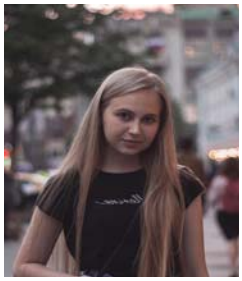
на данный момент невозможно прежде всего из-за того, что интеллектуальный капитал в целом и часть его составляющих не отвечают критериям признания в качестве объекта бухгалтерского учета в соответствии с Международным стандартом финансовой отчетности «Нематериальные активы», а именно: идентифицируемость и подконтрольность [5]. В процессе подготовки подобного стандарта также могут возникнуть сложности, связанные с многообразием подходов и методик оценки, однако нельзя сказать, что хоть одна из них полностью лишена недостатков и дает стопроцентно достоверные результаты. Сложность также заключается и в том, что нет единого научного подхода к определению и составу компонентов интеллектуального капитала.

Вне всяких сомнений, интеллектуальный капитал является стратегически важной составляющей любого бизнеса. Он влияет на экономические результаты деятельности организации и генерирует ее стоимость, поэтому его учет и оценка необходимы, но на данный момент это полноценно возможно лишь в рамках управленческого учета. На мой взгляд, целесообразно разработать комбинированную систему оценки интеллектуального капитала в рамках деятельности хозяйствующих субъектов, для которых очевидно его влияние на формирование стоимости. Как правило, это компании крупного и среднего бизнеса, занятые информационным или высоконаучным производством. Для подобных организаций важно формировать отчет об интеллектуальном капитале с выделением отраженных и не отраженных в финансовой отчетности элементов, создающих конкурентное преимущество, генерирующих стоимость компании и приносящих им экономические выгоды.

Список литературы

1. Федеральный закон от 29.07.1998 N 135-ФЗ (ред. от 03.08.2018) «Об оценочной деятельности в Российской Федерации».
2. Приказ Минэкономразвития России от 20.05.2015 N 297 «Об утверждении Федерального стандарта оценки «Общие понятия оценки, подходы и требования к проведению оценки (ФСО N 1)».
3. Приказ Минэкономразвития России от 20.05.2015 N 299 (ред. от 06.12.2016) «Об утверждении Федерального стандарта оценки «Требования к отчету об оценке (ФСО N 3)».
4. «Международный стандарт финансовой отчетности (IFRS) 13 «Оценка справедливой стоимости» (введен в действие на территории Российской Федерации Приказом Минфина России от 28.12.2015 N 217н) (ред. от 11.07.2016).
5. «Международный стандарт финансовой отчетности (IAS) 38 «Нематериальные активы» (введен в действие на территории Российской Федерации Приказом Минфина России от 28.12.2015 N 217н) (ред. от 30.10.2018) (с изм. и доп., вступ. в силу с 01.01.2019)
6. Головина Е.Ю. Интеллектуальные методы для создания систем поддержки принятия решений [Электронный ресурс]: учебное пособие/ Головина Е.Ю.— Электрон. текстовые данные.— М.: Издательский дом МЭИ, 2011.— 104 с
7. Петрухина Е.В. Роль интеллектуального капитала в обеспечении инновационного развития предприятий // В сборнике «Проблемы развития инновационно-креативной экономики». — 2010 — с. 356-361. —
8. Оценка стоимости нематериальных активов и интеллектуальной
9. собственности / Козырев А.Н., Макаров В.Л. – М.: Интерреклама, 2003. – 352 с.
10. Валдайцев С. В. Оценка интеллектуальной собственности: учебник. – М.: Экономика, 2009.
11. Быкова А. А. Влияние интеллектуального капитала на результаты деятельности компании // Вестник С.-Петерб. ун-та. Сер. Менеджмент. 2011. №1.
12. Ивлиева Н. Н. Оценка стоимости нематериальных активов и интеллектуальной собственности // М., Московская финансово-промышленная академия. 2006.
13. Самусенко С. А. Интеллектуальный капитал как объект учета: новые аспекты // Международный бухгалтерский учет. 2014. № 42.
14. https://ru.wikipedia.org/
15. https://www.sveiby.com/

ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ ЭФФЕКТИВНОСТИ ПАРОЛЬНОЙ ЗАЩИТЫ



Усоева Алёна Сергеевна
студентка 2 курса специальности «Веб-технологии», направление «Информатика и вычислительная техника» Московского политехнического университета

Шабайкина Алена Алексеевна
студентка 2 курса специальности «Веб-технологии», направление «Информатика и вычислительная техника» Московского политехнического университета

Бритвина Валентина Валентиновна
Кандидат педагогических наук, доцент кафедры «Инфокогнитивные технологии» Московского политехнического университета.

Аннотация: *В статье рассматривается вопрос о необходимости грамотного подбора парольной защиты и предлагаются рекомендации по увеличению ее эффективности.*

Ключевые слова: *пароль, безопасность, уязвимость, несанкционированный доступ, защита*

Abstract: *The need of correct password security and some ways to increase the effeciency of such kind of security are considered in this article.*

Keywords: *password, cyber security, vulnerability, unauthorized access*

Введение. Пароль - комбинация цифр, букв и знаков, защищающая данные от несанкционированного доступа. С древних времен люди использовали этот способ для обеспечения безопасности. Так, например, римские военные командиры контролировали, кто входит в расположение подразделения путем проверки пароля, который было необходимо называть часовым [1].

