоканальная

аутентификации. Многофакторная аутентификация является экспансивным развитием однофакторной аутентификации, двухфакторная аутентификация является поэтапным метолом аутентификации, многоканальная аутентификация не имеет достаточно глубоких исследований и реализация и в некоторых источниках ее приравнивают к многофакторной как носителя фактора владения.

На текущий момент можно выделить три направления развития цифровой аутентификации:

1. Развитие стандартов и протоколов цифровой аутентификации (OAuth[4], OpenID[5], OpenIDConnect[5], WebAuth[6])и использование доверенных провайдеров аутентификации (Google, Microsoft, Facebook)[11].

2. Двухфакторная аутентификация[7,10].

3. Развитие аутентификаторов[8,13,14].

Из вышеизложенного можно сделать следующие выводы: ввиду отсутствия оптимального баланса стоимость/стойкость существует большой запрос на улучшение процесса аутентификации. Решением удовлетворения этого запроса может быть появление новых вариантов аутентификаторов, методов аутентификации, новых подходов к организации аутентификационного процесса. Уязвимости факторов аутентификации также вызывают необходимость в оптимизации процессов цифровой аутентификации. Также, особо хочется отметить, что во многих случаях субъектом цифровой аутентификации является человек, что привносит во весь процесс человеческий фактор, т.е. новым решениям желательно уменьшать риски человеческого фактора. Идеальным решением было бы наличие аутентификатора сочетающего все три фактора цифровой аутентификации, сосредоточенных в субъекте процесса, для взаимной компенсации недостатков.

Литература:

1. NIST Special Publication 800-63B // National Institute of Standards and Technology. – 2017.

2. Information technology — Security techniques — Entity authentication assurance framework: ISO/IEC 29115:2013 // International Organization for Standardization (ISO). – 2013.

3. The current state of Authentication: We have a password problem / Article / Drew Thomas . – 2016.

4. The OAuth 2.0 / Standard description / IETF. – 2012.

5. OpenID Specification / Official site / OpenID Foundation. – 2014.

6. WebAuth / W3C recommendations / W3C. – 2019.

7. Two-factor authentication / Article / Bruce Shneider / Communications in ACM. - 2005.

8. Методи біометрічної автентифікаціїї користувачів інформаційних систем за їх клавіатурним та крукписним почерком: Автореферат/ Висоцька О.О. / Київ. - 2019.

9. Аудит та управління інцидентами інформаційної безпеки: навч. посіб. / [Корченко О.Г., Гнатюк С.О., Казмірчук С.В. таін.]. – К.:Центрнавч.-наук. танаук.-пр. виданьНАСБУкраїни, 2014. – 190 с.

10 Authentication in web applications: master dissertation / Patrick Cervicek. – 2009

11. Модель и методика многомодальной аутентификации пользователя автоматизированной системы: диссертация / Никитин В.В. – 2018

12.Asynchronous Challenge-Response Authentication Solution Based on Smart Card in Cloud Environment/ Conference paper / Guifen Zhao, Ying Li, Liping Du, Xin Zhao / IEEE. – 2015

13. Multi-level authentication technique for accessing cloud services / Conference paper / H ADinesha, V K Agrawal / IEEE. – 2012

14. The Adoption of Single Sign-On and Multifactor Authentication in Organisations: A Critical Evaluation Using TOE Framework / Article / Marise-Marie D'Costa-Alphonso. – 2010

УДК 621.395.7

КІБЕРБЕЗПЕКА ТА ЗАХИСТ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Касьяненко Д.І.
аспірант ПВНЗ «Європейський університет»
yoobao7000@gmail.com

Анотація. *Теза присвячена теоретичним аспектам кібербезпеки та захису критичної інформаційної інфраструктури*

Кібербезпека з давньогрецької мови "кібер" (уряд або управління). сукупність умов, що забезпечують гарантовану захищеність усіх складових елементів інформаційних систем від максимального числа загроз і небажаних впливів на фізичному, фінансовому, емоційно-психічному, духовно-освітньому, політичному і професійному рівнях впливу або негативних наслідків у разі здійснення помилок, при пошкодженнях, аваріях, нещасні випадки, а також іншої шкоди в кіберпросторі, що вважається небажаним збитком.

Принципами в основі кібербезпеки є нагальний підхід в сфері кібербезпеки виражається у вигляді багаторівневого захисту, що охоплює комп'ютери, мережі, програми або дані, які необхідно убезпечити. Співробітники, робочі процеси і технології повинні доповнювати один одного в організаціях, щоб забезпечити ефективний захист від кібератак а також користувачі повинні розуміти і дотримуватися основних принципів інформаційної безпеки, такі як вибір надійних та складних паролів, уважне ставлення до вкладень в електронних листах а також резервне копіювання даних.