ISSN 2306-0417

www.aurora-group.eu
www.nbpublish.com

Вопросы безопасности

AURORA Group s.r.o.
nota bene

Выходные данные

Номер подписан в печать: 04-04-2024
Учредитель: Даниленко Василий Иванович, w.danilenko@nbpublish.com
Издатель: ООО <НБ-Медиа>
Главный редактор: Шульц Владимир Леопольдович, доктор философских наук, cona01@yandex.ru
ISSN: 2409-7543
Контактная информация:
Выпускающий редактор - Зубкова Светлана Вадимовна
E-mail: info@nbpublish.com
тел.+7 (966) 020-34-36
Почтовый адрес редакции: 115114, г. Москва, Павелецкая набережная, дом 6А, офис 211.
Библиотека журнала по адресу: http://www.nbpublish.com/library_tariffs.php

Publisher's imprint

Number of signed prints: 04-04-2024
Founder: Danilenko Vasiliy Ivanovich, w.danilenko@nbpublish.com
Publisher: NB-Media ltd
Main editor: Shul'ts Vladimir Leopol'dovich, doktor filosofskikh nauk, cona01@yandex.ru
ISSN: 2409-7543
Contact:
Managing Editor - Zubkova Svetlana Vadimovna
E-mail: info@nbpublish.com
тел.+7 (966) 020-34-36
Address of the editorial board : 115114, Moscow, Paveletskaya nab., 6A, office 211 .
Library Journal at : http://en.nbpublish.com/library_tariffs.php

Редсовет

Батьковский Александр Михайлович – доктор экономических наук, АО Центральный научно-исследовательский институт экономики, систем управления и информации «Электроника» , советник генерального директора, 127299, Москва, ул. Космонавта Волкова, 12, batkovskiy_a@instel.ru

Чирун Сергей Николаевич – доктор политических наук, доцент, профессор, Кемеровский государственный университет, институт истории и международных отношений, 650000, г. Кемерово, ул. Красная, 6, Sergii-Tsch@mail.ru

Быков Илья Анатольевич – доктор политических наук, доцент Санкт-Петербургский государственный университет, Кафедра связей с общественностью в политике и государственном управлении, 199004, Россия, Санкт-Петербург область, г. Санкт-Петербург, ул. 1-Я линия, 26, оф. 509

Зайцев Александр Владимирович - доктор политических наук, кандидат философских наук, доцент, Костромской государственный университет, кафедра философии, культурологии и социальных коммуникаций Россия, Кострома, улица Дзержинского, 17/11, остромская область, г. Кострома, ул. Дзержинского, д. 17. aleksandr-kostroma@mail.ru

Акопов Григорий Леонидович - доктор политических наук, Московский государственный технический университет гражданской авиации Ростовский филиал, Заведующий кафедрой социально-экономических дисциплин, Южно-Российский институт РАНХиГС, профессор кафедры политологии и этнополитики, 344009, Россия, Ростовская область, г. Ростов-на-Дону, ул. Шолохова, 262в, оф. 1, ag078@icloud.com

Деметрадзе Марине Резоевна - доктор политических наук, Российский научно-исследовательский институт культурного и природного наследия имени Д. С. Лихачёва , главный научный сотрудник, институт мировых цивилизации , профессор, Российская академия народного хозяйства и государственной службы при Президенте РФ (РАНХиГС) , профессор, 117292, Россия, г. москва, ул. нахимовский проспект дом 48 кв.96, 48, demetradze1959@mail.ru

Шашкова Анна Владиславовна - доктор политических наук, Московский государственный институт международных отношений, профессор, 125299, Россия, г. Москва, пр-д Вернадского, 76, ауд. 3024, a.shashkova@inno.mgimo.ru

Судоргин Олег Анатольевич – доктор политических наук, профессор, МАДИ, первый проректор, профессор по кафедре МАДИ «История и культурология», 125319. Москва, Ленинградский пр., дом 64, оф. 250. sudorgin@madi.ru

Волох Владимир Александрович - доктор политических наук, профессор кафедры государственного управления и политических технологий Института государственного управления и права Государственного университета управления. Рязанский проспект, 99, г. Москва, Россия, 109542; E-mail: v.volokh@yandex.ru

Попова Ольга Валентиновна - доктор политических наук, профессор, заведующая кафедрой политических институтов и прикладных политических исследований Санкт-Петербургского государственного университета. Университетская набережная, 7-9. г. Санкт-Петербург, Россия, 199034. E-mail: politinstitute2010@mail.ru

Боташева Асият Казиевна - доктор политических наук, профессор кафедры журналистики, медиакоммуникаций и связей с общественностью Института международных

отношений ФГБОУ ВО "Пятигорский государственный университет". 357532, Ставропольский край, г. Пятигорск, пр. Калинина, 9. E-mail: ab-ww@mail.ru

Литвинова Татьяна Николаевна - доктор политических наук, Одинцовский филиал Федерального государственного автономного образовательного учреждения высшего образования "Московский государственный институт международных отношений (университет) Министерства ино, профессор кафедры регионального управления и национальной политики, 143005, Россия, Московская область, г. Одинцово, ул. Чикина, 9, кв. 99, tantin@mail.ru

Сыченко Елена Вячеславовна – PhD (Университет Катании, Италия), доцент кафедры трудового права Санкт-Петербургского государственного университета, 199034, г. Санкт-Петербург, 22 линия В.О., 7. e.sychenko@mail.ru

Нарутто Светлана Васильевна – доктор юридических наук, профессор кафедры конституционного и муниципального права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА), 125993. г. Москва, ул. Садовая-Кудринская 9, svetanarutto@yandex.ru

Толстолуцкий Владимир Юрьевич – доктор медицинских наук, профессор, Нижний Новгород, ННГУ, юридический факультет, кафедра уголовного права и процесса, 603950, г. Нижний Новгород, пр. Гагарина, 23, tolvlad@yandex.ru

Краснянская Татьяна Максимовна – доктор психологических наук, профессор, профессор кафедры общей, социальной психологии и истории психологии, Московский гуманитарный университет 111395, г. Москва, ул. Юности, 5 ktm8@yandex.ru

Кравец Игорь Александрович – доктор юридических наук, профессор, заведующий кафедрой теории истории государства и права, конституционного права Новосибирский национальный исследовательский государственный университет, 630090, Новосибирская обл., г. Новосибирск, ул. Пирогова, 1, kravigor@gmail.com

Николайчук Ольга Алексеевна – доктор экономических наук, профессор, Финансовый университет при Правительстве Российской Федерации, профессор Департамента экономической теории, 125993, Москва, ГСП-3, Ленинградский проспект, д. 49, 18111959@mail.ru

Гомонов Николай Дмитриевич – доктор юридических наук, профессор, Северо-Западный институт (филиал) Московского гуманитарно-экономического университета, декан юридического факультета, 183052, г. Мурманск, просп. Кольский, 51, Gomonov_Nikolay@mail.ru

Поляков Виктор Павлович – доктор педагогических наук, профессор, главный научный сотрудник лаборатории психолого-педагогического и учебно-методического обеспечения развития информатизации образования Центра информатизации образования Федерального государственного бюджетного научного учреждения «Институт управления образованием Российской академии образования», 105062, г. Москва, ул. Макаренко, д. 5/16, стр. 1Б, polvikpal@mail.ru

Ефименко Дмитрий Борисович – доктор технических наук, доцент по кафедре транспортной телематики, Московский автомобильно-дорожный государственный технический университет (МАДИ)», декан факультета логистики и общетранспортных проблем, заведующий кафедрой «Правовое и таможенное регулирование на транспорте» MADI, 125319. Москва, Ленинградский пр., дом 64, оф. 207л. ed2002@mail.ru

Беляева Галина Серафимовна – доктор юридических наук, профессор Белгороский государственный национальный исследовательский университет, кафедра административного и международного права, 308015, Россия, г. Белгород, ул. Победы, 85,

Лютикова Лариса Адольфовна - кандидат физико-математических наук, заведующая отделом Нейроинформатики и машинного обучения Институт прикладной математики и автоматизации Кабардино-Балкарского научного центра РАН – филиал Кабардино-Балкарского научного центра РАН (ИПМА КБНЦ РАН), 360000, Россия, Республика Кабардино-Балкария, г. Нальчик, ул. Шортанова, 89а Мобильный телефон: 89631664014

Мустафаев Арслан Гасанович – доктор технических наук, профессор, государственное автономное образовательное учреждение высшего образования "Дагестанский государственный университет народного хозяйства" Кафедра: Информационные технологии и информационная безопасность, 367015, Россия, Республика Дагестан, г. Махачкала, ул. Атаева, 5, каб. 4.5. Мобильный телефон: 89886361596

Черкасов Валерий Николаевич – доктор экономических наук, кандидат технических наук, Первый заместитель главного редактора научно-практического журнала «Информационная безопасность регионов», Саратовский социально-экономический институт (филиал) ФГБОУ ВПО «РЭУ им. Г. В. Плеханова», 410009, Россия, Саратовская область, г. Саратов, ул. Дачная, 30А, кв. 116, Мобильный телефон: 89173013484

Шульц Владимир Леопольдович — член-корреспондент Российской академии наук, заместитель президента Российской академии наук, доктор философских наук, директор Центра исследования проблем безопасности Российской академии наук, Председатель редакционного совета, главный редактор научного журнала (сетевого издания) «Вопросы безопасности». 119991, Россия, г. Москва, Ленинский проспект, 14

Махутов Николай Андреевич — член-корреспондент Российской академии наук, заместитель академика-секретаря Отделения энергетики, машиностроения, механики и процессов управления Российской академии наук. 119991, Россия, г. Москва, Ленинский проспект, 14

Юсупов Рафаэль Мидхатович — член-корреспондент Российской академии наук, директор Санкт-Петербургского института информатики и автоматизации Российской академии наук. 199178, Россия, г. Санкт-Петербург,14 линия, дом 39

Боярски Марек — доктор права, профессор, ректор Вроцлавского университета (Польша, г. Вроцлав). University Of Wroclaw, Pl. Uniwersytecki, 1, 50-137. Wroclaw, Poland

Гропп Вальтер — доктор права, профессор, руководитель профессуры, Юстус Либих — Университет Гиссен, (Германия, г. Гиссен). Raum 219, 2. Etage, Licher Stra?e, 76. 35394, Giessen, Deutschland

Зибер Ульрих — доктор права, профессор, директор Института зарубежного и международного уголовного права. Макса Планка, (Германия, г. Фрайбург). Gunterstal str., 73, 79100 Freiburg i. Breisgau, Deutschland

Зинн Арндт — доктор права, профессор, руководитель Института экономического уголовного права Университета Оснабрюк, руководитель кафедры немецкого и европейского уголовного права и уголовного процесса, международного уголовного права и сравнительного правоведения (Германия, г. Оснабрюк). Universitat Osnabruck, Postfach 44 69, 49069 Osnabruck, Deutschland

Хинрих Юлиус — доктор права, профессор юридического факультета Гамбургского уверситета, Центр „Юридический диалог с развивающимися странами" по исследованиям гражданского права и хозяйственного права, координатор проекта ЕС "China-EU School of Law". Universitat Hamburg, Mittelweg. 177. 20148, Hamburg, Deutschland

Хэ Бинсун — доктор права, профессор, начальник Центра по изучению терроризма и организованной преступности, заместитель Начальника Центра по изучению уголовных законов, специальный консультант докторантов Политико-юридического университета Китая. 100088, КНР, г. Пекин, район Хайдянь, Ул. Ситучэнлу д.25.

Базарнова Юлия Генриховна - доктор технических наук, Профессор, Высшая школа биотехнологии и пищевых технологий, Санкт-Петербургский Политехнический университет Петра Великого.

Белозеров Валерий Владимирович - доктор технических наук, профессор, Донской государственный технический университет, Генеральный директор, ООО "НПТ Центр ОКТАЭДР".

Волков Вячеслав Дмитриевич - доктор технических наук, профессор, кафедра Электромеханических систем и электроснабжения, Воронежский государственный технический университет.

Гладков Игорь Александрович - доктор технических наук, член-корреспондент, Российская академия космонавтики им. К.Э. Циолковского, ведущий научный сотрудник, ФГУП Ордена Трудового Красного Знамени, Научно-исследовательский институт радио.

Кучкаров Захирджан Анварович - доктор экономических наук, кандидат технических наук, профессор, кафедра Концептуального анализа и проектирования, Московский физико-технический институт (государственный университет).

Пайсон Дмитрий Борисович - доктор экономических наук, кандидат технических наук, Директор Информационно-исследовательского центра, Объединенная ракетно-космическая корпорация.

Сычева Ольга Владимировна - доктор сельскохозяйственных наук, кандидат технических наук, профессор, кафедра технологии производства и переработки сельскохозяйственной продукции, Ставропольский государственный аграрный университет.

Зинкин Валерий Николаевич - доктор медицинских наук, ведущий научный сотрудник, Центральный научно-исследовательский институт ВВС Минобороны России.

Сукиасян Самвел Грантович - доктор медицинских наук, профессор, кафедра развития и прикладной психологии, Армянский государственный педагогический университет, заведующий, отделение реабилитации психического здоровья "Стресс", Медицинский реабилитационный центр "Артмед", заведующий, кафедра психического здоровья и психиатрии, Армянский медицинский институт.

Белинская Елена Павловна - доктор психологических наук, профессор, кафедра социальной психологии, Московский государственный университет имени М.В.Ломоносова.

Желински Мартин - доктор права, профессор, Конституционный трибунал Республики Польша (Constitutional Tribunal (Poland))Poland, 00-918 Warsaw, Al. J. Ch. Szucha 12a

Батурин Юрий Михайлович - доктор юридических наук, профессор МГУ им. М.И. Ломоносова, чл.-корр. РАН, директор Института истории естествознания и техники им. С.И.

Вавилова Российской академии наук (ИИЕТ РАН), 109012, РФ, Москва, Старопанский переулок, д. 1/5, ИИЕТ РАН

Новицкая Татьяна Евгеньевна - доктор юридических наук, профессор, Лауреат Государственной премии Российской Федерации, профессор кафедры истории государства и права юридического факультета Московского государственного университета имени М.В. Ломоносова.

Нижник Надежда Степановна - доктор юридических наук, кандидат исторических наук, профессор, профессор кафедры теории государства и права Санкт-Петербургского университета МВД России.

