6. Введение в криптографию / Под ред. В.В.Ященко. – СПб.: Питер, 2001. – 288 с.

7. По Э. Золотой жук // В кн.: Американская новелла, М.: ГИХЛ. 1958. – С. 54-83.

8. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах. – М.: Горячая Линия-Телеком, 2001. – 148 с.

В.А. Белов, Д.В. Бобров, З.Ф. Камальдинова, А.А. Каштанов, В.С. Милов

КОНЦЕПЦИЯ СИСТЕМЫ ГАРАНТИРОВАННОЙ ИДЕНТИФИКАЦИИ ЛИЧНОСТИ ПОЛЬЗОВАТЕЛЯ В СЕТИ

(Самарский государственный технический университет)

Мы живём в том веке, когда новыми информационными технологиями никого не удивишь. Люди из разных уголков планеты свободно общаются между собой, при этом обмениваясь фотографиями или видеофайлами. Сейчас сложно представить, как мы будем жить без Интернета, ведь именно с его помощью все люди получают нужную для себя информацию.

Но чем больше мы полагаемся на Интернет, тем острее стоит вопрос защиты данных, которые мы туда вносим. Пароль для хакеров уже давно считается самым слабым местом. Такие простые методы как полный перебор (Брутфорс), перехват через открытую точку Wi-fi и банальное подглядывание дают злоумышленнику возможность с легкостью получить доступ к вашей конфиденциальной информации.

И именно поэтому следует разработать другие, более надежные, способы идентификации в сети.

Актуальность исследования. В эпоху бурно развивающихся информационных технологий и масштабности распространённости использования различных сервисов и служб, крайне важно развивать и совершенствовать системы защиты информации. Одной из важнейших задач теории защиты информации является идентификация пользователя в сети.

Данная проблема затрагивает каждого пользователя, так как каждый человек не хочет утечки собственных данных и для их защиты требуется выбрать наиболее рациональный и безопасный способ распознавания пользователя в сети. С каждым днем актуальность данной проблемы будет расти прямо пропорционально развитию информационных технологий.

Цель работы: провести исследования существующих способов идентификации пользователей в сети. Выбрать самый быстрый, эффективный и безопасный способ путем сравнения достоинств и недостатков каждого из метода.

Задачи, поставленные для достижения цели:

– изучить виды идентификации пользователей в сети;

– изучить плюсы и минусы каждого из способа идентификации пользователя в сети и составить таблицу, наглядно показывающую достоинства и недостатки каждого из метода;

– изучить возможности внедрения, распространения и роста каждого способа идентификации;

– на основе полученных данных выбрать наиболее эффективный и безопасный способ идентификации в сети.

Идентификация — это присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов [1]. Идентификация является защитным механизмом, который применяется в сфере обеспечения информационной безопасности при взаимодействии пользователей и ИС.

Идентификация личности в сети Интернет необходима:

1. С целью взаимодействия с другими гражданами (общение в социальных сетях, на форумах, в новостных порталах и т.д.) для получения информации о пользователе Интернета из открытых источников.

2. Для выявления лиц, совершивших какие-либо мошеннические или противоправные деяния.

3. Целью предоставления государственных услуг или получения ими возможности совершения каких-либо правоотношений.

В первом случае строгая идентификация пользователей является не обязательной, а в большей степени добровольной процедурой. Можно создать такой инструмент, который позволял бы идентифицировать человека по одним персональным данным, например, дата рождения, номер документа, удостоверяющего личность, не раскрывая их при этом широкому круг лиц.

Во втором случае идентификация в сети Интернет имеет ряд отличий от классической теории криминалистической идентификации и требует отдельного изучения.

Особое значение проблема идентификации личности приобретает в процессе предоставления государственных, муниципальных и банковских услуг в электронном виде, в результате которого появляется необходимость по представлению гражданам и органам государственной и муниципальной власти инструмента для безопасной идентификации посредством сети Интернет.

Статистика распространения биометрии. В целях получения более обширных данных в данной области мы обратились к исследованию компании Comparitech, которая изучила больше 50 стран на предмет использования и защиты персональных данных. Их интересовало, как собираются и хранятся биометрические данные (см. рисунок 1).

На этом основании каждой стране присуждались баллы (максимум 25). Чем выше балл у страны, тем обширнее и жестче ведется сбор биометрических данных. В каждой изученной исследователями стране биометрия используется в банкинге. Во многих странах также ведется сбор биометрических данных иностранцев. Хотя биометрические данные признаны чрезвычайно чувствительной информацией, во многих странах допускается их повсеместное исполь-

зование. Более того, в большинстве стран используются или тестируются камеры видеонаблюдения с функцией распознавания лиц [2].