В современном мире функция защиты от несанкционированного доступа все так же актуальна. Пароли используются везде: в электронной почте, банковских счетах, социальных сетях и т.д. К сожалению, многие пользователи не осознают, что ненадежная комбинация символов не обеспечивает безопасность персональных данных, а отсутствие подобной защиты делает конфиденциальную информацию уязвимой для взлома.

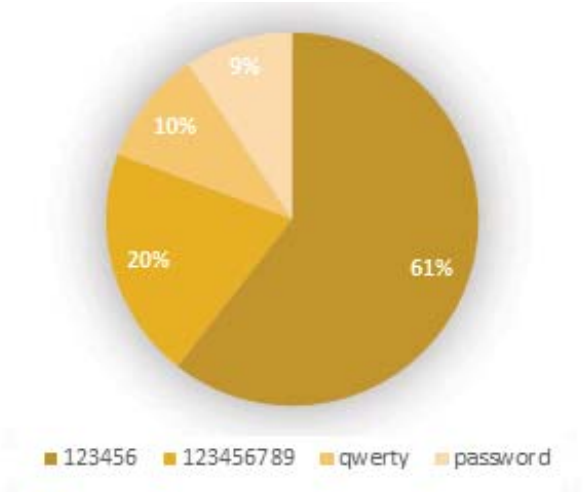


Рис.1. Самые ненадежные пароли за 2019 г.

В 2019 году национальный центр кибербезопасности Великобритании назвал список самых ненадежных паролей мира [2]. Некоторые из них представлены на рис.1.

Цели исследования: разработать практические рекомендации по обеспечению надежности парольной защиты

Задачи исследования:

- Осветить проблему необходимости эффективной парольной защиты
- Разработать практические рекомендации по составлению надежных паролей

Результаты исследования

В современном мире все большую популярность набирает миф о том, что частая смена пароля является весомой профилактикой при борьбе со взломами. Многие крупные корпорации требуют от своих сотрудников регулярного обновления комбинации символов с целью увеличения безопасности. К сожалению, этот способ не является эффективным, а скорее даже служит причиной к упрощению взлома, ведь частая смена пароля влечет за собой ухудшение его качества и надежности. Сейчас к паролю имеются два требования. С одной стороны, он должен быть эффективным, а с другой легко запоминающимся.

Совместить эти два качества непросто, поэтому кажется, что достаточно придумать и выучить одну надежную комбинацию и использовать ее для всех сервисов. К сожалению, данный способ также не является правильным, ведь нередко случается утечка информации. Таким образом, взломав один из сервисов, на котором используется ваш пароль, хакер получает доступ ко многим другим. Чтобы сохранить конфиденциальность данных и обеспечить защиту от несанкционированного доступа, необходимо использовать надежные комбинации символов. Далее речь пойдет о правильном составлении таких комбинаций.

Практические рекомендации по составлению пароля

Пароль является надежным, если соответствует двум основным принципам, а именно:

1. В комбинации использованы как можно более разнообразные символы (что обеспечивает паролю наименьшую предсказуемость)
2. Значительная длина пароля

Стоит также отметить, что эти качества способны компенсировать друг друга: вы можете не использовать символы вида «%», «#», «&» или разные регистры, но сделать ваш пароль длиннее.

Для каждого сервиса или сайта используйте свой уникальный пароль, чтобы не дать злоумышленнику получить вашу конфиденциальную информацию из всех источников сразу.

Надежный пароль совсем не обязательно должен представлять собой случайную комбинацию символов. Несмотря на то, что такие пароли, безусловно, оправданы с точки зрения безопасности, не всегда удается быстро и легко запоминать их. Именно поэтому стоит составить комбинацию, которую просто выучить, но длиннее (12 символов и более). Более того, стоит руководствоваться тем, что пароль может быть сложным на вид, но совершенно простым для взлома и хищения ваших персональных данных.

Как правило, зная правильные подходы и методы, пользователь может запомнить любую комбинацию букв и знаков. Наиболее эффективным является ассоциативный метод, например:

1. Возьмите фразу (строку из песни, цитату из книги, реплику из фильма и т.д.), которая является значимой для вас
2. Выпишите первые буквы первых пяти слов
3. Между каждой буквой вставьте один специальный символ

Дополнив данную комбинацию, вы можете генерировать другие исключительные и единственные в своем роде пароли

Чтобы запомнить по одному паролю для каждого сайта, используйте первое слово, которое ассоциируется у вас с данным сервисом, в составляемом вами пароле. (Если о социальной сети «Вконтакте» вам напоминает синий цвет, тогда вы можете взять слово «blue»)

Кроме того, обезопасить свои данные поможет двухфакторная аутентификация, а точно не забыть придуманные комбинации различные менеджеры паролей [3].

Вывод: Таким образом, на основе проведенных исследований, можно сделать вывод о том, что обеспечение надежности паролей является актуальной задачей современности. Придерживаясь описанных в работе методов и рекомендаций, пользователь сможет обезопасить свою персональную информацию и не дать злоумышленникам получить доступ к ней.

Рис.2. Пример составления парольной защиты.

Список литературы

1. Сухова А.Р., Гатиятуллин Т.Р. К вопросу о безопасности парольной защиты. Наука, техника и образование. 2016. №1 (19). С. 82-84.
2. Карпов П.С. Названы пароли, которые легче всего взломать. Федерал пресс. 22 апреля 2019 года.
3. Статья «Ошибочное понимание ИТ-безопасности: пароли» [Электронный ресурс] – Режим доступа: https://www.kaspersky.ru/