Редкоус Владимир Михайлович - доктор юридических наук, профессор, ведущий научный сотрудник сектора административного права и административного процесса ИГП РАН, профессор кафедры УДПООП ЦКШУ Академии управления МВД России. 119019 Москва, ул. Знаменка, д.10, E-mail: rwmmos@rambler.ru

Аюпова Зауре Каримовна - доктор юридических наук, Казахский национальный университет, профессор, 050020, Казахстан, г. Алматы, ул. ул.Тайманова, 222, кв. 16, zaure567@yandex.ru

Безверхов Артур Геннадьевич - доктор юридических наук, ФГАОУ ВО "Самарский национальный исследовательский университет имени академика С. П. Королева", Юридический институт, директор института; Кафедра теории и истории государства и права и международного права, заведующий кафедрой; Кафедра уголовного права и криминологии, профессор, 443011, Россия, Самарская область область, г. Самара, ул. академика Павлова, 1 Г, ауд. 209, bezverkhov-artur@yandex.ru

Беляева Галина Серафимовна - доктор юридических наук, Белгородский государственный национальный исследовательский университет, заведующий кафедрой административного права и процесса, 308503, Россия, Белгородская область, пос. Майский, ул. Агрономическая, 5, gala.belyaeva2014@yandex.ru

Васильев Алексей Михайлович - доктор исторических наук, федеральное государственное бюджетное образовательное учреждение высшего образования "Кубанский государственный университет" (ФГБОУ ВО «КубГУ»), профессор кафедры уголовного права и криминологии, федеральное государственное бюджетное образовательное учреждение высшего образования "Кубанский государственный университет" (ФГБОУ ВО «КубГУ»), профессор кафедры уголовного права и криминологии, 350072, Россия, Краснодарский край, г. Краснодар, ул. 2-й кадетский переулок, 12, 12, alexey771977@mail.ru

Глущенко Валерий Владимирович - доктор технических наук, Московский политехнический университет (работал с 01.09.2020,уволен по истеченю контракта 31.08.2021), профессор центра проектной деятельности (0,37 ставки), Российский университет транспорта (РУТ МИИТ) (уволен по истечению контракта 30.10.2019), профессор кафедры производственного менеджмента и кадрового обеспечения транспортного комплекса, Московский авиационный институт (уволен по собственному желанию в октябре 2012 года), профессор кафедры производственного менеджмента и маркетинга, 107564, Россия, Москва, г. Москва, ул. 1-я Гражданская,, д.101,, кв. 27, glu-valery@yandex.ru

Гомонов Николай Дмитриевич - доктор юридических наук, федеральное государственное бюджетное образовательное учреждение высшего образования «Мурманский арктический государственный университет», профессор кафедры юриспруденции, 183010, Россия, Мурманская область, г. Мурманск, ул. Халтурина, 7, оф. 10, Gomonov_Nikolay@mail.ru

Кобец Петр Николаевич - доктор юридических наук, Всероссийский научно-исследовательский институт Министерства внутренних дел Российской Федерации», главный научный сотрудник отдела научной информации, подготовки научных кадров и обеспечения деятельности научных советов Центра организационного обеспечения научной деятельности , 121069, Россия, г. Москва, ул. Поварская, д. 25, стр. 1, pkobets37@rambler.ru

Краснянская Татьяна Максимовна - доктор психологических наук, Московский гуманитарный университет, профессор кафедры общей,социальной психологии и истории психологии, 107207, Россия, г. Москва, ул. Уральская, 6, к.5., кв. 34, ktm8@yandex.ru

Кудратов Некруз Абдунабиевич - доктор юридических наук, Таджикский государственный университет коммерции, Декан факультета, 734061, Таджикистан, г. Душанбе, ул. Дехоти, 1/2, каб. 309, nek-kudratov@mail.ru

луговской Александр Михайлович - доктор географических наук, Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский государственный университет геодезии и картографии» (МИИГАиК), профессор кафедры географии факультета картографии и геоинформатики , 1090548, Россия, Московская область, г. Москва, ул. Шоссейная, 13, оф. 49, alug1961@yandex.ru

Мальцева Анна Васильевна - доктор социологических наук, Санкт-Петербургский государственный университет, доцент, ФГБНУ НИИ "Реестр экспертов научно-технической сферы при Министерстве образования и науки РФ", член реестра экспертов, ВЦИОМ, член Экспертно-консультативного совета , 194354, Россия, Санкт-Петербург, г. Санкт-Петербург, ул. Есенина, 12 к1, кв. 413, annamaltseva@rambler.ru

Мустафаев Арслан Гасанович - доктор технических наук, Дагестанский государственный университет народного хозяйства, Профессор, 367008, Россия, республика Дагестан, г. Махачкала, ул. Джамалутдина Атаева, 5, каб. 3.4, arslan_mustafaev@mail.ru

Овчаров Антон Олегович - доктор экономических наук, Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского», профессор кафедры бухгалтерского учета, главный научный сотрудник Центра макро и микроэкономики, 603135, Россия, г. Нижний Новгород, проспект Ленина, 45 корпус 3, кв. 47, anton19742006@yandex.ru

Пояркова Екатерина Васильевна - доктор технических наук, федеральное государственное бюджетное образовательное учреждение высшего образования «Оренбургский государственный университет», заведующий кафедрой механики материалов, конструкций и машин, 460018, Россия, Оренбургская область, г. Оренбург, проспект Победы, 13, ауд. 20.402, yarko.e@mail.ru

Редкоус Владимир Михайлович - доктор юридических наук, Федеральное

государственное бюджетное учреждение науки Институт государства и права Российской академии наук, ведущий научный сотрудник сектора административного права и административного процесса , Федеральное государственное казенное образовательное учреждение высшего образования «Академия управления Министерства внутренних дел Российской Федерации», Профессор кафедры управления деятельностью подразделений обеспечения охраны общественного порядка центра командно-штабных учений, 117628, Россия, г. Москва, ул. Знаменские садки, 1 корпус 1, кв. 12, rwmmos@rambler.ru

Сайфутдинов Тахир Исмаилджанович - доктор юридических наук, Кыргызско-Казахский университет, проректор по научной работе, Ошский государственный юридический институт, профессор кафедры уголовного права и процесса, 720072, Киргизия, г. Бишкек, ул. Тулебердиева, 80, saifutdinovt@bk.ru

Editorial collegium

Batkovsky Alexander Mikhailovich - Doctor of Economics, JSC Central Research Institute of Economics, Control Systems and Information "Electronics", Advisor to the General Director, 127299, Moscow, st. Cosmonaut Volkov, 12, batkovskiy_a@instel.ru

Chirun Sergey Nikolaevich – Doctor of Political Sciences, Associate Professor, Professor, Kemerovo State University, Institute of History and International Relations, 650000, Kemerovo, Krasnaya str., 6, Sergii-Tsch@mail.ru

Ilya A. Bykov – Doctor of Political Sciences, Associate Professor, St. Petersburg State University, Department of Public Relations in Politics and Public Administration, 199004, Russia, St. Petersburg region, St. Petersburg, 1st line str., 26, office 509

Zaitsev Alexander Vladimirovich - Doctor of Political Sciences, Candidate of Philosophical Sciences, Associate Professor, Kostroma State University, Department of Philosophy, Cultural Studies and Social Communications Russia, Kostroma, Dzerzhinsky Street, 17/11, Ostrom region, Kostroma, Dzerzhinsky Street, 17. aleksandr-kostroma@mail.ru

Akopov Grigory Leonidovich - Doctor of Political Sciences, Moscow State Technical University of Civil Aviation Rostov Branch, Head of the Department of Socio-Economic Disciplines, RANEPA South Russian Institute, Professor of the Department of Political Science and Ethnopolitics, 344009, Russia, Rostov region, Rostov-on-Don, Sholokhova str., 262b, office 1, ag078@icloud.com

Demetradze Marina Rezoevna - Doctor of Political Sciences, D. S. Likhachev Russian Research Institute of Cultural and Natural Heritage, Chief Researcher, Institute of World Civilizations, Professor, Russian Presidential Academy of National Economy and Public Administration (RANEPA), Professor, 48 Nakhimovsky Prospekt, Moscow, 117292, Russia sq.96, 48, demetradze1959@mail.ru

Anna Vladislavovna Shashkova - Doctor of Political Sciences, Moscow State Institute of International Relations, Professor, 76 Vernadsky Ave., Moscow, 125299, Russia, room 3024, a.shashkova@inno.mgimo.ru

Oleg A. Sudorgin – Doctor of Political Sciences, Professor, MADI, First Vice-rector, Professor at the Department of MADI "History and Cultural Studies", 125319. 64 Leningradsky Ave., office 250, Moscow. sudorgin@madi.ru

Volokh Vladimir Aleksandrovich - Doctor of Political Sciences, Professor of the Department of Public Administration and Political Technologies of the Institute of Public Administration and Law of the State University of Management. Ryazan Avenue, 99, Moscow, Russia, 109542; E-mail: v.volokh@yandex.ru

Popova Olga Valentinovna - Doctor of Political Sciences, Professor, Head of the Department of Political Institutions and Applied Political Studies of St. Petersburg State University. Universitetskaya embankment, 7-9. St. Petersburg, Russia, 199034. E-mail: politinstitute2010@mail.ru

Asiyat Kazievna Botasheva - Doctor of Political Sciences, Professor of the Department of Journalism, Media Communications and Public Relations of the Institute of International Relations of the Pyatigorsk State University. 357532, Stavropol Territory, Pyatigorsk, Kalinin Ave., 9. E-mail: ab-ww@mail.ru

Litvinova Tatiana Nikolaevna - Doctor of Political Sciences, Odintsovo Branch of the Federal State Autonomous Educational Institution of Higher Education "Moscow State Institute of International Relations (University) Ministry of Foreign Affairs, Professor of the Department of Regional Management and National Policy, 143005, Russia, Moscow region, Odintsovo, Chikina str., 9, sq. 99, tantin@mail.ru

Sychenko Elena Vyacheslavovna – PhD (University of Catania, Italy), Associate Professor of the Department of Labor Law of St. Petersburg State University, 199034, St. Petersburg, 22 line V.O., 7. e.sychenko@mail.ru

Narutto Svetlana Vasilyevna – Doctor of Law, Professor of the Department of Constitutional and Municipal Law of the Kutafin Moscow State Law University (MGUA), 125993. Moscow, Sadovaya-Kudrinskaya str. 9, svetanarutto@yandex.ru

Tolstolutsky Vladimir Yuryevich – Doctor of Medical Sciences, Professor, Nizhny Novgorod, UNN, Faculty of Law, Department of Criminal Law and Procedure, 23 Gagarin Ave., Nizhny Novgorod, 603950, tolvlad@yandex.ru

Krasnianskaya Tatiana Maksimovna – Doctor of Psychological Sciences, Professor, Professor of the Department of General, Social Psychology and History of Psychology, Moscow Humanitarian University 111395, Moscow, Yunosti str., 5 ktm8@yandex.ru

Igor Kravets – Doctor of Law, Professor, Head of the Department of Theory of the History of State and Law, Constitutional Law Novosibirsk National Research State University, 630090, Novosibirsk Region, Novosibirsk, Pirogova str., 1, kravigor@gmail.com

Nikolaichuk Olga Alekseevna – Doctor of Economics, Professor, Financial University under the Government of the Russian Federation, Professor of the Department of Economic Theory, 125993, Moscow, GSP-3, Leningradsky Prospekt, 49, 18111959@mail.ru

Nikolay Dmitrievich Gomonov – Doctor of Law, Professor, North-Western Institute (branch) Moscow University of Humanities and Economics, Dean of the Faculty of Law, 183052, Murmansk, ave. Kola, 51, Gomonov_Nikolay@mail.ru

Polyakov Viktor Pavlovich – Doctor of Pedagogical Sciences, Professor, Chief researcher of the Laboratory of Psychological, Pedagogical and Educational methodological support for the development of Informatization of Education of the Center for Informatization of Education of the Federal State Budgetary Scientific Institution "Institute of Education Management of the Russian Academy of Education", 105062, Moscow, Makarenko str., 5/16, p. 1B, polvikpal@mail.ru

Efimenko Dmitry Borisovich – Doctor of Technical Sciences, Associate Professor at the Department of Transport Telematics, Moscow Automobile and Road State Technical University (MADI), Dean of the Faculty of Logistics and General Transport Problems, Head of the Department "Legal and Customs Regulation in Transport" MADI, 125319. Moscow, Leningradsky ave., 64, office 207l. ed2002@mail.ru

Belyaeva Galina Serafimovna – Doctor of Law, Professor Belgorod State National Research University, Department of Administrative and International Law, 85 Pobedy Str., Belgorod, 308015, Russia,

Lyutikova Larisa Adolfovna - Candidate of Physical and Mathematical Sciences, Head of the Department of Neuroinformatics and Machine Learning Institute of Applied Mathematics and Automation of the Kabardino-Balkarian Scientific Center of the Russian Academy of Sciences –

branch of the Kabardino-Balkarian Scientific Center of the Russian Academy of Sciences (IPMA KBSC RAS), 360000, Russia, Republic of Kabardino-Balkaria, Nalchik, 89a Shortanova str. Mobile phone: eightyninebillionsixhundredthirtyonemillionsixhundredsixtyfourthousandfourteen

Mustafayev Arslan Hasanovich – Doctor of Technical Sciences, Professor, State Autonomous Educational Institution of Higher Education "Dagestan State University of National Economy" Department: Information Technology and Information Security, 367015, Russia, Republic of Dagestan, Makhachkala, Ataeva str., 5, office 4.5. Mobile phone: 89886361596

Cherkasov Valery Nikolaevich – Doctor of Economics, Candidate of Technical Sciences, First Deputy Editor-in-Chief of the scientific and practical journal "Information Security of Regions", Saratov Socio-Economic Institute (branch) of Plekhanov Russian University of Economics, 410009, Saratov region, Saratov, Dachnaya str., 30A, sq. 116, Mobile phone: 89173013484

Vladimir Leopoldovich Shultz — Corresponding Member of the Russian Academy of Sciences, Deputy President of the Russian Academy of Sciences, Doctor of Philosophy, Director of the Center for Security Research of the Russian Academy of Sciences, Chairman of the Editorial Board, editor-in-chief of the scientific journal (online publication) "Security Issues". 14 Leninsky Prospekt, Moscow, 119991, Russia

Makhutov Nikolay Andreevich — Corresponding Member of the Russian Academy of Sciences, Deputy Academician-Secretary of the Department of Energy, Mechanical Engineering, Mechanics and Management Processes of the Russian Academy of Sciences. 14 Leninsky Prospekt, Moscow, 119991, Russia

Yusupov Rafael Midhatovich — Corresponding Member of the Russian Academy of Sciences, Director of the St. Petersburg Institute of Informatics and Automation of the Russian Academy of Sciences. 199178, Russia, St. Petersburg, line 14, house 39

Boyarski Marek — Doctor of Law, Professor, Rector of the University of Wroclaw (Poland, Wroclaw). University Of Wroclaw, Pl. Uniwersytecki, 1, 50-137. Wroclaw, Poland

Gropp Walter — Doctor of Law, Professor, Head of the Professorship, Justus Liebig — University of Giessen, (Germany, Giessen). Raum 219, 2. Etage, Licher Stra?e, 76. 35394, Giessen, Deutschland

Sieber Ulrich — Doctor of Law, Professor, Director of the Institute of Foreign and International Criminal Law. Max Planck, (Germany, Freiburg). Gunterstal str., 73, 79100 Freiburg i. Breisgau, Deutschland

Zinn Arndt — Doctor of Law, Professor, Head of the Institute of Economic Criminal Law at Osnabr?ck University, Head of the Department of German and European Criminal Law and Criminal Procedure, International Criminal Law and Comparative Law (Germany, Osnabr?ck). Universitat Osnabruck, Postfach 44 69, 49069 Osnabruck, Deutschland

Hinrich Julius — Doctor of Law, Professor at the Faculty of Law of Hamburg University, Center for "Legal Dialogue with Developing Countries" on Civil Law and Business Law Studies, coordinator of the EU project "China-EU School of Law". Universitat Hamburg, Mittelweg. 177. 20148, Hamburg, Deutschland

He Bingsun is a Doctor of Law, Professor, Head of the Center for the Study of Terrorism and Organized Crime, Deputy Head of the Center for the Study of Criminal Laws, special consultant to doctoral students of the Political Law University of China. 100088, China, Beijing, Haidian district, Situchenglu str., 25.