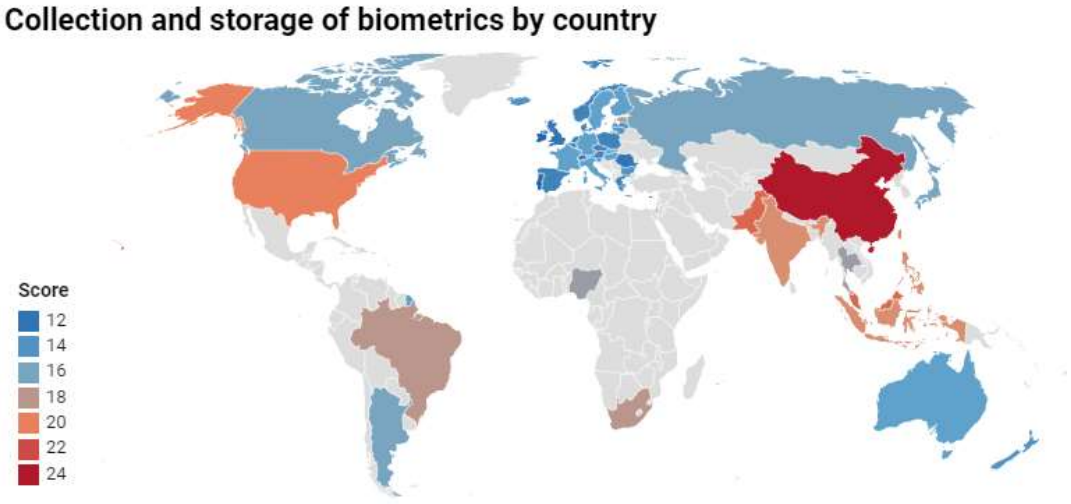

Рисунок1 - Статистика внедрения и сбора биометрических данных в разных странах

Как показало исследование, в целом по Европе дела с защитой биометрических данных обстоят лучше, чем за ее пределами. По словам специалистов, это связано с действием в Евросоюзе «Общего регламента по защите данных» (GDPR).

Также нам бы хотелось рассмотреть российский биометрический рынок в период с 2019 по 2022 год. По результатам исследования исследования J'son & Partners Consulting. В данном проекте приняли участие больше 40 экспертов. Российский рынок сейчас находится в стадии большего развития, чем мировой. Доля России в мировом объеме рынка постоянно продолжает расти (см. рисунок 2).

Исследования самого удобного и безопасного способа идентификации в сети мы решили провести по нескольким критериям:

1. Стоимость.
2. Скорость развития способа.
3. Безопасность.
4. Доверие пользователя.
5. Трудоемкость внедрения.

Сравнение будет проходить по десятибалльной системе. Каждому способу будет проставлена оценка по каждому критерию, где десять — это максимальный балл. В итоге будет выбран наиболее подходящий способ аутентификации. Оценивание критериев проводилось экспертами с кафедры информационной безопасности СамГТУ. И, основываясь на согласованной оценке экспертов, можно сделать вывод о наиболее безопасном и приемлемом способе идентификации пользователей.

