

3.2.1. Гигиена
(медицинские науки)

УДК 613: 004
doi: 10.17021/2021.2.3.21.25

РАЗРАБОТКА СПОСОБА ОЦЕНКИ НОВЫХ ИНФОРМАЦИОННЫХ РИСКОВ В СОВРЕМЕННЫХ УСЛОВИЯХ

Ирина Александровна Молодцова¹, Людмила Петровна Сливина²

^{1,2} Волгоградский государственный медицинский университет, Волгоград, Россия.

¹irina.molodtsova@gmail.com

²gigienafuv@gmail.com

Аннотация. В работе рассмотрен способ оценки рисков. Представлен алгоритм анализа информационных рисков с использованием методов нечеткой логики. Представлена характеристика новой угрозы — сублиминальное воздействие. Приведены особенности реализации этапов оценки риска сублиминального воздействия. Предложена методика, которая позволяет учитывать биофизиологические особенности человека и технические показатели информационной системы. Рассмотрен пример реализации оценки риска с использованием программного пакета fuzzyTECH. Даны общие рекомендации по применению методики

Ключевые слова: риск, факторы риска, информация, здоровье, сублиминальное воздействие, угроза сублиминального воздействия.

Для цитирования: Молодцова И.А., Сливина Л.П. Разработка способа оценки новых информационных рисков в современных условиях // Прикаспийский вестник медицины и фармации. 2021. Т. 2, № 3. С. 21–25.

DEVELOPMENT OF A METHOD FOR ASSESSING NEW INFORMATION RISKS IN MODERN CONDITIONS

Irina A. Molodtsova¹, Lyudmila P. Slivina²

^{1,2} Volgograd State Medical University, Volgograd, Russia

¹irina.molodtsova@gmail.com

²gigienafuv@gmail.com

Abstract. The paper considers the method of risk assessment. An algorithm for analyzing information risks using fuzzy logic methods is presented. The characteristic of a new threat — subliminal impact—is presented. The features of the implementation of the stages of assessing the risk of subliminal exposure are given. A method is proposed that allows us to take into account the bio-physiological characteristics of a person and the technical indicators of the information system. An example of implementing a risk assessment using the fuzzyTECH software package is considered. General recommendations for the use of the method are given.

Key words: risk, risk factors, information, health, subliminal exposure, threat of subliminal exposure.

For citation: Molodtsova I.A., Slivina L.P.: Development of a method for assessing new information risks in modern conditions // Caspian Journal of Medicine and Pharmacy. 2021 : 2 (3): 21–25 (In Russ.).

Введение. В условиях цифровой экономики возрастает роль технических источников информации [2, 8, 12, 14]. Согласно отчету Digital в 2020 году в мире более 5 миллиардов человек пользуются мобильными телефонами, 80 % пользователей интернета от 16 до 64 лет ежемесячно играют в видеоигры больше 30 минут в день. В нашей стране 81 % жителей (118 миллионов) пользуются интернетом в среднем ежедневно по 7 часов 17 минут в день.

Восприятие человеком цифровой информации происходит с помощью органов чувств. При этом, около 90 % всей поступающей информации воспринимается посредством зрительного и слухового анализаторов (70 % и 20 % соответственно) [3, 7, 13].

Использование цифровых технологий позволяют с одной стороны повысить оптические и акустические характеристики информации, с другой — порождают новые угрозы и риски [5, 9, 10].

Более 60% воспринимаемой информации не фиксируется сознанием, а представляет набор факторов сублиминального воздействия. Риск реализации новой угрозы требует оценки.

Характеристика понятия «сублиминальное воздействие» представлена в научных исследованиях Дюк В.А., Кравчик М.Р., Сенкевич Ю.И. Научно-методические основы влияния информационных воздействий на индивидуальное и массовое сознание, психические процессы, технологии формирования поведения отдельных лиц и групп населения, «подталкивание» их к принятию требуемых решений, информационно-психологической безопасности изучали Кара-Мурза С.Г., Грачёв Г.В., Щекотихин В.М., Бухарин С.Н., Цыганов В.В., Модестов С.А., Панарин И.Н., Лисичкин В.А., Шелепин Л.А., Манойло А.В., Почепцов Г.Г., Расторгуев С.П., Новиков Д.А., Чхартишвили А.Г., Губанов Д.А., Караяни А.Г., Волконогов Д.А., Волковский Н.Л., Минаев В.А., Овчинский А.С., Скрыль С.В., Тростянский С.Н., Прокофьев, В.Ф., Шейнов В. П., Баришполец В.А., Воронцова Л.В., Фролов, Д.Б., Крысько В.Г., Шеремет И.А., Семашко К.В.; средства и способы предъявления неосознаваемой акустической, зрительной и комбинированной информации - Макаренко С.И., Смирнов Г.Е., Крылова И.А., Чернышенко В.В., Орловский М.А., Остапенко И.Н., Костюк А.В., Епанешников Н.М., Королев А.В., Королева В.В. и др.; влияние подпороговых визуальных стимулов - Bargh A., Pietromonaco P., Gilbert D. T., Nixon J. G., Krosnick J. A., Betz A. L., Jussim L. J., Spencer S. J., Fein S., Wolfe C.T.; включенных в фильм образов на эмоции и степень тревожности - Костандова Э.А., Kay W.B., Nisbett R. E., Wilson T. D.; активизация сублиминальными стимулами бессознательных конфликтов - Бабаева Ю.Д., Войскунский А.Е., Евстигнеева Ю.М., Иванов М.С.

Однако существуют противоречия. Одним из компонентов информационной системы является человек. Используемые способы оценки рисков не учитывают его характеристик, как субъекта информационной системы на которого направлено воздействие [1, 4, 7, 11].

Цель: разработать способ оценки риска сублиминального воздействия аудиовизуальной информации, которая позволит учитывать био-физиологические особенности субъекта и технические показатели информационной системы.

Материалы и методы исследования. Для реализации цели и задач исследования применяли методы системного анализа, математические модели оценки рисков. Использование нечеткой логики позволило включить в модель оценки риска как физиологические характеристики состояния организма человека, так и показатели программно-технического устройства, являющегося носителем информации. Реализацию практической работы проводили с использованием среды разработки приложений Visual Studio, в системе Rand Model Designer; программного пакета fuzzyTECH. Вычисления выполнены с использованием компьютерной программы «SPSS 16.0 for Windows».

Результаты исследования и их обсуждение. Внешние условия, социальная и правовая среда могут влиять на восприятие аудиовизуальной информации. Сублиминальное (подпороговое) воздействие определяется как изменение аффективных и когнитивных реакций человека, вызванное внешними стимулами различной модальности, слишком малыми по интенсивности или длительности для того, чтобы быть осознанными [6, 11, 12].

Угроза сублиминального воздействия информации — это совокупность условий и факторов, создающих возможность неосознанного изменения аффективных и когнитивных реакций человека малыми по интенсивности или длительности внешними стимулами, реализованных с помощью ИТ-технологий. Для оценки риска сублиминального воздействия мы выделили несколько блоков: факторы спонтанного сублиминального воздействия, био-физиологические особенности человека, физические характеристики информационной системы.

Существует много способов оценки рисков информационного воздействия много. Однако они в основном базируются на характеристиках источника воздействия и техническими параметрами устройств. Работы по оценке сублиминального риска фрагментарны.

При этом не учитываются био-физиологические параметры организма человека, как субъекта информационной системы, сочетанное действие и взаимовлияние разных физических параметров программно-технического устройства, которые могут быть потенциальными факторами риска нарушения здоровья. В настоящее время особый интерес при оценке рисков в информационных системах представляет оценка риска воздействия информации на уровне подсознания. В этой связи нами был

разработан способ комплексной оценки риска реализации новой угрозы сублиминального воздействия.

Основой сублиминального воздействия являются спонтанные сублиминальные факторы информационного контента, среди которых можно выделить несколько групп: базовые (страх, бомбардирование информацией, слушание авторитетов), переменные (элементы виртуального воспроизведения - реклама, кинофильмы, онлайн игры); управления (характеристики среды обитания, стандарты микросоциума, средства коммуникации).

Второй блок параметров, который использовались для формирования базы знаний нечеткой модели оценки риска сублиминального воздействия информации составили физические факторы: длина и частота волны, освещенность (E), яркость (L), площадь поверхности экрана монитора (S), контраст объекта с фоном (k), коэффициент пульсации освещенности (k_E), показатель ослепленности (P_o), скорость передачи данных (B), удельная поглощенная мощность (SAR), угол наклона экрана монитора, цветовая температура и другие.

В качестве био-физиологических параметров были определены анатомо-физиологические особенности органов речеобразования, слухового и зрительного анализаторов для оценки разборчивости и видимости аудиовизуального контента.

При сублиминальном воздействии акустической информации разборчивость речи является интегральной оценкой речевого сигнала в соответствии с международным стандартом ISO/TR 4870, ГОСТ 25902-83, ГОСТ 51061-97, ANSI S3.2.

Для характеристики разборчивости речи при оценке акустических свойств определяем: AI (Articulation Index) — индекс артикуляции; % ALcons (Percentage Articulation Loss of Consonants) — процент артикуляционных потерь согласных; STI (Speech Transmission Index) — индекс передачи речи; SII (Speech Intelligibility Index) – индекс разборчивости речи; RASTI (Rapid Speech Transmission Index) – быстрый индекс передачи речи [0;1]. Разборчивость зависит от 2 характеристик: громкость звука (дБ) – можем измерить в диапазоне [-10; +130], частота звука (Гц) – можем измерить в диапазоне частот [125; 8000].

Видимость – это возможность полного или частичного наблюдения объекта. Условия видимости: характеристики объекта – расстояние до объекта (удаление), размер, яркость, освещенность, цвет, фон; состояния атмосферы; физиологические особенности глаза – угол, острота зрения.

Оценку рисков сублиминального воздействия информации проводим поэтапно на основе принципов системного анализа:

- 1 - выделение блоков, их элементов, параметров и критериев оценки;
- 2 - определение иерархии частей блоков;
- 3 - выделение качественных и количественных свойств элементов блоков, доминирующие связи;
- 4 - анализ характеристик элементов блоков на основе положений нечеткой логики (формирование базы правил, фаззификация входных переменных, операции блока логического заключения, дефаззификация выходных переменных, определяем результаты, которые могут считаться улучшением и их критерии);
- 5 этап - оценка риска.

В результате анализа получена математическая модель оценки риска сублиминального воздействия аудиовизуальной информации, которая имеет вид:

$$S_{CE}(d) = \sum_i [P_{DPi} \cdot S_{DPi}(d)]$$

где S_{CE} – индекс риска сублиминального воздействия, P_{DP} – вероятность наступления сублиминального воздействия; S_{DP} – индекс риска блоков факторов.

Для оценки рисков при комплексном воздействии используем критерии оценки индекса риска сублиминального воздействия аудиовизуальной информации: 0 - 0,2 – низкий; 0,3 - 0,5 – средний; 0,6 - 0,8 – высокий; 0,9 - 1,0 – очень высокий.

Визуализация модель оценки рисков при комбинированном вводе представлена на рисунке 1.

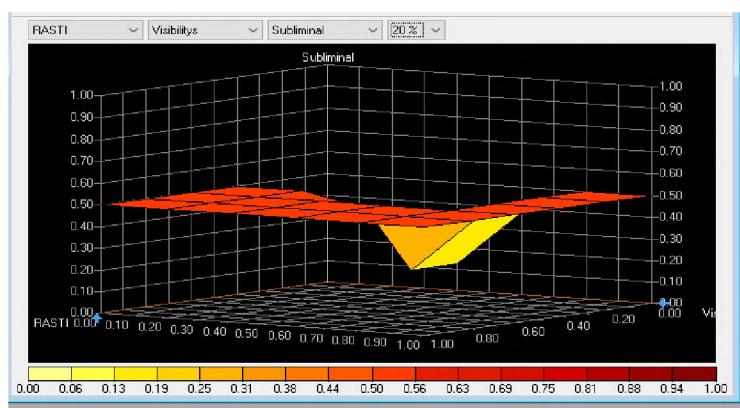


Рис. 1 – Визуализация оценки риска по индексу сублиминального воздействия

В полученной модели можно изменять параметры характеристик и получать в автоматическом режиме оценку риска, что является существенным преимуществом разработанного способа.

Выводы или заключение. Предложенный способ позволяет оценить риск с учетом комплекса воздействующих факторов, в том числе учитывать био-физиологические особенности человека, технические показатели информационной системы и их изменения, разработать персонализированные мероприятия по профилактике возможного негативного влияния информации.

Список источников

1. Аралбаев Т.З., Абрамова Т.В. Особенности оперативного поиска информации о сетевом трафике по первичным данным аномальной активности компьютерной сети // Информационное противодействие угрозам терроризма. 2015. №24. С.76–81.
2. Костюк А.В., Еланешников Н.М. Информационная безопасность личности как нравственная проблема // материалы межведомственной научно-практической конференции «Актуальные проблемы военной педагогики и психологии в системе военных образовательных организаций». Санкт-Петербург, 2020. С. 350–357.
3. Неизвестный С.И. Социально-психологические проблемы перехода к цифровой экономике / С.И. Неизвестный // Ученые записки РГСУ. 2018. Т. 17, № 2(147). С. 5–13.
4. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». М., 2018. 97с.
5. Аудиовизуальные технологии воздействия на подсознание. URL : <https://psi-technology.net/articles/technology/audiovizualnye-tehnologii-vozdjeystviya-na-podsoznanie.php>
6. Информационно-психологическая и когнитивная безопасность // под ред. И.Ф. Кефели, Р.М. Юсупова. СПб.: ИД «Петрополис», 2017. 287 с.
7. Петренко С. А., Ступин Д. Д. Национальная система раннего предупреждения о компьютерном нападении: научная монография / под ред. С.Ф. Боева. Иннополис: Афина, 2017. 440 с.
8. Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации № 646 от 05.12.2016г. URL : <http://www.scrf.gov.ru/documents/6/5.html>
9. Макаренко С.И. Информационное противоборство и радиоэлектронная борьба в сетевых войнах начала XXI века. Научно-технические технологии, 2017. 549 с.
10. Максимова Е.А., Бердник М.В., Молодцова И.А. Информационная гигиена как фактор предотвращения последствий Z-цифровизации // Вестник УрФО. Безопасность в информационной сфере. №3 (29). 2018. С.67–73.
11. Аносов Р.С., Аносов С.С., Шахалов И.Ю. Концептуальная модель анализа риска безопасности информационных технологий // Вопросы кибербезопасности. 2020. №2(36). С. 2–10.
12. ГОСТ Р 8.827-2013 ГСИ. Метод измерения и определения индекса цветопередачи источников излучения. М.: Стандартинформ, 2014. 16 с.
13. Молодцова И.А., Сливина Л.П., Максимова Е.А. Методологические основы информационной гигиены. Волгоград, 2020. 132с.
14. Дюк В.А., Кравчик М.Р., Сенкевич Ю.И. Обнаружение сублиминального визуального воздействия на человека средствами интеллектуального анализа данных электроэнцефалографических измерений // Вестник Санкт-Петербургского университета. 2015. сер.10. вып.1. С.83–93.

References

1. Aralbaev T.Z., Abramova T.V. Features of online search for information about network traffic based on primary data of anomalous activity of a computer network. *Informatsionnoe protivodeystvie ugrozam = Information countermeasures against terrorism threats*. 2015; (24): 76–81. (In Russ.).
2. Kostyuk A.V., Epaneshnikov N.M. Personal information security as a moral problem. Materials of the interdepartmental scientific-practical conference "Actual problems of military pedagogy and psychology in the system of military educational organizations." St. Petersburg. 2020: 350–357. (In Russ.).
3. Neizvestnyy S.I. Socio-psychological problems of the transition to the digital economy. *Scientific notes of the RSSU*. 2018; 17, 2(147): 5–13. (In Russ.).
4. Federal Law of July 27, 2006 No. 149-FZ "On Information, Information Technologies and Information Protection". Moscow. 2018: 97. (In Russ.).
5. Audiovisual technologies for influencing the subconscious. URL : <https://psi-technology.net/articles/technology/audiovizualnye-tehnologii-vozdejstviya-na-podsoznanie.php> (In Russ.).
6. Informational psychological and cognitive security. Ed. I.F. Kefeli, R.M. Yusupov. St. Petersburg: Publishing House "Petropolis". 2017: 287. (In Russ.).
7. Petrenko S. A., Stupin D. D. National computer attack early warning system: scientific monograph. Ed. S.F. Boeva. Innopolis: Athena. 2017: 440. (In Russ.).
8. Information security doctrine of the Russian Federation. Approved by the Decree of the President of the Russian Federation, no. 646 dat. 05.12.2016. URL : <http://www.scrf.gov.ru/documents/6/5.html> (In Russ.).
9. Makarenko S.I. Information confrontation and electronic warfare in network-centric wars at the beginning of the XXI century. *Naukoemkie tekhnologii = High technology*. 2017: 549. (In Russ.).
10. Maksimova E.A., Berdnik M.V., Molodtsova I.A. Information hygiene as a factor in preventing the consequences of Z-digitalization. *Vestnik UrFO. Bezopasnost' v informatsionnoy sfere = Bulletin of the Ural Federal District. Information security*. 2018; 3 (29): 67–73. (In Russ.).
11. Anosov R.S., Anosov S.S., Shakhlov I.Yu. Conceptual model of information technology security risk analysis. *Voprosy kiberbezopasnosti = Cybersecurity issues*. 2020; 2(36): 2–10. (In Russ.).
12. GOST R 8.827-2013 GSI. Method for measuring and determining the color rendering index of radiation sources. M.: Standortinform. 2014: 16. (In Russ.).
13. Molodtsova I.A., Slivina L.P., Maksimova E.A. Methodological foundations of information hygiene. Volgograd. 2020: 132. (In Russ.).
14. Dyuk V.A., Kravchik M.R., Senkevich Yu.I. Detection of subliminal visual impact on a person by means of intelligent analysis of electroencephalographic measurement data. *Vestnik Sankt-Peterburgskogo universiteta = Bulletin of St. Petersburg University*. 2015, series 10, issue 1: 83–93. (In Russ.).

Информация об авторах

И.А. Молодцова, кандидат медицинских наук, доцент кафедры профильных гигиенических дисциплин, Волгоградский государственный медицинский университет, Волгоград, Россия.

Л.П. Сливина, доктор медицинских наук, профессор, заведующая кафедрой профильных гигиенических дисциплин, Волгоградский государственный медицинский университет, Волгоград, Россия.

Information about the authors

I.A. Molodtsova, Cand. Sci. (Med.), Docent, Volgograd State Medical University, Volgograd, Russia.

L.P. Slivina, Dr. Sci. (Med.), Professor, Volgograd State Medical University, Volgograd, Russia.*

* Статья поступила в редакцию 11.06.2021; принята к публикации 21.08.2021.
The article was submitted 11.06.2021; accepted for publication 21.08.2021.