Bazarnova Yulia Genrikhovna - Doctor of Technical Sciences, Professor, Higher School of Biotechnology and Food Technologies, Peter the Great St. Petersburg Polytechnic University.

Belozerov Valery Vladimirovich - Doctor of Technical Sciences, Professor, Don State Technical University, General Director, OOO "NPT Center OCTAHEDRON".

Vyacheslav D. Volkov - Doctor of Technical Sciences, Professor, Department of Electromechanical Systems and Power Supply, Voronezh State Technical University.

Gladkov Igor Aleksandrovich - Doctor of Technical Sciences, Corresponding Member, K.E. Tsiolkovsky Russian Academy of Cosmonautics, Leading Researcher, FSUE of the Order of the Red Banner of Labor, Radio Research Institute.

Zakhirjan Anvarovich Kuchkarov - Doctor of Economics, Candidate of Technical Sciences, Professor, Department of Conceptual Analysis and Design, Moscow Institute of Physics and Technology (State University).

Payson Dmitry Borisovich - Doctor of Economics, Candidate of Technical Sciences, Director of the Information and Research Center, United Rocket and Space Corporation.

Sycheva Olga Vladimirovna - Doctor of Agricultural Sciences, Candidate of Technical Sciences, Professor, Department of Technology of Production and Processing of Agricultural Products, Stavropol State Agrarian University.

Valery N. Zinkin - Doctor of Medical Sciences, Leading Researcher, Central Research Institute of the Air Force of the Ministry of Defense of Russia.

Sukiasyan Samvel Grantovich - MD, Professor, Department of Development and Applied Psychology, Armenian State Pedagogical University, Head, Department of Mental Health Rehabilitation "Stress", Medical Rehabilitation Center "Artmed", Head, Department of Mental Health and Psychiatry, Armenian Medical Institute.

Belinskaya Elena Pavlovna - Doctor of Psychological Sciences, Professor, Department of Social Psychology, Lomonosov Moscow State University.

Martin Zelinsky - Doctor of Law, Professor, Constitutional Tribunal of the Republic of Poland (Constitutional Tribunal (Poland))Poland, 00-918 Warsaw, Al. J. Ch. Szucha 12a

Baturin Yuri Mikhailovich - Doctor of Law, Professor of Lomonosov Moscow State University, Corresponding Member of the Russian Academy of Sciences, Director of the Institute of the History of Natural Science and Technology named after S.I. Vavilov of the Russian Academy of Sciences (IIET RAS), 109012, RF, Moscow, Staropansky Lane, 1/5, IIET RAS

Novitskaya Tatiana Evgenievna - Doctor of Law, Professor, Laureate of the State Prize of the Russian Federation, Professor of the Department of History of State and Law of the Faculty of Law of Lomonosov Moscow State University.

Nizhnik Nadezhda Stepanovna - Doctor of Law, Candidate of Historical Sciences, Professor, Professor of the Department of Theory of State and Law of the St. Petersburg University of the Ministry of Internal Affairs of Russia.

Redkous Vladimir Mikhailovich - Doctor of Law, Professor, leading researcher of the Sector of Administrative Law and Administrative Process of the IGP RAS, Professor of the Department of UDPOP of the CCSHU Academy of Management of the Ministry of Internal Affairs of Russia. 10 Znamenka str., Moscow, 119019, E-mail: rwmmos@rambler.ru

Ayupova Zaure Karimovna - Doctor of Law, Kazakh National University, Professor, 050020, Kazakhstan, Almaty, ul. Taimanova, 222, sq. 16, zaure567@yandex.ru

Bezverkhov Artur Gennadievich - Doctor of Law, Samara National Research University named after Academician S. P. Korolev, Law Institute, Director of the Institute; Department of Theory and History of State and Law and International Law, Head of the Department; Department of Criminal Law and Criminology, Professor, 443011, Russia, Samara Region, Samara region, akademika Pavlova str., 1 G, room 209, bezverkhov-artur@yandex.ru

Belyaeva Galina Serafimovna - Doctor of Law, Belgorod State National Research University, Head of the Department of Administrative Law and Procedure, 308503, Russia, Belgorod region, village Maysky, Agronomic str., 5, gala.belyaeva2014@yandex.ru

Vasiliev Alexey Mikhailovich - Doctor of Historical Sciences, Federal State Budgetary Educational Institution of Higher Education "Kuban State University" (FGBOU VO "KubGU"), Professor of the Department of Criminal Law and Criminology, Federal State Budgetary Educational Institution of Higher Education "Kuban State University" (FGBOU VO "KubGU"), Professor of the Department of Criminal Law and Criminology criminology, 350072, Russia, Krasnodar Territory, Krasnodar, ul. 2nd kadetskiy lane, 12, 12, alexey771977@mail.ru

Glushchenko Valery Vladimirovich - Doctor of Technical Sciences, Moscow Polytechnic University (worked from 01.09.2020, dismissed at the expiration of the contract on 31.08.2021), Professor of the Center for Project Activities (0.37 rate), Russian University of Transport (RUT MIIT) (dismissed at the expiration of the contract on 30.10.2019), Professor of the Department of Production Management and Personnel Support of the Transport Complex, Moscow Aviation Institute (dismissed at his own request in October 2012), Professor of the Department of Production Management and Marketing, 107564, Russia, Moscow, Moscow, 1st Grazhdanskaya str.,, 101,, sq. 27, glu-valery@yandex.ru

Nikolay Dmitrievich Gomonov - Doctor of Law, Federal State Budgetary Educational Institution of Higher Education "Murmansk Arctic State University", Professor of the Department of Jurisprudence, 7 Khalturina str., office 10, Murmansk, Murmansk Region, 183010, Russia, Gomonov_Nikolay@mail.ru

Kobets Pyotr Nikolaevich - Doctor of Law, All-Russian Research Institute of the Ministry of Internal Affairs of the Russian Federation, Chief Researcher of the Department of Scientific Information, Training of Scientific Personnel and Ensuring the activities of Scientific Councils of the Center for Organizational Support of Scientific Activity, 121069, Russia, Moscow, Povarskaya str., 25, p. 1, pkobets37@rambler.ru

Krasnianskaya Tatiana Maksimovna - Doctor of Psychological Sciences, Moscow Humanitarian University, Professor of the Department of General, Social Psychology and History of Psychology, 107207, Russia, Moscow, Uralskaya str., 6, room 5., sq. 34, ktm8@yandex.ru

Kudratov Nekruz Abdunabievich - Doctor of Law, Tajik State University of Commerce, Dean of the Faculty, 734061, Tajikistan, Dushanbe, 1/2 Dekhoti str., room 309, nek-kudratov@mail.ru

Lugovskoy Alexander Mikhailovich - Doctor of Geographical Sciences, Federal State

Budgetary Educational Institution of Higher Education "Moscow State University of Geodesy and Cartography" (MIIGAiK), Professor of the Department of Geography, Faculty of Cartography and Geoinformatics, 1090548, Russia, Moscow region, Moscow, Shosseynaya str., 13, office 49, alug1961@yandex.ru

Maltseva Anna Vasilyevna - Doctor of Sociology, St. Petersburg State University, Associate Professor, Research Institute "Register of Experts in the Scientific and Technical field under the Ministry of Education and Science of the Russian Federation", member of the Register of Experts, VTSIOM, member of the Expert Advisory Council, 194354, Russia, St. Petersburg, St. Petersburg, Yesenina St., 12 k1, sq. 413, annamaltseva@rambler.ru

Mustafayev Arslan Hasanovich - Doctor of Technical Sciences, Dagestan State University of National Economy, Professor, 367008, Russia, Republic of Dagestan, Makhachkala, Jamalutdin Atayev str., 5, office 3.4, arslan_mustafaev@mail.ru

Ovcharov Anton Olegovich - Doctor of Economics, Federal State Autonomous Educational Institution of Higher Education "National Research Nizhny Novgorod State University named after N.I. Lobachevsky", Professor of Accounting Department, Chief Researcher of the Center for Macro and Microeconomics, 603135, Russia, Nizhny Novgorod, Lenin Avenue, 45 building 3, sq. 47, anton19742006@yandex.ru

Ekaterina V. Poyarkova - Doctor of Technical Sciences, Federal State Budgetary Educational Institution of Higher Education "Orenburg State University", Head of the Department of Mechanics of Materials, Structures and Machines, 460018, Russia, Orenburg region, Orenburg, Pobedy Avenue, 13, room 20.402, yarko.e@mail.ru

Redkous Vladimir Mikhailovich - Doctor of Law, Federal State Budgetary Institution of Science Institute of State and Law of the Russian Academy of Sciences, Leading Researcher of the Sector of Administrative Law and Administrative Process, Federal State State Educational Institution of Higher Education "Academy of Management of the Ministry of Internal Affairs of the Russian Federation", Professor of the Department of Management of Public Order Units of the Center for Command and Controlstaff exercises, 117628, Russia, Moscow, Znamenskiye sadki str., 1 building 1, sq. 12, rwmmos@rambler.ru

Sayfutdinov Tahir Ismaildzhanovich - Doctor of Law, Kyrgyz-Kazakh University, Vice-Rector for Research, Osh State Law Institute, Professor of the Department of Criminal Law and Procedure, 720072, Kyrgyzstan, Bishkek, Tuleberdieva str., 80, saifutdinovt@bk.ru

Требования к статьям

Журнал является научным. Направляемые в издательство статьи должны соответствовать тематике журнала (с его рубрикатором можно ознакомиться на сайте издательства), а также требованиям, предъявляемым к научным публикациям.

Рекомендуемый объем от 12000 знаков.

Структура статьи должна соответствовать жанру научно-исследовательской работы. В ее содержании должны обязательно присутствовать и иметь четкие смысловые разграничения такие разделы, как: предмет исследования, методы исследования, апелляция к оппонентам, выводы и научная новизна.

Не приветствуется, когда исследователь, трактуя в статье те или иные научные термины, вступает в заочную дискуссию с авторами учебников, учебных пособий или словарей, которые в узких рамках подобных изданий не могут широко излагать свое научное воззрение и заранее оказываются в проигрышном положении. Будет лучше, если для научной полемики Вы обратитесь к текстам монографий или диссертационных работ оппонентов.

Не превращайте научную статью в публицистическую: не наполняйте ее цитатами из газет и популярных журналов, ссылками на высказывания по телевидению.

Ссылки на научные источники из Интернета допустимы и должны быть соответствующим образом оформлены.

Редакция отвергает материалы, напоминающие реферат. Автору нужно не только продемонстрировать хорошее знание обсуждаемого вопроса, работ ученых, исследовавших его прежде, но и привнести своей публикацией определенную научную новизну.

Не принимаются к публикации избранные части из диссертаций, книг, монографий, поскольку стиль изложения подобных материалов не соответствует журнальному жанру, а также не принимаются материалы, публиковавшиеся ранее в других изданиях.

В случае отправки статьи одновременно в разные издания автор обязан известить об этом редакцию. Если он не сделал этого заблаговременно, рискует репутацией: в дальнейшем его материалы не будут приниматься к рассмотрению.

Уличенные в плагиате попадают в «черный список» издательства и не могут рассчитывать на публикацию. Информация о подобных фактах передается в другие издательства, в ВАК и по месту работы, учебы автора.

Статьи представляются в электронном виде только через сайт издательства http://www.e-notabene.ru кнопка "Авторская зона".

Статьи без полной информации об авторе (соавторах) не принимаются к рассмотрению, поэтому автор при регистрации в авторской зоне должен ввести полную и корректную информацию о себе, а при добавлении статьи - о всех своих соавторах.

Не набирайте название статьи прописными (заглавными) буквами, например: «ИСТОРИЯ КУЛЬТУРЫ…» — неправильно, «История культуры…» — правильно.

При добавлении статьи необходимо прикрепить библиографию (минимум 10–15 источников, чем больше, тем лучше).

При добавлении списка использованной литературы, пожалуйста, придерживайтесь следующих стандартов:

- ГОСТ 7.1-2003 Библиографическая запись. Библиографическое описание. Общие требования и правила составления.
- ГОСТ 7.0.5-2008 Библиографическая ссылка. Общие требования и правила составления

В каждой ссылке должен быть указан только один диапазон страниц. В теле статьи ссылка на источник из списка литературы должна быть указана в квадратных скобках, например, [1]. Может быть указана ссылка на источник со страницей, например, [1, с. 57], на группу источников, например, [1, 3], [5-7]. Если идет ссылка на один и тот же источник, то в теле статьи нумерация ссылок должна выглядеть так: [1, с. 35]; [2]; [3]; [1, с. 75-78]; [4]....
А в библиографии они должны отображаться так:
[1]
[2]
[3]
[4]....

Постраничные ссылки и сноски запрещены. Если вы используете сноску, не содержащую ссылку на источник, например, разъяснение термина, включите сноску в текст статьи.

После процедуры регистрации необходимо прикрепить аннотацию на русском языке, которая должна состоять из трех разделов: Предмет исследования; Метод, методология исследования; Новизна исследования, выводы.

Прикрепить 10 ключевых слов.

Прикрепить саму статью.

Требования к оформлению текста:

- Кавычки даются уголками (« ») и только кавычки в кавычках — лапками (“ ”).
- Тире между датами дается короткое (Ctrl и минус) и без отбивок.
- Тире во всех остальных случаях дается длинное (Ctrl, Alt и минус).
- Даты в скобках даются без г.: (1932–1933).
- Даты в тексте даются так: 1920 г., 1920-е гг., 1540–1550-е гг.
- Недопустимо: 60-е гг., двадцатые годы двадцатого столетия, двадцатые годы XX столетия, 20-е годы XX столетия.
- Века, король такой-то и т.п. даются римскими цифрами: XIX в., Генрих IV.
- Инициалы и сокращения даются с пробелом: т. е., т. д., М. Н. Иванов. Неправильно: М.Н. Иванов, М.Н. Иванов.