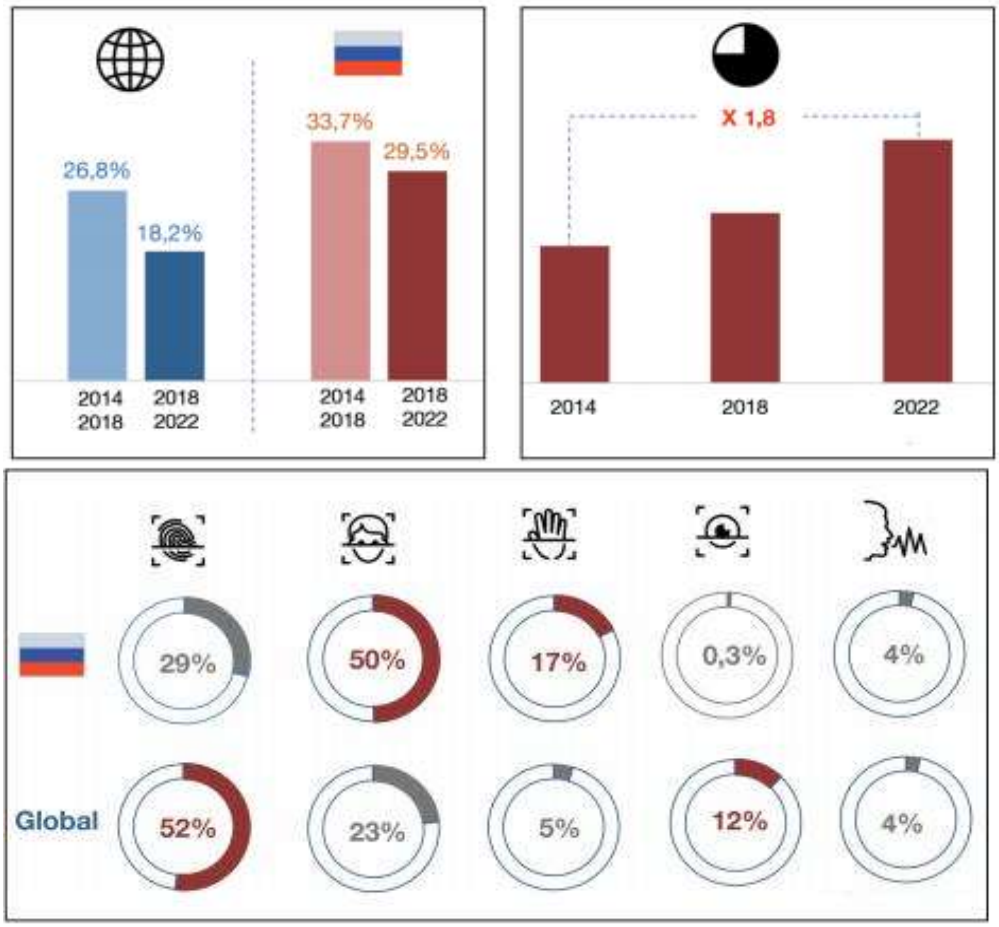

Рисунок 2 – Структура мирового и российского рынка биометрических технологий

Для наиболее точного выбора метода идентификации, было осуществлено разделение критериев по подгруппам, где каждая подгруппа имела свою степень важности.

1. Первая группа важности – Безопасность, стоимость изготовления.
2. Вторая группа важности – Доверие пользователя, скорость развития способа.
3. Третья группа важности – Трудоемкость внедрения.

Расчёты были произведены с помощью метода аналитической иерархии Томаса Саати.

Вывод

Все вышеперечисленные виды идентификации обладают своими преимуществами и недостатками. В ходе исследования самым эффективным и надёжным методом гарантированной идентификации личности пользователя в Сети является биометрия. Она показала наивысший балл в скорости развития и безопасности, что является основополагающими критериями для надежного и востребованного метода идентификации. Хоть и такие привычные способы идентификации как пароль, PIN-код и другие являются эффективными, но они не имеют возможностей развиваться дальше. В век бурно развивающихся инновационных технологий человечеству нужны более простые, эффективные и безопасные методы идентификации в сети как биометрия. В итоге можно уви-

деть, что самыми оптимальными вариантами являются такие биометрические методы идентификации пользователей как «По отпечатку пальцев» и «По венозному рисунку ладони». Они являются не слишком дорогими, но достаточно эффективными методами.

Литература

1. Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения». - М.: ГТК РФ, 1992. - 13 с.

2. Биометрическая идентификация [Электронный ресурс]/ российский интернет-портал и аналитическое агентство. URL: https://www.tadviser.ru/index.php/Статья:Биометрическая_идентификация_(мировой_рынок)#.

Д.С. Баканов

ПОСТРОЕНИЕ МОДЕЛИ ДЛЯ ПРЕДСКАЗАНИЯ ВРЕДОНОСНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

(Самарский университет)

Индустрия вредоносного программного обеспечения (ПО) продолжает расти. По оценкам лаборатории Касперского, лишь за один месяц 2020 года совершено свыше 10 млн. заражений [1]. И эта цифра продолжает расти.

Задача построения модели машинного обучения (МО), которая могла бы предсказать то, что ЭВМ в ближайшее время может быть заражена, была сформулирована компанией Microsoft на ресурсе Kaggle [2].

Данные представленные компанией Microsoft представляют таблицу (рисунок 1) с различными признаками (переменная в названии столбца таблицы). Исходом (признак, который надо предсказать) является переменная HasDetections, которая принимает значение 1 – данная машина заражена, 0 – иначе.

	MachineIdentifier	ProductName	EngineVersion	...	Wdft_IsGamer	Wdft_RegionIdentifier	HasDetections
0	0000028988387b115f69f31a3bf04f09	win8defender	1.1.15100.1	...	0.0	10.0	0
1	000007535c3f730efa9ea0b7ef1bd645	win8defender	1.1.14600.4	...	0.0	8.0	0
2	000007905a28d863f6d0d597892cd692	win8defender	1.1.15100.1	...	0.0	3.0	0
3	00000b11598a75ea8ba1beea8459149f	win8defender	1.1.15100.1	...	0.0	3.0	1
4	000014a5f00daa18e76b81417eeb99fc	win8defender	1.1.15100.1	...	0.0	1.0	1

Рисунок 9 – Внешний вид таблицы с данными

В данной таблице, как можно видеть из рисунка 1, каждый признак имеет разный тип данных. На рисунке 2 представлено распределение признаков по следующим типам значений: