УДК 004

НЕКОТОРЫЕ ПРОБЛЕМЫ, СВЯЗАННЫЕ С ФАКТОРАМИ АУТЕНТИФИКАЦИИ, И НЕОБХОДИМОСТЬ ВЫРАБОТКИ НОВЫХ ФАКТОРОВ АУТЕНТИФИКАЦИИ

Лемешко Д.В.

Московский государственный технический университет им. Н.Э. Баумана
Москва, Российская Федерация

Аннотация. Актуальность данной статьи заключается в том, что на протяжении долгого времени продолжают использовать три фактора аутентификации: фактор знания, фактор владения и фактор свойства (биометрические особенности индивида). Тем самым, эти три фактора начинают утрачивать свою уникальность и оригинальность, что негативно сказывается на состоянии защищенности информационных систем. Поэтому, крайне важно выработать новые факторы аутентификации.
Ключевые слова: аутентификация, факторы аутентификации, угрозы и риски.

SOME ISSUES CONNECTED WITH AUTHENTICATION FACTORS AND THE NECESSITY TO DEVELOP NEW AUTHENTICATION FACTORS

Lemeshko D.

Bauman Moscow State Technical University
Moscow, Russia

Abstract. The relevance of this article is about the fact that for a long time we continue to use three authentication factors: the knowledge factor, the possession factor and the characteristic factor (biometric features of the individual). Thus, these three factors begin to lose their uniqueness and originality, which negatively affects the state of security of information systems. Therefore, it is crucial to develop new authentication factors.
Key words: authentication, authentication factors, threats and risks.

Адрес для переписки: Лемешко Д.В., 2-я Бауманская ул., 5, стр.1, г. Москва 105005, Российская Федерация
e-mail: lemeshkodiana@yandex.ru

Введение. В наши дни безопасная передача данных должна быть продумана до мелочей. Пользователи должны быть уверены в том, что полученная информация не была модифицирована, осталась конфиденциальной и обеспечивается гарантия доступа авторизованным пользователям. Соответственно, чтобы стать авторизованным пользователем, необходимо пройти процедуру аутентификации. Здесь могут возникнуть риски и угрозы, связанные с основными факторами аутентификации, такими как: фактор знания, фактор владения и фактор свойства.

Возникающие угрозы и риски. Фактор знания: субъект доступа должен знать определенную информацию [1]. Значит, субъект доступа должен знать, например, пин-код или пароль. При этом могут возникать следующие угрозы и риски (табл. 1).

Таблица 1. Возникающие угрозы и риски

Угроза	Риск
1) непреднамеренное разглашение пароля	Риск пропуска злоумышленника далее в систему (в случае 2FA/MFA) или возможность прочтения злоумышленником конфиденциальных данных (в случае однофакторной аутентификации)
2) хищение пароля	
3) подбор пароля	
4) push-уведомления	

Фактор владения: субъект доступа должен обладать определенным предметом, содержащим аутентификационную информацию [1]. Значит, субъект доступа должен владеть, например, смарт-картой или USB-токеном. Отсюда возникают некоторые угрозы и риски (табл. 2).

Биометрический фактор: субъекту доступа должен быть свойственен определенный признак (характеристика), информация о котором (которой) используется при аутентификации [1]. Аутентифицироваться возможно при помощи отпечатков пальцев, радужной оболочки глаза, голоса и т.д. При биометрической аутентификации возникают следующие угрозы и риски (табл. 3).

Таблица 2. Возникающие угрозы и риски владения физическим устройством

Угроза	Риск
1) потеря физического устройства	1) не будет возможности аутентифицироваться, когда будет нужно; необходимо будет заявить об утере физического устройства и оформлять новое (риск новых затрат, риск покупки несертифицированного устройства)
2) кража физического устройства	2) злоумышленники могут попытаться ввести стандартный пин-код от производителя, чтобы вернуть доступ к физическому устройству; либо, посредством получения прав администратора, злоумышленники, зная пин-код администратора, смогут разблокировать физическое устройство

Таблица 3. Возникающие угрозы и риски биометрической аутентификации

Угроза	Риск
1) злоумышленник может обладать схожими биометрическими характеристиками с легальным пользователем	1) в систему проникнет нелегальный пользователь
2) возможность утери биометрических характеристик легальным пользователем	2) невозможность аутентификации и проведения последующих операций в системе

Тем самым, видно, что три фактора не являются надежными на 100%, так как присутствуют некоторые угрозы и риски. В процессе аутентификации может и повезти – пользователь может и не столкнуться ни с какими угрозами. Однако, всегда нужно продумывать любые сценарии развития событий.