ВСЕ СТАТЬИ ПУБЛИКУЮТСЯ В АВТОРСКОЙ РЕДАКЦИИ.

По вопросам публикации и финансовым вопросам обращайтесь к администратору
Зубковой Светлане Вадимовне
E-mail: info@nbpublish.com
или по телефону +7 (966) 020-34-36

Подробные требования к написанию аннотаций:

Аннотация в периодическом издании является источником информации о содержании статьи и изложенных в ней результатах исследований.

Аннотация выполняет следующие функции: дает возможность установить основное

содержание документа, определить его релевантность и решить, следует ли обращаться к полному тексту документа; используется в информационных, в том числе автоматизированных, системах для поиска документов и информации.

Аннотация к статье должна быть:

- информативной (не содержать общих слов);
- оригинальной;
- содержательной (отражать основное содержание статьи и результаты исследований);
- структурированной (следовать логике описания результатов в статье);

Аннотация включает следующие аспекты содержания статьи:

- предмет, цель работы;
- метод или методологию проведения работы;
- результаты работы;
- область применения результатов; новизна;
- выводы.

Результаты работы описывают предельно точно и информативно. Приводятся основные теоретические и экспериментальные результаты, фактические данные, обнаруженные взаимосвязи и закономерности. При этом отдается предпочтение новым результатам и данным долгосрочного значения, важным открытиям, выводам, которые опровергают существующие теории, а также данным, которые, по мнению автора, имеют практическое значение.

Выводы могут сопровождаться рекомендациями, оценками, предложениями, гипотезами, описанными в статье.

Сведения, содержащиеся в заглавии статьи, не должны повторяться в тексте аннотации. Следует избегать лишних вводных фраз (например, «автор статьи рассматривает...», «в статье рассматривается…»).

Исторические справки, если они не составляют основное содержание документа, описание ранее опубликованных работ и общеизвестные положения в аннотации не приводятся.

В тексте аннотации следует употреблять синтаксические конструкции, свойственные языку научных и технических документов, избегать сложных грамматических конструкций.

Гонорары за статьи в научных журналах не начисляются.

Цитирование или воспроизведение текста, созданного ChatGPT, в вашей статье

Если вы использовали ChatGPT или другие инструменты искусственного интеллекта в своем исследовании, опишите, как вы использовали этот инструмент, в разделе «Метод» или в аналогичном разделе вашей статьи. Для обзоров литературы или других видов эссе, ответов или рефератов вы можете описать, как вы использовали этот инструмент, во введении. В своем тексте предоставьте prompt - командный вопрос, который вы использовали, а затем любую часть соответствующего текста, который был создан в ответ.

К сожалению, результаты «чата» ChatGPT не могут быть получены другими читателями, и хотя невосстановимые данные или цитаты в статьях APA Style обычно цитируются как личные сообщения, текст, сгенерированный ChatGPT, не является сообщением от человека.

Таким образом, цитирование текста ChatGPT из сеанса чата больше похоже на совместное использование результатов алгоритма; таким образом, сделайте ссылку на автора алгоритма записи в списке литературы и приведите соответствующую цитату в тексте.

Пример:

На вопрос «Является ли деление правого полушария левого полушария реальным или метафорой?» текст, сгенерированный ChatGPT, показал, что, хотя два полушария мозга в некоторой степени специализированы, «обозначение, что люди могут быть охарактеризованы как «левополушарные» или «правополушарные», считается чрезмерным упрощением и популярным мифом» (OpenAI, 2023).

Ссылка в списке литературы

OpenAI. (2023). ChatGPT (версия от 14 марта) [большая языковая модель]. https://chat.openai.com/chat

Вы также можете поместить полный текст длинных ответов от ChatGPT в приложение к своей статье или в дополнительные онлайн-материалы, чтобы читатели имели доступ к точному тексту, который был сгенерирован. Особенно важно задокументировать точный созданный текст, потому что ChatGPT будет генерировать уникальный ответ в каждом сеансе чата, даже если будет предоставлен один и тот же командный вопрос. Если вы создаете приложения или дополнительные материалы, помните, что каждое из них должно быть упомянуто по крайней мере один раз в тексте вашей статьи в стиле APA.

Пример:

При получении дополнительной подсказки «Какое представление является более точным?» в тексте, сгенерированном ChatGPT, указано, что «разные области мозга работают вместе, чтобы поддерживать различные когнитивные процессы» и «функциональная специализация разных областей может меняться в зависимости от опыта и факторов окружающей среды» (OpenAI, 2023; см. Приложение A для полной расшифровки). .

Ссылка в списке литературы

OpenAI. (2023). ChatGPT (версия от 14 марта) [большая языковая модель]. https://chat.openai.com/chat Создание ссылки на ChatGPT или другие модели и программное обеспечение ИИ

Приведенные выше цитаты и ссылки в тексте адаптированы из шаблона ссылок на программное обеспечение в разделе 10.10 Руководства по публикациям (Американская психологическая ассоциация, 2020 г., глава 10). Хотя здесь мы фокусируемся на ChatGPT, поскольку эти рекомендации основаны на шаблоне программного обеспечения, их можно адаптировать для учета использования других больших языковых моделей (например, Bard), алгоритмов и аналогичного программного обеспечения.

Ссылки и цитаты в тексте для ChatGPT форматируются следующим образом:

OpenAI. (2023). ChatGPT (версия от 14 марта) [большая языковая модель]. https://chat.openai.com/chat

Цитата в скобках: (OpenAI, 2023)

Описательная цитата: OpenAI (2023)

Давайте разберем эту ссылку и посмотрим на четыре элемента (автор, дата, название и

источник):

Автор: Автор модели OpenAI.

Дата: Дата — это год версии, которую вы использовали. Следуя шаблону из Раздела 10.10, вам нужно указать только год, а не точную дату. Номер версии предоставляет конкретную информацию о дате, которая может понадобиться читателю.

Заголовок. Название модели — «ChatGPT», поэтому оно служит заголовком и выделено курсивом в ссылке, как показано в шаблоне. Хотя OpenAI маркирует уникальные итерации (например, ChatGPT-3, ChatGPT-4), они используют «ChatGPT» в качестве общего названия модели, а обновления обозначаются номерами версий.

Номер версии указан после названия в круглых скобках. Формат номера версии в справочниках ChatGPT включает дату, поскольку именно так OpenAI маркирует версии. Различные большие языковые модели или программное обеспечение могут использовать различную нумерацию версий; используйте номер версии в формате, предоставленном автором или издателем, который может представлять собой систему нумерации (например, Версия 2.0) или другие методы.

Текст в квадратных скобках используется в ссылках для дополнительных описаний, когда они необходимы, чтобы помочь читателю понять, что цитируется. Ссылки на ряд общих источников, таких как журнальные статьи и книги, не включают описания в квадратных скобках, но часто включают в себя вещи, не входящие в типичную рецензируемую систему. В случае ссылки на ChatGPT укажите дескриптор «Большая языковая модель» в квадратных скобках. OpenAI описывает ChatGPT-4 как «большую мультимодальную модель», поэтому вместо этого может быть предоставлено это описание, если вы используете ChatGPT-4. Для более поздних версий и программного обеспечения или моделей других компаний могут потребоваться другие описания в зависимости от того, как издатели описывают модель. Цель текста в квадратных скобках — кратко описать тип модели вашему читателю.

Источник: если имя издателя и имя автора совпадают, не повторяйте имя издателя в исходном элементе ссылки и переходите непосредственно к URL-адресу. Это относится к ChatGPT. URL-адрес ChatGPT: https://chat.openai.com/chat. Для других моделей или продуктов, для которых вы можете создать ссылку, используйте URL-адрес, который ведет как можно более напрямую к источнику (т. е. к странице, на которой вы можете получить доступ к модели, а не к домашней странице издателя).

Другие вопросы о цитировании ChatGPT

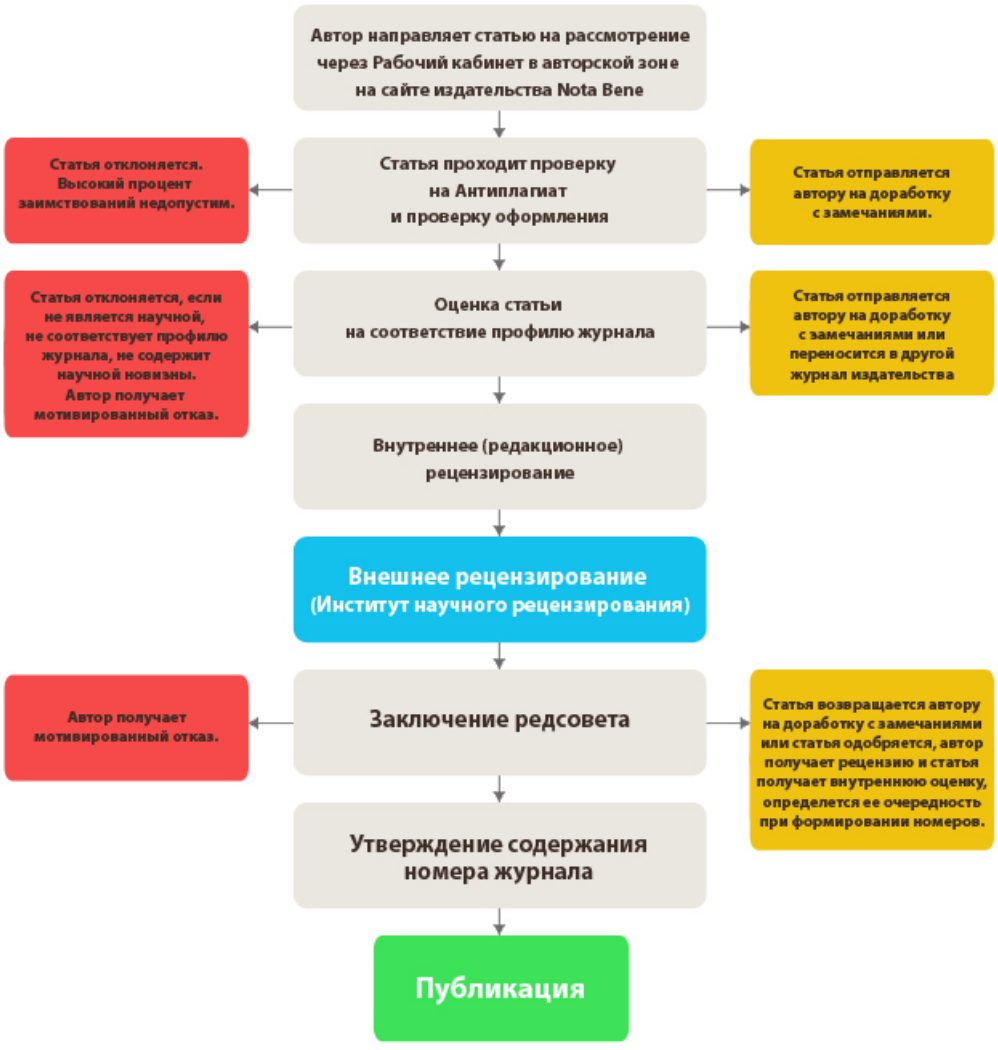
Вы могли заметить, с какой уверенностью ChatGPT описал идеи латерализации мозга и то, как работает мозг, не ссылаясь ни на какие источники. Я попросил список источников, подтверждающих эти утверждения, и ChatGPT предоставил пять ссылок, четыре из которых мне удалось найти в Интернете. Пятая, похоже, не настоящая статья; идентификатор цифрового объекта, указанный для этой ссылки, принадлежит другой статье, и мне не удалось найти ни одной статьи с указанием авторов, даты, названия и сведений об источнике, предоставленных ChatGPT. Авторам, использующим ChatGPT или аналогичные инструменты искусственного интеллекта для исследований, следует подумать о том, чтобы сделать эту проверку первоисточников стандартным процессом. Если источники являются реальными, точными и актуальными, может быть лучше прочитать эти первоисточники, чтобы извлечь уроки из этого исследования, и перефразировать или процитировать эти статьи, если применимо, чем использовать их интерпретацию модели.

Материалы журналов включены:

- в систему Российского индекса научного цитирования;
- отображаются в крупнейшей международной базе данных периодических изданий Ulrich's Periodicals Directory, что гарантирует значительное увеличение цитируемости;
- Всем статьям присваивается уникальный идентификационный номер Международного регистрационного агентства DOI Registration Agency. Мы формируем и присваиваем всем статьям и книгам, в печатном, либо электронном виде, оригинальный цифровой код. Префикс и суффикс, будучи прописанными вместе, образуют определяемый, цитируемый и индексируемый в поисковых системах, цифровой идентификатор объекта — digital object identifier (DOI).

Отправить статью в редакцию

Этапы рассмотрения научной статьи в издательстве NOTA BENE.



Содержание

Contents

Вопросы безопасности
Правильная ссылка на статью:
Сергеева А.А., Гурев М.С., Кириллова Я.М., Пяткова О.В., Фейзуллаев Ф.М., Лотоцкий А.С. — Некоторые особенности противодействия мошенничеству, совершаемому с использованием электронных средств платежа, по законодательству России и Китая // Вопросы безопасности. – 2024. – № 1. DOI: 10.25136/2409-7543.2024.1.69010 EDN: JMCGPE URL: https://nbpublish.com/library_read_article.php?id=69010

Некоторые особенности противодействия мошенничеству, совершаемому с использованием электронных средств платежа, по законодательству России и Китая

Сергеева Анжелика Анатольевна

кандидат юридических наук

доцент, кафедра уголовного права и процесса, Санкт-Петербургский институт (филиал) Всероссийского государственного университета юстиции

190000, Россия, Санкт-Петербург, г. Санкт-Петербург, пер. Басков, 16

lokhi@yandex.ru

Гурев Михаил Сергеевич

кандидат юридических наук

доцент, кафедра уголовного права и процесса, Санкт-Петербургский институт (филиал) Всероссийского государственного университета юстиции

190000, Россия, г. Санкт-Петербург, пер. Басков, 16

lokhi@rambler.ru

Кириллова Яна Максимовна

кандидат юридических наук

доцент, кафедра уголовного права и процесса, Санкт-Петербургский институт (филиал) Всероссийского государственного университета юстиции

190000, Россия, г. Санкт-Петербург, пер. Басков, 16

lokhi@rambler.ru

Пяткова Оксана Владимировна

кандидат юридических наук

доцент, кафедра уголовного права и процесса, Санкт-Петербургский институт (филиал) Всероссийского государственного университета юстиции

190000, Россия, г. Санкт-Петербург, пер. Басков, 16

lokhi@rambler.ru

Фейзуллаев Фирудин Махрамали Оглы

кандидат юридических наук

доцент, кафедра уголовного права и процесса, Санкт-Петербургский институт (филиал) Всероссийского государственного университета юстиции

190000, Россия, г. Санкт-Петербург, пер. Басков, 16

lokhi@rambler.ru

Лотоцкий Антон Сергеевич

старший преподаватель, кафедра уголовного права и процесса, Санкт-Петербургский институт (филиал) Всероссийского государственного университета юстиции

190000, Россия, г. Санкт-Петербург, пер. Басков, 16

lokhi@rambler.ru

Статья из рубрики "Экономическое обеспечение национальной безопасности"

DOI:

10.25136/2409-7543.2024.1.69010

EDN:

JMCGPE

Дата направления статьи в редакцию:

15-11-2023

Дата публикации:

22-11-2023

Аннотация: Актуальность исследования обусловлена увеличением посягательств на денежные средства, функционирующие в безналичной форме. В перспективе развитие цифровой экономики будет сопряжено с возрастанием таких рисков. В этой связи авторами предпринято сравнение российского и китайского опыта их минимизации. В обеих странах фиксируется стабильный рост количества хищений, совершенных с использованием неправомерного доступа к электронным платежным системам. При этом уголовно-правовые нормы, предназначенные для противодействия мошенническим действиям, имеют определенные недостатки. Неоднозначным является и судебное толкование этих норм. В условиях ограниченного функционирования международных платежных систем хищения безналичных денежных средств могут совершаться новыми способами. В перспективе безналичные расчеты будут увеличиваться в объемах, поэтому необходимо совершенствование безопасности их проведения. Авторами использован сравнительно-правовой метод, а также анализ и синтез, что позволило придать исследованию завершенный характер. В рамках статьи обобщен российский и китайский опыт противодействия хищениям денежных средств, размещенных в безналичной форме. Поскольку доля безналичных расчетов в России и Китае является значительной, в их совершение вовлечены не только хозяйствующие субъекты, но и граждане. Последние, не обладая финансовой грамотностью, могут становиться жертвами мошенников. Государственная политика в части регулирования безналичных расчетов выстроена в направлении установления контроля за функционированием электронных площадок. Однако это представляется недостаточным, поскольку не снижает финансовые риски. Уголовно-правовое поле остается фактически единственным рычагом противодействия хищениям данного вида. Вместе с тем, структура уголовно-

правового запрета не отражает характера и степени общественной опасности мошеннических действий и не содержит четкого отличия их от тайного хищения.

Ключевые слова:

цифровая экономика, киберпреступность, профилактика, средства платежа, безналичные расчеты, мошенничество, хищение, обман, ущерб, наказание

Мошенничество, совершенное с использованием электронных средств платежа, является одним из преступлений, возникших в связи с бурным развитием электронных технологий, совершенствованием системы безналичных расчетов с участием граждан и организаций, проникновением в повседневную жизнь различных технических устройств, упрощающих оборот денежных средств. Зародившись практически одновременно с появлением дистанционных средств продажи товаров, эта форма криминальной активности стала динамично развиваться и, осложнившись одновременно с совершенствованием систем безопасности безналичных расчетов, постепенно приобрела трансграничный характер. В связи с этим процесс противодействия хищениям денежных средств изрядно затруднен.

Как известно, в период пандемии Covid-19 дистанционная купля-продажа товаров стала пользоваться широкой популярностью: практически во всех государствах вводились ограничения оборота товаров потребительского назначения, торговые предприятия и заведения общественного питания не работали, контактные формы оказания услуг не осуществлялись. Для многих граждан их дистанционное приобретение оказалось востребованным, поскольку безналичные расчеты к тому времени стали достаточно привычными.

Так, уже по итогам 2018 г. в России более 56% платежей совершалось безналичным способом: с использованием платежных карт, мобильных приложений для смартфонов, механизмов дистанционных онлайн продаж; при этом общая сумма платежей превысила 22 трлн рублей [1]. В КНР стоимость рынка электронной коммерции в 2018 г. превысила 600 млрд юаней, а в его обслуживание было вовлечено более 3 млн человек [2]. При таких обстоятельствах и достаточно высоких темпах роста (в РФ они превысили 40%, в КНР 72%) увеличивается риск совершения хищений денежных средств, а значит, инструменты, обеспечивающие доступ к ним, должны получать дальнейшую техническую защиту и правовую охрану. В период пандемии объем электронной коммерции и доля безналичных расчетов выросли как в России, так и в Китае (в Китае в 2021 г. было совершено платежей с использованием банковских карт на сумму 1 трлн юаней, онлайн платежей – на сумму 2,35 трлн юаней; в России доля безналичных расчетов достигла 78% в 2022 г.). Одновременно в обеих странах фиксировался стабильный рост количества хищений, совершенных с использованием неправомерного доступа к электронным платежным системам.

Исследование особенностей противодействия мошенничеству, совершаемому с использованием электронных средств платежа, представляет интерес, поскольку такие преступления характеризуются устойчивой повторяемостью и негативной динамикой. Сравнение российского и китайского опыта, в свою очередь, рассматривается авторами как эффективный методологический инструмент, поскольку обе страны являются экономическими партнерами, преодолевают в настоящее время последствия санкционной политики, развивают евразийские механизмы сотрудничества. При этом на примере КНР можно выделить отдельные параметры правового регулирования,

заслуживающие внимания при совершенствовании российского законодательства. В этой связи, наряду с признанными методами диалектического познания, при проведении исследования использовался сравнительно-правовой метод с ограниченной страноведческой выборкой.

В целях противодействия правонарушениям, совершаемым с использованием электронных средств платежа, в КНР был принят закон «Об электронной коммерции», вступивший в силу с 1 января 2019 г. Право заключать сделки с использованием электронных средств платежа возникает после обязательной регистрации предпринимательской деятельности. Это правило распространяется и на субъектов, занимающихся продажей товаров и услуг в социальных сетях. Микробизнес должен быть зарегистрирован на территории КНР, а его владелец – встать на учет в качестве налогоплательщика. Площадки для электронной коммерции обязаны следить за тем, чтобы такие лица размещали в открытом доступе информацию о себе, а при необходимости – сведения о получении лицензии. Для граждан КНР порядок доступа к заключению сделок на электронных площадках упрощен: они могут получить специальное разрешение на занятие предпринимательской деятельностью с использованием сети «Интернет», зарегистрировав индивидуальное предприятие (в этом случае не требуется аренда офиса, но запрещается ведение деятельности офф-лайн). При этом регистрироваться в качестве индивидуального предпринимателя не обязаны лица, которые занимаются продажей товаров собственного изготовления или нерегулярно оказывают платные услуги небольшой стоимости, не требующие лицензирования. Иностранные граждане получают право заключать сделки на электронных площадках после создания компании с ограниченной ответственностью, что сопряжено с арендой офиса, бухгалтерским сопровождением бизнеса. В соответствии с Законом «Об электронной коммерции» обеспечивается и защита прав потребителей: предприниматели обязаны направлять каждому клиенту электронные счета (инвойсы), служащие подтверждением оплаты товаров и услуг, а владельцы электронных площадок – следить за соблюдением прав потребителей. Крупнейшие электронные площадки Китая (Taobao, JD) работают по таким правилам уже более пяти лет, но эти правила утверждались не законом, а ведомственным нормативным правовым актом – приказом Министерства коммерции КНР. По сути, владельцы электронных площадок могут быть уподоблены саморегулируемым организациям, практика учреждения которых сложилась в различных областях российской бизнес-среды (строительство и др.).

Для сравнения, в России в порядке эксперимента внедряется регистрация «самозанятых» - лиц, занимающихся возмездным оказанием услуг без регистрации в качестве индивидуальных предпринимателей. В этих целях принят специальный закон, а также производится экспериментальное взимание налога на доходы таких лиц. Плательщики этого налога осуществляют предпринимательскую деятельность без регистрации, не имеют работодателя и не привлекают наемных работников. В том числе, они могут вести клиентскую базу или рекламировать реализуемые товары, работы, услуги с использованием сети «Интернет», осуществлять расчетные операции с использованием электронных средств платежа. Однако, в отличие от приведенных выше положений Закона КНР, имеющих профилактическое значение, в России такой нормативный правовой акт принят, главным образом, для повышения налоговой дисциплины и обеспечения исполнения такими гражданами обязанности уплачивать налоги и сборы с полученных доходов.

Как представляется, Пленум Верховного Суда РФ, давший толкование признакам специальных видов мошенничества осенью 2017 г., опередил законодательную

инициативу, реализованную весной 2018 г. и приведшую к включению в ст. 158 УК РФ квалифицирующего признака «с банковского счета, а равно в отношении электронных денежных средств». Признав указанные деяния тяжким преступлением, законодатель опирался на п. 17 постановления Пленума Верховного Суда РФ. Однако если редакция ст. 159.3 УК РФ в момент его принятия включала обязательный признак «использование поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты путем обмана уполномоченного работника кредитной, торговой или иной организации», что позволяло дать такое толкование, то в данный момент ситуация сложилась иная. Объективная сторона мошенничества с использованием электронных денежных средств в ч. 1 ст. 159.3 УК РФ подробно не раскрыта. Из этого следует, что, руководствуясь правилами отграничения данного вида мошенничества от кражи, правоприменитель будет квалифицировать незаконный доступ к денежным средствам, зачисленным на баланс платежной карты, электронного кошелька или иной виртуальной платежной системы, как тайное хищение чужого имущества. По ст. 159.3 УК РФ становится возможным квалифицировать только те действия, которые сопряжены с осуществлением кибер-атак, применением специального оборудования, позволяющего получить доступ к персональной информации о владельце карты, совершением онлайн-расчетов с использованием фальсифицированных версий сайтов операторов Интернет-торговли.

Однако вышеназванные действия охватываются составом неправомерного доступа к компьютерной информации (ст. 272 УК РФ) или же составом неправомерного оборота средств платежей (ст. 187 УК РФ), что также может породить трудности для правоприменителя. Более того, некоторые авторы полагают, что использование оборудования, позволяющего получить сведения о состоянии счетов владельцев электронных платежных карт (например, при скимминге), охватывается составом кражи, подобно тому, как это рекомендуется Пленумом Верховного Суда РФ при квалификации снятия денежных средств через банкомат в отсутствие сотрудника кредитной организации, вводимого в заблуждение [3].

Исходя из этого, можно заключить, что в процессе совершенствования законодательства в УК РФ было сформировано два одинаковых по структуре запрета (п. «г» ч. 3 ст. 158 УК РФ и ч. 1 ст. 159.3 УК РФ), обладающих разными по строгости санкциями[4]. Вследствие этого противоправный доступ к денежным средствам, зачисленным на баланс платежной карты или находящимся в обороте электронных платежных систем, квалифицируется как тайное хищение чужого имущества, даже если необходимая для этого информация была получена от их владельца, находящегося под влиянием обмана или заблуждения.

Для сравнения, в объективной стороне преступления, предусмотренного ст. 196 УК КНР, используется такая характеристика деяния, как осуществление мошеннической деятельности. Это также позволяет заключить, что данное преступление совершается только в активной форме. В целом такая конструкция состава преступления позволяет признать его оконченным в момент совершения действий, независимо от того, состоялось ли выбытие денежной суммы из законного владения. В других статьях УК КНР (например, в ст. 265) используется формулировка «завладение путем мошенничества», что позволяет признать данное преступление оконченным в момент, когда имущество обращено в пользу виновного, и он имеет реальную возможность им распорядиться.

Подводя итог, необходимо отметить, что в уголовно-правовой науке структура специальных составов мошенничества подвергается критике [5]. Применительно к рассматриваемому составу преступления справедливо отмечается, что диспозиция новой

редакции ч.1 ст. 159.3 УК РФ не содержит на указание адресата обмана, не указывает на источник происхождения средства электронного платежа. Установив традиционные для состава мошенничества квалифицирующие признаки в ст. 159.3 УК РФ, законодатель не учитывал специфику совершения данного вида хищения и не привел характерных исключительно для этой формы общественно опасного поведения параметров. Соглашаясь с этим, укажем, что ее положения нуждаются в совершенствовании.

В настоящее время в уголовном законодательстве РФ и КНР сложился идентичный подход к определению мошенничества, в соответствии с которым выделяется общая и специальные нормы, отражающие особенности совершения данного преступления применительно к различным видам общественных отношений, возникающих, в том числе, в сфере высоких технологий, финансовой сфере и сфере использования электронных средств платежа. В уголовном законодательстве Российской Федерации и Китайской народной республики сложилось недостаточно ясное закрепление состава мошенничества с использованием электронных денежных средств, не позволяющее однозначно отграничить его от других видов хищения, а описание квалифицирующих признаков по типовому для всех хищений механизму способствовало «выпадению» из сферы внимания законодателя и правоприменителя перечня обстоятельств, существенно повышающих характер и степень общественной опасности содеянного.

В целях преодоления выявленного пробела представляется необходимым уточнить конструкцию рассматриваемого состава, отразив в ст. 159.3 УК РФ такие особенности, как:

- совершение с использованием клиентских баз или баз данных, содержащих информацию о лицах, владеющих банковскими картами или иными электронными средствами платежа;

- совершение с использованием ресурсов информационно-телекоммуникационной сети «Интернет»;

- неправомерный доступ к мобильным приложениям и иному контенту, допускающему совершение безналичных расчетов без процедуры подтверждения.

Предлагаемые изменения позволят создать развернутый правовой инструментарий, доступный для восприятия правоприменителем и конкретизирующий содержание уголовно-правового запрета.

Библиография

1. Трофименкова Е.В., Юн Сунбэй, Ян Минсы. Развитие российско-китайской электронной торговли // Ойкумена. Регионоведческие исследования. 2021. № 4. С. 49-55.
2. Фэнчао Цуй. Развитие и изменение электронной коммерции в Китае // Научный журнал. 2018. № 1. С. 80-82.
3. Кочои С.М. Новые нормы о мошенничестве в УК: особенности и различия // Криминологический журнал Байкальского государственного университета экономики и права. 2013. № 4. С. 105-108.
4. Питулько К.В., Сергеева А.А. Проблемы пресечения мошеннических действий, совершаемых с использованием ресурсов сети «Интернет» // Уголовный закон в эпоху искусственного интеллекта и цифровизации : сборник трудов по материалам Всероссийской научно-практической конференции с международным участием в рамках I Саратовского международного юридического форума, посвященного 90-

летнему юбилею Саратовской государственной юридической академии, Саратов, 09 июня 2021 года. Саратов, 2021. С. 224-227.

5. Бойко С.Я. Уголовная ответственность за мошенничество: теоретико-прикладное исследование. М., 2019. С. 8.