Выработка новых факторов аутентификации. Действительно, многие пользователи и злоумышленники уже адаптировались к трем приведенным выше факторам аутентификации. Эти факторы не являются уже чем-то новым, рынок перенасыщен, обход этих факторов возможен.

Одним из таких новейших факторов мог бы стать фактор выбора. Гипотетически, фактор выбора должен обеспечить пользователя возможностью пройти аутентификацию любым удобным для него способом. Одним из преимуществ может быть то, что злоумышленник не будет знать заранее, что же выберет легальный пользователь в качестве аутентификационного фактора. Тем самым, минимизируются риски и устранятся угрозы, связанные с процессом аутентификации.

Еще одним из факторов мог бы стать фактор, основанный на анонимных блокчейн-протоколах. Анонимные блокчейн-протоколы должны позволить легальному пользователю скрыть процесс аутентификации для того, чтобы злоумышленник не был осведомлен о действиях легального лица. По итогу, угрозы и риски сводятся на нет.

Соответственно, выработка новых аутентификационных факторов поспособствует усилению состояния защищенности передаваемых данных, также легальный пользователь будет знать, что он будет защищен от различных нападок, пользователь сможет выбрать любой из факторов, через который он захочет провести аутентификацию, и, наконец, снизятся риски и устранятся угрозы.

Литература

1. Защита информации. Идентификация и аутентификация. Общие положения : ГОСТ Р 58833-2020

2. Digital Identity Guidelines. Authentication and Lifecycle Management : NIST SP 800-63B, 2017.

3. Information Technology – Security Techniques – Entity Authentication Assurance Framework : ISO/IEC 29115-2:2018, 2018.

УДК 534.87

АКУСТИКА И ЗВУК. ИЗМЕРИТЕЛЬНЫЕ МИКРОФОНЫ КАК ЧАСТЬ СИСТЕМЫ ДЛЯ ИЗМЕРЕНИЯ УРОВНЯ ЗВУКОВОГО ДАВЛЕНИЯ

Линкевич О.С.[1], Гуревич В.Л.[2]

[1]РУП «Белорусский государственный институт метрологии»
[2]Белорусский национальный технический университет
Минск, Республика Беларусь

Аннотация. Понимать что такое акустика, уровень звукового давления и как работают звуковые волны очень важно. Шумовое загрязнение окружающей среды – одна из актуальнейших научно-технических проблем акустической экологии и является мировой проблемой. Решением этой проблемы является контроль шумовых характеристик воздушной акустики, электроакустических параметров звуковопроизводящих устройств и прочее. Одним из средств этого контроля являются измерительные микрофоны в составе шумомера.

Ключевые слова: звук, уровень звукового давления, реверберация, измерительные микрофоны.

ACOUSTICS AND SOUND. MEASURING MICROPHONES AS A PART OF THE SOUND PRESSURE LEVEL MEASUREMENT SYSTEM

Linkevich O.[1], Hurevich V.[2]

[1]Belarusian State Institute of Metrology
[2]Belarusian National Technical University
Minsk, Belarus

Abstract. It is very important to understand what acoustics and sound pressure levels are, and how sound waves work. Noise pollution of the environment is one of the most pressing scientific and technical problems of acoustic ecology and this problem is global. The solution to this problem is controling the noise characteristics of air acoustics, electro-acoustic parameters of sound-emitting devices, etc. One of the means of this control are measuring microphones as part of a sound level meter.

Key words: sound, sound pressure level, reverberation, measurement microphones.

Адрес для переписки: Линкевич О.С., пр. Независимости, 65, г. Минск 220113, Республика Беларусь
e-mail: oleg.linkevicg99@yandex.ru

Звук и звуковое давление. Изучением звука занимается акустика. Акустика описывает генерацию, распространение и отражение звука, а также механические основы этих явлений.

Звук – это колебания, или механическое возмущение, в упругих средах. Магнитуду этих колебаний называют уровнем звукового давления, а колебания, которые воспринимаются ухом, –