Результаты процедуры рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов издательства можно ознакомиться здесь.

Предметом исследования в представленной на рецензирование статье являются, как это следует из ее наименования, некоторые особенности противодействия мошенничеству, совершаемому с использованием электронных средств платежа. Особое внимание автор уделил анализу соответствующего законодательства Китая и России. Заявленные границы исследования полностью соблюдены ученым.
Методология исследования в тексте статьи не раскрывается, но очевидно, что автором использовались всеобщий диалектический, логический, статистический, формально-юридический, сравнительно-правовой методы исследования.
Актуальность избранной автором темы исследования несомненна и обоснована им следующим образом: "По итогам 2018 г. в России более 56% платежей совершалось безналичным способом: с использованием платежных карт, мобильных приложений для смартфонов, механизмов дистанционных онлайн продаж; при этом общая сумма платежей превысила 22 трлн рублей [1]. В КНР стоимость рынка электронной коммерции в 2018 г. превысила 600 млрд юаней, а в его обслуживание было вовлечено более 3 млн человек [2]. При таких обстоятельствах и достаточно высоких темпах роста (в РФ они превысили 40%, в КНР 72%) увеличивается риск совершения хищений денежных средств, а значит, инструменты, обеспечивающие доступ к ним, должны получать дальнейшую техническую защиту и правовую охрану. В период пандемии объем электронной коммерции и доля безналичных расчетов выросли как в России, так и в Китае (в Китае в 2021 г. было совершено платежей с использованием банковских карт на сумму 1 трлн юаней, онлайн платежей – на сумму 2,35 трлн юаней; в России доля безналичных расчетов достигла 78% в 2022 г.). Одновременно в обеих странах фиксировался стабильный рост количества хищений, совершенных с использованием неправомерного доступа к электронным платежным системам". Дополнительно ученому необходимо перечислить фамилии ведущих специалистов, занимавшихся исследованием поднимаемых в статье проблем, а также раскрыть степень их изученности.
Научная новизна работы проявляется в некоторых заключениях автора, к примеру: "... в процессе совершенствования законодательства в УК РФ было сформировано два одинаковых по структуре запрета (п. «г» ч. 3 ст. 158 УК РФ и ч. 1 ст. 159.3 УК РФ), обладающих разными по строгости санкциями [4]. Вследствие этого противоправный доступ к денежным средствам, зачисленным на баланс платежной карты или находящимся в обороте электронных платежных систем, квалифицируется как тайное хищение чужого имущества, даже если необходимая для этого информация была получена от их владельца, находящегося под влиянием обмана или заблуждения"; но в целом работа носит описательный, информационный характер. Автор не предложил логически стройной, оригинальной концепции противодействия мошенничеству, совершаемому с использованием электронных средств платежа. Таким образом, в представленном виде статья не вносит особого вклада в развитие отечественной правовой науки.
Научный стиль исследования выдержан автором в полной мере.

Структура работы вполне логична. Во вводной части статьи ученый обосновывает актуальность избранной им темы исследования. В основной части работы автор осуществляет сравнительный анализ противодействия мошенничеству, совершаемому с использованием электронных средств платежа, в КНР и в России, выявляет соответствующие проблемы и в общих чертах намечает пути их решения. В заключительной части статьи содержатся выводы по результатам проведенного исследования.

Содержание статьи полностью соответствует ее наименованию и не вызывает особых нареканий, однако некоторые положения работы нуждаются в конкретизации. В чем конкретно состоит положительный опыт КНР в части противодействия мошенничеству, совершаемому с использованием электронных средств платежа? Что можно было бы позаимствовать российскому законодателю? Отмечая существующие проблемы юридической техники в исследуемых статьях УК РФ, автор не предлагает конкретных изменений в их формулировках. Между тем именно в этом могла бы проявиться научная новизна исследования.

Ученый отмечает: "По ст. 159.3 УК РФ становится возможным квалифицировать только те действия, которые сопряжены с осуществлением кибер-атак, применением специального оборудования, позволяющего получить доступ к персональной информации о владельце карты, совершением онлайн-расчетов с использованием фальсифицированных версий сайтов операторов Интернет-торговли. Однако вышеназванные действия охватываются составом неправомерного доступа к компьютерной информации (ст. 272 УК РФ) или же составом неправомерного оборота средств платежей (ст. 187 УК РФ), что также может породить трудности для правоприменителя". Обозначенная автором проблема нуждается в более подробном рассмотрении.

Библиография исследования представлена 5 источниками (монографией и научными статьями), не считая нормативного материала. С формальной точки зрения этого достаточно; с фактической - ряд положений статьи нуждается в конкретизации.

Апелляция к оппонентам имеется, как общая, так и частная (С. М. Кочои). Научная дискуссия ведется автором корректно. Положения работы не всегда обосновываются в достаточной степени.

Выводы по результатам проведенного исследования имеются ("Подводя итог, необходимо отметить, что в уголовно-правовой науке структура специальных составов мошенничества подвергается критике [5]. Применительно к рассматриваемому составу преступления справедливо отмечается, что диспозиция новой редакции ч.1 ст. 159.3 УК РФ не содержит на указание адресата обмана, не указывает на источник происхождения средства электронного платежа. Соглашаясь с этим, укажем, что ее положения нуждаются в совершенствовании"), но они формулированы очень кратко и не обладают свойством научной новизны. Таким образом, выводы нуждаются в уточнении и конкретизации.

Интерес читательской аудитории к представленной на рецензирование статье может быть проявлен прежде всего со стороны специалистов в сфере уголовного права и уголовного процесса при условии ее доработки: раскрытии методологии исследования, дополнительном обосновании актуальности его темы, введении дополнительных элементов научной новизны, уточнении и конкретизации некоторых положений работы и выводов по результатам проведенного исследования.

Результаты процедуры повторного рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.

Со списком рецензентов издательства можно ознакомиться здесь.

Предмет исследования. В рецензируемой статье «Некоторые особенности противодействия мошенничеству, совершаемому с использованием электронных средств платежа, по законодательству России и Китая» предметом исследования являются нормы российского и китайского права, предусматривающие уголовную ответственность за мошенничество, совершаемое с применение современных информационно-коммуникационных технологий.

Методология исследования. Основной метод исследования – это сравнительное правоведение. При написании статьи использовались также такие методы как: логический, теоретико-прогностический, формально-юридический, системно-структурный и правового моделирования. Методологический аппарат составили следующие диалектические приемы и способы научного познания: анализ, абстрагирование, индукция, дедукция, гипотеза, аналогия, синтез, типология, классификация, систематизация и обобщение. В работе использовалось сочетание эмпирической и теоретической информации. Применение современных методов позволило изучить сложившиеся подходы, взгляды на предмет исследования, выработать авторскую позицию и аргументировать ее.

Актуальность исследования. Актуальность темы исследования, заявленной автором, не вызывает сомнения. Автор справедливо отмечает, что «…исследование особенностей противодействия мошенничеству, совершаемому с использованием электронных средств платежа, представляет интерес, поскольку такие преступления характеризуются устойчивой повторяемостью и негативной динамикой. Сравнение российского и китайского опыта, в свою очередь, рассматривается авторами как эффективный методологический инструмент, поскольку обе страны являются экономическими партнерами, преодолевают в настоящее время последствия санкционной политики, развивают евразийские механизмы сотрудничества». Эти обстоятельства указывают на актуальность доктринальных разработок по данной тематике с целью совершенствования отечественного нормотворчества и практики его применения.

Научная новизна. Не подвергая сомнению важность проведенных ранее научных исследований, послуживших теоретической базой для данной работы, тем не менее, можно отметить, что в этой статье впервые сформулированы заслуживающие внимания положения, например: «…В уголовном законодательстве Российской Федерации и Китайской народной республики сложилось недостаточно ясное закрепление состава мошенничества с использованием электронных денежных средств, не позволяющее однозначно отграничить его от других видов хищения, а описание квалифицирующих признаков по типовому для всех хищений механизму способствовало «выпадению» из сферы внимания законодателя и правоприменителя перечня обстоятельств, существенно повышающих характер и степень общественной опасности содеянного (орфография автора статьи)». Автором по результатам написания статьи сделан ряд теоретических выводов и предложений, что указывает не только на важность этого исследования для юридической науки, но и определяет его практическую значимость.

Стиль, структура, содержание. Статья написана научным стилем, использована специальная юридическая терминология. Однако встречаются ошибки, опечатки (например, в написании официальных названий государств: «Китайской народной республики»). В целом же материал изложен последовательно и ясно. Статья структурирована. Тема раскрыта, содержание статьи соответствует ее названию. Представляется, что ведение не совсем отвечает требованиям, предъявляемым к этой части научной статьи. А также, в заключении следовало бы сформулировать те, основные результаты, которые достиг автор в ходе исследования. Замечания по содержанию статьи носят рекомендательный характер. Грамматические ошибки следует

исправить.

Библиография. Автором использовано недостаточное количество доктринальных источников (для научной статьи не менее 10), мало представлено ссылок на публикации последних лет. Имеющиеся ссылки на источники оформлены в соответствии с требования библиографического ГОСТа.

Апелляция к оппонентам. По отдельным вопросам заявленной тематики представлена научная дискуссия, обращения к оппонентам корректные. Все заимствования оформлены ссылками на автора и источник опубликования.

Выводы, интерес читательской аудитории. Статья «Некоторые особенности противодействия мошенничеству, совершаемому с использованием электронных средств платежа, по законодательству России и Китая» рекомендуется к опубликованию. Статья соответствует тематике журнала «Вопросы безопасности». Статья написана на актуальную тему, имеет практическую значимость и отличается научной новизной. Данная статья может представлять интерес для широкой читательской аудитории, прежде всего, специалистов в области уголовного права и компаративистики, а также, будет полезна для преподавателей и обучающихся юридических вузов и факультетов.

Вопросы безопасности
Правильная ссылка на статью:
Куцев В.В. — Формы и методы предупреждения преступлений в сфере незаконного оборота наркотиков // Вопросы безопасности. – 2024. – № 1. DOI: 10.25136/2409-7543.2024.1.69561 EDN: QUZZSS URL: https://nbpublish.com/library_read_article.php?id=69561

Формы и методы предупреждения преступлений в сфере незаконного оборота наркотиков

Куцев Владимир Валентинович

Депутат, Представительное Собрание Рыльского района Курской области

307370, Россия, Курская область, г. Рыльск, ул. К. Либкнехта, 21

Avto1772@mail.ru

Статья из рубрики "Внутренние угрозы и контрмеры"

DOI:

10.25136/2409-7543.2024.1.69561

EDN:

QUZZSS

Дата направления статьи в редакцию:

08-01-2024

Дата публикации:

15-01-2024

Аннотация: Предметом настоящего исследования выступают формы и методы предупреждения преступлений в сфере незаконного оборота наркотиков. Цель исследования заключается в проведении анализа форм и методов предупреждения наркопреступлений, их дифференциации, выявлении актуальных проблем и выработке путей их решения. Обращено внимание, что основными субъектами деятельности по предупреждению наркопреступности выступают государство и общество. Роль государства заключается в координации и определении векторов борьбы с наркопреступностью, составлении планов и программ предупредительной и профилактической деятельности, определении компетенции иных субъектов предупреждения. Общество также играет немаловажную роль в снижении объёмов наркопреступности, поэтому важно задействовать и привлекать граждан к участию в

предупреждении преступлений в сфере незаконного оборота наркотиков. Определено, что качественному взаимодействию институтов гражданского общества с правоохранительными органами и государственными структурами способствует механизм обратной связи. Методология исследования включает ряд общенаучных методов научного познания. В ходе исследования использовались такие методы: метод анализа и синтеза, методы дедукции и индукции, метод анализа научной литературы, метод систематизации, формально-юридический, диалектический и иные методы. Исследование выстроено в соответствии с принципами логики и структурированности. Научная новизна настоящего исследования заключается в выделении актуальных проблем профилактики наркопреступлений, как одного из методов предупреждения преступлений в сфере незаконного оборота наркотиков. Особое внимание обращено на совершенствование практики социальной реабилитации наркоманов. Данная тема выступала предметом научных исследований, но основной акцент многими исследователями делается на наркологическом лечении. При этом социальная реабилитация и трудоустройство наркоманов обладают не меньшим значением, так как серьёзно снижают вероятность совершения такими лицами преступлений в сфере незаконного оборота наркотиков. Рассмотренный метод предупреждения наркопреступлений, выражающийся в индивидуальной профилактической работе с наркозависимыми лицами, поспособствует также снижению спроса на наркотики, что сократит количество преступлений в сфере их незаконного оборота. Проведённое исследование позволило сделать вывод о высокой важности такого метода предупреждения преступлений в сфере незаконного оборота наркотиков, как индивидуальная профилактическая работа с наркозависимыми лицами, их адаптация и социальная реабилитация. Рассмотрены некоторые проблемы в этой сфере, предложены возможные пути их решения.

Ключевые слова:

наркопреступность, предупреждение наркопреступлений, субъекты предупреждения, методы предупреждения, преступность, реабилитация, профилактика, угроза безопасности, наркозависимые лица, правоохранительные органы

Предупреждение преступлений выступает важным направлением борьбы с преступностью, поскольку преследует цель по сдерживанию криминализации общества [1]. В рамках настоящего исследования будут рассмотрены формы и методы предупреждения преступлений в сфере незаконного оборота наркотиков.

Многие известные учёные прошлого и современности отмечали, что предупреждение намного лучше, чем наказание. При этом единого общепринятого определения предупреждения преступности не сформулировано до сих пор. Если обобщить точки зрения большинства исследователей, то можно прийти к выводу, что под предупреждением преступности в целом в большинстве случаев понимается система мер, реализуемых уполномоченными органами, по противодействию процессам детерминации преступности [2].

В науке криминологии предупреждение преступности рассматривается как многоуровневая система мер, реализуемых государством и обществом, направленных на распознавание (идентификацию), ослабление, нейтрализацию или полное устранение причин и условий преступности [3]. Задача предупреждения преступности заключается в

том, чтобы удерживать людей от совершения преступления.

В научной литературе встречаются и другие подходы к определению понятия предупреждения преступности. Так, в исследовании С. И. Голик и Б. П. Михайлова предупреждение преступности рассматривается в качестве совокупности мер и мероприятий по снижению преступности, ликвидации или нейтрализации причин, условий и факторов, которые её порождают [4]. Также встречается мнение, что предупреждение преступности — это особый режим функционирования государственных органов власти, при котором обеспечивается согласованная реализация мер профилактического, правового, организационного и иного характера.

Проведённый теоретический анализ научных источников на предмет определения понятия «предупреждение преступности» позволяет заключить, что в большинстве случаев авторы рассматривают это направление борьбы с преступностью в качестве деятельности, осуществляемой государством и обществом. Это подчёркивает важность предупреждения преступности для обеспечения национальной безопасности и безопасности общества.

Если говорить о предупреждении в контексте наркопреступности, то следует отметить, что за счёт реализуемых государственными и общественными институтами мер достигается снижение уровня наркопреступности, сокращается уровень смертности и заболеваемости населения от наркотиков, стабилизируется ситуация в обществе, а также повышается авторитет государства. Поэтому предупреждению наркопреступности на современном этапе уделяется повышенное внимание.

Переходя к рассмотрению непосредственно форм и методов предупреждения преступлений в сфере незаконного оборота наркотиков, следует отметить, что в криминологии отсутствует единообразная позиция относительно того, что необходимо понимать под формами предупреждения наркопреступности. Некоторые авторы выделяют три формы — профилактику, пресечение, предотвращение [5]. По мнению других исследователей, существует всего две формы предупреждения преступности – профилактика и пресечение [6]. Также встречается позиция, что формы предупреждения преступности определяются исходя из субъекта, осуществляющего данную деятельность. Целесообразно рассмотреть формы предупреждения наркопреступности с учётом последней приведённой позиции.

Так, субъектами предупреждения наркопреступности выступают государство и общество.

Государство, как субъект предупреждения преступлений в сфере незаконного оборота наркотиков, представлено государственными и правоохранительными органами. Соответственно, основная деятельность по предупреждению преступности реализуется государственными органами и правоохранительной системой. Роль государственных органов власти в предупреждении наркопреступности – координирующая. Это означает, что государственными органами устанавливаются векторы борьбы с преступностью, принимаются программы и планы по предупреждению преступности, осуществляется нормотворческая деятельность, определяется компетенция иных субъектов предупреждения. К числу таких органов относятся МВД России, Государственный антинаркотический комитет, иные федеральные органы власти, а также органы власти субъектов РФ и органы местного самоуправления. Сказанное позволяет заключить, что субъектный состав государственных органов, задействованных в предупреждении наркопреступности, достаточно широкий.

Непосредственно реализация функций по противодействию незаконному обороту наркотиков возложена на Генеральную прокуратуру РФ, СК России, ФСБ России и др.

Основной объём работы по предупреждению наркопреступности выполняется правоохранительными органами. Сотрудники данных органов проводят специальные и общие мероприятия профилактической и предупреждающей направленности выявляют факты совершения преступлений, занимаются выявлением, поиском и задержанием подозреваемых, расследуют и раскрывают уголовные дела [7].

Общество, как один из субъектов деятельности по предупреждению преступлений в сфере незаконного оборота наркотиков, также играет важную роль в сдерживании криминализации населения и сокращении преступности. Содействие граждан и институтов гражданского общества государственным и правоохранительным органам в борьбе с преступностью обладает большим значением и приводит к серьёзным результатам в снижении объёмов наркопреступности и сокращении спроса на наркотики. Взаимодействие институтов гражданского общества с государственными и правоохранительными органами обеспечивается за счёт механизма обратной связи. Об эффективности участия рассматриваемого субъекта в предупреждении преступлений в сфере незаконного распространения наркотиков свидетельствует проанализированная следственная и судебная практика. Так, благодаря содействию граждан правоохранительными органами выявляются наркопритоны, преступные группировки, места распространения наркотиков, а также наркозависимые лица. Методом предупреждения наркопреступности, при реализации которого активно задействуется общество, выступает акция «Сообщи, где торгуют смерть». Эта акция проводится в масштабах всей страны и показала достаточно высокие результаты. Только в 2022 г. на телефоны горячей линии поступило более 26 тыс. обращений граждан.

Далее целесообразно рассмотреть методы предупреждения преступлений в сфере незаконного оборота наркотиков. Такими методами, как показывает анализ правоприменительной практики, выступают:

— организация координационных совещаний правоохранительных органов по вопросам предупреждения наркопреступности;

— освещение основных результатов деятельности по предупреждению наркопреступности в СМИ;

— проведение лекций и бесед с учащимися образовательных учреждений по антинаркотической теме, разъяснение опасности наркопреступлений и жёсткости наказания за их совершение;

— повышение правовой культуры, правовой грамотности и правосознания общества, формирование негативного отношения к наркотикам, их употреблению и незаконному распространению;

— проведение индивидуальной профилактики наркопреступлений;

— предотвращение подготавливаемых наркопреступлений путём реализации мер организационного, оперативно-розыскного, уголовно-процессуального и иного характера.

Среди всех перечисленных методов предупреждения преступлений в сфере незаконного оборота наркотиков особым значением обладают меры профилактики. Под профилактикой незаконного оборота наркотиков в научной литературе понимается

совместная деятельность государства и общества, направленная на выявление, устранение или нейтрализацию условий и причин совершения таких преступлений. Понятие профилактики также включает устранение конкретных условий, содействующих вовлечению населения в незаконный оборот наркотиков; определение способов, методов и форм социального контроля за оборотом наркотиков; воздействие на условия жизни и воспитания лиц из группы риска; реализацию уголовно-правовых, уголовно-процессуальных и иных мер.

Отдельно следует обратить внимание, что меры профилактики дифференцируются на общие, групповые и индивидуальные. Меры первой группы проводятся с неопределённым кругом лиц (рекламные кампании, профилактические рейды, обследование мест вероятного скопления наркозависимых и др.). В основе выбора таких мер лежит предварительный анализ наркоситуации. Меры второй группы предполагают работу с лицами из группы риска (несовершеннолетними из неблагополучных семей, наркозависимыми лицами, семьями, находящимися в социально опасном положении). Третья группа мер реализуется в отношении конкретных лиц (наркоманов, наркопреступников). К числу наиболее приоритетных направлений индивидуальной профилактической работы можно отнести адаптацию и ресоциализацию наркозависимых лиц [8]. Несмотря на высокую значимость этого направления профилактической деятельности, а данной сфере существуют некоторые нерешённые проблемы. Целесообразно выделить эти проблемы и предложить возможные пути их решения.

Так, понятием адаптации и ресоциализации наркозависимых лиц охватывается деятельность по восстановлению личностного и социального статуса таких людей, оказанию им помощи в возобновлении социальных связей, помощь в лечении, социальной реабилитации и трудоустройстве. Результатом становится обретение лицом способности нормально функционировать в обществе [9].

Целесообразно выделить ключевые проблемы в данной сфере. Во–первых, деятельность по социальной реабилитации наркозависимых лиц проводится в соответствии с положениями закона о социальном обслуживании, а порядок реализации данной деятельности регламентируется на уровне нормативно-правовых актов субъектов Российской Федерации. Закон носит «рамочный» характер и нуждается в «детализации» на уровне уполномоченных ведомств. Во–вторых, на законодательном уровне не определены формы социальной реабилитации наркозависимых лиц и не урегулированы вопросы государственного контроля (надзора) за соблюдением обязательных требований в этой сфере. В–третьих, существуют проблемы с трудоустройством наркозависимых лиц после прохождения ими наркологического лечения и социальной реабилитации, так как работодатели с большой неохотой принимают таких лиц на работу.

Для решения перечисленных проблем необходимо разработать соответствующие поправки в законодательство, так как в текущей ситуации меры социальной реабилитации наркозависимых лиц являются недостаточными ввиду отсутствия детализации законодательных положений на уровне уполномоченных ведомств. Решить проблему с нежеланием работодателей принимать на работу лиц, прошедших наркологическое лечение и социальную реабилитацию можно путём установления льгот (по аналогии с теми льготами, которые предусмотрены при трудоустройстве инвалидов) [10]. Устранение проблем в сфере адаптации и социальной реабилитации наркоманов и разработка специальных программ поспособствует улучшению процесса нормативной социализации лиц данной категории, что положительно отразится на деятельности по предупреждению преступлений в сфере незаконного оборота наркотиков.

Таким образом, в настоящем исследовании рассмотрены определения понятия «предупреждение преступности», предлагаемые в научной литературе. Определено, что единообразное определение этого понятия отсутствует. При этом большинство исследователей рассматривают данное направление борьбы с преступностью в качестве деятельности государства и общества по согласованной реализации мер профилактического, правового, организационного и иного характера с целью противодействия процессам, детерминирующим преступность. Обращено внимание на особую значимость предупреждения наркопреступности для обеспечения национальной безопасности и безопасности общества.

Рассмотрены основные формы предупреждения преступности в сфере незаконного оборота наркотиков. Предложено дифференцировать формы в зависимости от субъекта, осуществляющего деятельность по предупреждению (государственные органы власти, правоохранительные органы, гражданское общество). Проанализированы методы предупреждения преступлений в сфере незаконного оборота наркотиков. Сделан вывод, что особым значением среди всех таких методов обладают меры профилактики. Определено, что к числу наиболее приоритетных направлений профилактической работы относится адаптация и ресоциализация наркоманов. Выявлены некоторые актуальные проблемы в этой сфере и предложены пути их решения.

Библиография

1. Аганов Г. М., Ковалева Е. Предупреждение преступлений и иных правонарушений средствами прокурорского надзора при исполнении наказания в виде лишения свободы // Уголовное право. 2005. № 4. С. 11.
2. Воронин Ю. А., Майоров А. В. Теоретические основы формирования системы противодействия преступности в России // Криминологический журнал Байкальского государственного ун-та экономики и права. 2013. № 1. С. 7-16.
3. Гоголева А. Я. Понятие профилактики и борьбы с преступностью // Молодой учёный. 2014. № 6.1 (65.1). С. 3-7.
4. Голик С. И., Михайлов Б. П. Организация и тактика общей профилактики преступлений органами внутренних дел. М., 1980. С. 10.
5. Готчина Л. В. Молодёжный наркотизм в современной России: криминологический анализ и профилактика: автореф. дис. … докт. юрид. наук. СПб, 2011. – 46 с.
6. Иванов В. А., Хлебникова Н. С. Роль гражданского общества в борьбе с незаконным оборотом наркотиков // Марийский юридический вестник. 2017. № 1(20). С. 17.
7. Планкина Н. Е. Социальная реабилитация лиц, страдающих наркотической зависимостью // Вестник Амурского государственного университета. Серия: Гуманитарные науки. 2018. № 82. С. 111-113.
8. Сидоренко А. В., Егоршин В. М. Меры предупреждения незаконного оборота наркотиков // Вестник Санкт-Петербургского университета МВД России.2012. № 2 (54). С. 157.
9. Шалагин А. Е. Преступления против здоровья населения: автореферат дис. ... доктора юридических наук. Казань, 2004.-25 с.
10. Щедрин Н. В. Основы общей теории предупреждения преступности. Красноярск, 1999. С. 562

Результаты процедуры рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов издательства можно ознакомиться здесь.

РЕЦЕНЗИЯ
на статью на тему «Формы и методы предупреждения преступлений в сфере незаконного оборота наркотиков».

Предмет исследования.
Предложенная на рецензирование статья посвящена актуальным вопросам предупреждения преступлений в сфере незаконного оборота наркотиков. Как отмечено в самой статье, «В рамках настоящего исследования будут рассмотрены формы и методы предупреждения преступлений в сфере незаконного оборота наркотиков». В качестве конкретного предмета исследования выступили, прежде всего, мнения ученых, эмпирические данные, иные материалы практики.
Методология исследования.
Цель исследования прямо в статье не заявлена. При этом она может быть ясно понята из названия и содержания работы. Цель может быть обозначена в качестве рассмотрения и разрешения отдельных проблемных аспектов вопроса о формах и методах предупреждения преступлений в сфере незаконного оборота наркотиков. Исходя из поставленных цели и задач, автором выбрана методологическая основа исследования.
В частности, автором используется совокупность общенаучных методов познания: анализ, синтез, аналогия, дедукция, индукция, другие. В частности, методы анализа и синтеза позволили обобщить и разделить выводы различных научных подходов к предложенной тематике.
Так, автором обобщена практика по поводу использования различных форм и методов предупреждения преступлений в сфере незаконного оборота наркотиков. В частности, указано следующее: «целесообразно рассмотреть методы предупреждения преступлений в сфере незаконного оборота наркотиков. Такими методами, как показывает анализ правоприменительной практики, выступают: организация координационных совещаний правоохранительных органов по вопросам предупреждения наркопреступности; освещение основных результатов деятельности по предупреждению наркопреступности в СМИ; проведение лекций и бесед с учащимися образовательных учреждений по антинаркотической теме, разъяснение опасности наркопреступлений и жёсткости наказания за их совершение; повышение правовой культуры, правовой грамотности и правосознания общества, формирование негативного отношения к наркотикам, их употреблению и незаконному распространению; проведение индивидуальной профилактики наркопреступлений; предотвращение подготавливаемых наркопреступлений путём реализации мер организационного, оперативно-розыскного, уголовно-процессуального и иного характера».
Также важным представляется следующий вывод: «Об эффективности участия рассматриваемого субъекта в предупреждении преступлений в сфере незаконного распространения наркотиков свидетельствует проанализированная следственная и судебная практика. Так, благодаря содействию граждан правоохранительными органами выявляются наркопритоны, преступные группировки, места распространения наркотиков, а также наркозависимые лица. Методом предупреждения наркопреступности, при реализации которого активно задействуется общество, выступает акция «Сообщи, где торгуют смерть». Эта акция проводится в масштабах всей страны и показала достаточно высокие результаты. Только в 2022 г. на телефоны горячей линии поступило более 26

тыс. обращений граждан».
Таким образом, выбранная автором методология в полной мере адекватна цели исследования, позволяет изучить все аспекты темы в ее совокупности.

Актуальность.
Актуальность заявленной проблематики не вызывает сомнений. Имеется как теоретический, так и практический аспекты значимости предложенной темы. С точки зрения теории тема форм и методов предупреждения преступлений в сфере незаконного оборота наркотиков сложна и неоднозначна. Действительно, в современных условиях вопросы оборота наркотиков сильно воздействуют на общество, негативно сказывается на физическом и нравственном здоровье граждан. Автор в полной мере прав в том, что «Если говорить о предупреждении в контексте наркопреступности, то следует отметить, что за счёт реализуемых государственными и общественными институтами мер достигается снижение уровня наркопреступности, сокращается уровень смертности и заболеваемости населения от наркотиков, стабилизируется ситуация в обществе, а также повышается авторитет государства. Поэтому предупреждению наркопреступности на современном этапе уделяется повышенное внимание».
Тем самым, научные изыскания в предложенной области стоит только поприветствовать.

Научная новизна.
Научная новизна предложенной статьи не вызывает сомнений. Во-первых, она выражается в конкретных выводах автора. Среди них, например, такой вывод:
«в настоящем исследовании рассмотрены определения понятия «предупреждение преступности», предлагаемые в научной литературе. Определено, что единообразное определение этого понятия отсутствует. При этом большинство исследователей рассматривают данное направление борьбы с преступностью в качестве деятельности государства и общества по согласованной реализации мер профилактического, правового, организационного и иного характера с целью противодействия процессам, детерминирующим преступность. Обращено внимание на особую значимость предупреждения наркопреступности для обеспечения национальной безопасности и безопасности общества. Рассмотрены основные формы предупреждения преступности в сфере незаконного оборота наркотиков. Предложено дифференцировать формы в зависимости от субъекта, осуществляющего деятельность по предупреждению (государственные органы власти, правоохранительные органы, гражданское общество). Проанализированы методы предупреждения преступлений в сфере незаконного оборота наркотиков. Сделан вывод, что особым значением среди всех таких методов обладают меры профилактики. Определено, что к числу наиболее приоритетных направлений профилактической работы относится адаптация и ресоциализация наркоманов. Выявлены некоторые актуальные проблемы в этой сфере и предложены пути их решения».
Указанный и иные теоретические выводы могут быть использованы в дальнейших научных исследованиях.
Во-вторых, автором предложены научные обобщения, связанные с конкретными формами и методами предупреждения наркопреступности, что может быть полезно для специалистов в данной сфере.
Таким образом, материалы статьи могут иметь определенных интерес для научного сообщества с точки зрения развития вклада в развитие науки.
Стиль, структура, содержание.
Тематика статьи соответствует специализации журнала «Вопросы безопасности», так как она посвящена правовым проблемам, связанным с криминологической характеристикой

преступлений в сфере незаконного оборота наркотиков.
Содержание статьи в полной мере соответствует названию, так как автор рассмотрел заявленные проблемы, достиг цели исследования.
Качество представления исследования и его результатов следует признать в полной мере положительным. Из текста статьи прямо следуют предмет, задачи, методология и основные результаты исследования.
Оформление работы в целом соответствует требованиям, предъявляемым к подобного рода работам. Существенных нарушений данных требований не обнаружено.

Библиография.
Следует высоко оценить качество использованной литературы. Автором активно использована литература, представленная авторами из России (Аганов Г.М., Ковалева Е., Воронин Ю.А., Майоров А.В., Голик С.И., Михайлов Б.П. и другие). Многие из цитируемых ученых являются признанными учеными в области заявленных проблем.
Таким образом, труды приведенных авторов соответствуют теме исследования, обладают признаком достаточности, способствуют раскрытию различных аспектов темы.

Апелляция к оппонентам.
Автор провел серьезный анализ текущего состояния исследуемой проблемы. Все цитаты ученых сопровождаются авторскими комментариями. То есть автор показывает разные точки зрения на проблему и пытается аргументировать более правильную по его мнению.

Выводы, интерес читательской аудитории.
Выводы в полной мере являются логичными, так как они получены с использованием общепризнанной методологии. Статья может быть интересна читательской аудитории в плане наличия в ней систематизированных позиций автора применительно к вопросам формирования форм и методов предупреждения преступлений в сфере незаконного оборота наркотиков

На основании изложенного, суммируя все положительные и отрицательные стороны статьи
«Рекомендую опубликовать»

Вопросы безопасности
Правильная ссылка на статью:
Даниловская А.В. Дифференциация уголовной ответственности как элемент уголовно-правовой политики в сфере охраны добросовестной конкуренции // Вопросы безопасности. 2024. № 1. DOI: 10.25136/2409-7543.2024.1.70062 EDN: XGRDHA URL: https://nbpublish.com/library_read_article.php?id=70062

Дифференциация уголовной ответственности как элемент уголовно-правовой политики в сфере охраны добросовестной конкуренции

Даниловская Анна Владимировна

кандидат юридических наук

доцент кафедры гражданского права и гражданского процессуального права, Тихоокеанский государственный университет

680000, Россия, Хабаровский край, г. Хабаровск, ул. Тихоокеанская, 134, оф. 417

d_a_v@list.ru

Статья из рубрики "Экономическое обеспечение национальной безопасности"

DOI:

10.25136/2409-7543.2024.1.70062

EDN:

XGRDHA

Дата направления статьи в редакцию:

28-02-2024

Дата публикации:

06-03-2024

Аннотация: Предметом исследования являются вопросы дифференциации уголовной ответственности за преступления, посягающие на добросовестную конкуренцию (далее также – антиконкурентные преступления), как элемент уголовно-правовой политики в сфере охраны добросовестной конкуренции. В частности, исследуются проблемы выделения такой группы преступлений, критерии дифференциации ответственности на примере анализа как поименованных, так и не предусмотренных составами преступлений отдельных квалифицирующих признаков преступлений, иные средства дифференциации ответственности за их совершение, проблемы построения санкций за совершение преступлений рассматриваемой группы. Цель работы заключается в оценке современного состояния, выявлении проблем дифференциации уголовной

ответственности за совершение преступлений, посягающих на добросовестную конкуренцию, в свете официального признания необходимости противодействия им как угрозе экономической безопасности, определении путей их решения. Методология исследования основана на общенаучных и частнонаучных методах познания – историко-правовом, методах системного анализа, логическом, сравнительном, формально-догматическом методах, методе правового прогнозирования и классификации, анкетировании. Новизна заключается: 1) в исследовании положений УК РФ в их соотношении с ФЗ «О защите конкуренции» в целях установления критериев выделения группы антиконкурентных преступлений и обоснования дифференциации ответственности за их совершение; 2) в предложениях о выделении в качестве самостоятельных составов преступлений отдельных видов нарушений антимонопольного законодательства, за которые уголовная ответственность не установлена, а также о включении в ряд статей УК РФ признака совершения преступления в целях недобросовестной конкуренции, как дифференцирующего ответственность за преступления с незаконным оборотом объектов интеллектуальной собственности в сфере предпринимательства; 3) в анализе проблем средств дифференциации ответственности за посягательства на добросовестную конкуренцию и в предложениях по их совершенствованию, 4) в предложении вести официальный учет группы антиконкурентных преступлений при формирования статической отчетности по совершаемым преступлениям в структуре преступлений экономической и коррупционной направленности. Выводы заключаются в том, что устранение проблем дифференциации уголовной ответственности за антиконкурентные преступления, а также официальный учет таких преступлений является залогом эффективности всей уголовно-правовой политики в сфере охраны добросовестной конкуренции.

Ключевые слова:

уголовно-правовая политика, дифференциация уголовной ответственности, картель, недобросовестная конкуренция, средства дифференциации ответственности, антиконкурентные преступления, уголовная ответственность, сговор на торгах, программа смягчения ответственности, ограничивающие конкуренцию соглашения

Дифференциация ответственности за совершение преступлений, посягающих на добросовестную конкуренцию (далее также - антиконкурентные преступления) является важным элементом современной уголовно-правовой политики в сфере охраны добросовестной конкуренции в силу значимости последней для обеспечения национальной, в том числе экономической безопасности страны. Отмеченные в указах Президента РФ от 13.05.2017 г. № 208 «О Стратегии экономической безопасности Российской Федерации на период до 2030 года» и от 2.07.2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» важные задачи, связанные с противодействием монополистической деятельности и антиконкурентным соглашениям, требуют проведения исследования вопросов дифференциации ответственности в отношении всей группы общественно-опасных деяний, посягающих на добросовестную конкуренцию, в целях выявления пробелов и противоречий в правовой защите добросовестной конкуренции. Данную группу образуют преступления, признаки которых прямо или косвенно соответствуют запретам ФЗ «О защите конкуренции» и предусмотрены ст. 128^{1},146, 147, 169, 178, 180, 183, 185^{3}, 185^{6}, 200^{4}, 285 и 286 УК РФ, что нашло отражение в анализе правоприменения.

Ретроспективный анализ указывает на то, что в истории российского уголовного права дифференциация ответственности за преступления против добросовестной конкуренции существовала, по крайней мере, с принятия Уложения о наказаниях уголовных и исправительных 1845 г. [1] Так, разграничивались стачки (ст. 913, 1180) и сговоры на торгах; сговор на торгах разделялся на сговор с целью склонения других участников отказаться от участия в торгах (ст. 1181) и сговор с участием должностных лиц (ст. 498); с целью отграничения преступного деяния от непреступного проводилось разделение по количественному и качественному составу субъектов: лица, не являющиеся ни торговцами, ни промышленниками, не могли быть субъектами уголовной ответственности за сговор или стачку. Более жесткие меры наказаний применялись к зачинщикам сговора, иные участники, присоединившиеся к сговору, наказывались мягче. Дифференцировались и недобросовестные действия с использованием чужих клейм и знаков (ст. 1354), совершенные путем разглашения коммерческой тайны (ст. 1355), а также распространения на бирже вредных для хода коммерции, заведомо ложных известий (ст. 1277).

Цель дифференциации уголовной ответственности представляется в науке как наличие на стадии законотворчества такой классификации преступлений, которая давала бы практике ориентиры в применении различных мер уголовно-правового воздействия к различным категориям преступников, в зависимости от характера совершенного деяния [2, с. 42]. Достижение этой цели в уголовно-правовой политике в сфере охраны добросовестной конкуренции связано, во-первых, с самим явлением – наличием классификации преступлений по групповому объекту посягательства, критерии которой заложены Конституцией РФ в виде запрета монополизации и недобросовестной конкуренции (ст. 34), и ФЗ «О защите конкуренции», содержащим запреты форм монополистической деятельности (ст. 10-11.1), недобросовестной конкуренции (ст. 14.1-14.8), ограничивающей конкуренцию деятельности органов государственной власти или местного самоуправления (ст. 15, 16), нарушений на торгах (ст. 17); во-вторых, с основным требованием к классификации преступлений – быть непротиворечивой и характеризующей деяния общностью групповых признаков, что позволило бы их отграничить от иных преступлений.

Из перечисленных составов только предусмотренное ст. 178 УК РФ преступление напрямую отражает запрет ст. 11 ФЗ «О защите конкуренции», как запрет на одну из наиболее опасных форм монополистической деятельности – ограничивающее конкуренцию соглашение между хозяйствующими субъектами-конкурентами (картель). В то же время соотношение запретов ФЗ «О защите конкуренции» с признаками составов других преступлений позволяет сделать вывод о том, что преступления, предусмотренные ст. 128^1, 146, 147, 180, 183, 185^3, 185^6 УК РФ, соответствуют формам недобросовестной конкуренции (ст. 14.1-14.7 ФЗ «О защите конкуренции»), по ст. 169, 285 и 286 УК РФ могут быть квалифицированы ограничивающие конкуренцию акты поведения должностных лиц органов государственной власти или местного самоуправления (ст. 15, 16 ФЗ «О защите конкуренции»), по ст. 200^4 УК РФ – нарушения при осуществлении закупок посредством посягательства на принцип обеспечения конкуренции при определении поставщика (как нарушение ст. 17 ФЗ «О защите конкуренции»).

В этой связи следует отметить, что проблемы классификации преступлений однозначно выявляют и проблемы дифференциации уголовной ответственности за их совершение, а следовательно, и всей уголовно-правовой политики: отсутствие четких ориентиров

относительно характера и степени общественной опасности группы деяний, имеющих один объект посягательства, нивелирует все попытки государства успешно противодействовать посягательствам на охраняемый объект, не позволяя расставить акценты согласно требованиям безопасности общества и государства. Сказанное имеет прямое отношение к проблеме классификации антиконкурентных преступлений, которая в современном уголовном законе представлена рассогласованной совокупностью таких деяний, расположенными в разных главах УК РФ, характеризующимися противоречивыми или спорными признаками и выпадающими элементами.

Так, антиконкурентные сговоры представляют собой целую систему различных соглашений с разными участниками, но УК РФ не содержит дифференцированного подхода к уголовно-правовой оценке видов соглашений, предусматривая уголовную ответственность только за картель, то есть антиконкурентное соглашение между хозяйствующими субъектами (ст. 178 УК РФ). При этом под картелем понимается, в сущности, любое ограничивающее конкуренцию соглашение между хозяйствующими субъектами-конкурентами, в то время как сговор на торгах принципиально отличается своими признаками от классического картеля, существующего, например, в силу договора о совместной деятельности, являясь по сути разновидностью мошенничества [3, с.122-124].

Антиконкурентная деятельность должностных лиц органов власти и местного самоуправления, реализованная через сговор с хозяйствующими субъектами, представляет собой самостоятельный вид коррупционной деятельности, совершаемый в сфере экономической деятельности и имеющий направленность на ограничение конкуренции, а потому должна выделяться отдельным составом преступлений, входящих в одну группу антиконкурентных деяний. Между тем современное состояние УК РФ приводит к квалификации таких соглашений по ст. 169, 285 или 286 УК РФ, находящихся в конкуренции между собой.

Одновременно с этим требуется ликвидация пробелов в уголовно-правовой защите отдельных благ, посягательства на которые хотя и образуют противоправное поведение согласно антимонопольному закону, но по непонятным причинам не нашли воплощения в уголовно-правовом запрете при одинаковой степени ценности с однородными объектами, поставленными под такую защиту. Речь идет, в частности, о защите деловой репутации юридического лица, прав на фирменное наименование, коммерческое обозначение, на топологию интегральных микросхем, селекционное достижение, обладание правами, на которые также может составлять конкурентное преимущество хозяйствующих субъектов наряду с правами на иные, поименованные в УК РФ, объекты интеллектуальной собственности.

Наличие перечисленных пробелов уголовного закона есть явное следствие не только неверной оценки отмеченных посягательств на добросовестную конкуренцию, но и нарушает принципы справедливости и равенства всех перед законом (в их совокупности с другими принципами уголовного права), а также корреспондирующий им принцип оптимальности, предложенный в науке как принцип дифференциации ответственности [Рогова Е.В. Учение о дифференциации уголовной ответственности : дис. … д-ра юрид. наук. М., 2014. С. 164]. Так, индивидуальный предприниматель имеет возможность уголовно-правовой защиты в рамках ст. 128^1 УК РФ в случае посягательств на его деловую репутацию посредством распространения заведомо ложных сведений. У юридического лица этой возможности нет, хотя оно может признаваться потерпевшим, согласно ст. 42 УПК РФ, именно в случае причинения преступлением вреда его

имуществу и деловой репутации. Такой ситуацией, во-первых, в неравное положение поставлены потерпевшие от распространения не соответствующей действительности информации лица, и это неравенство предопределено их статусом. Во-вторых, это противоречит принципу равенства граждан перед законом и принципу вины: лицо, распространившее ложные сведения о деятельности юридического лица, не подлежит уголовной ответственности, в то время как аналогичные действия в отношении физического лица ее влекут. В-третьих, необъяснимым выглядит придание разной степени общественной опасности деяний, направленных против имеющей одинаковое для всех хозяйствующих субъектов значение деловой репутации как одного из элементов своего конкурентного преимущества и успешности экономической деятельности [4, с. 550], когда за одно из них установлены меры уголовного наказания, а за другое нет. В этой связи установление уголовной ответственности за дискредитацию означает не столько расширение и углубление сферы уголовной ответственности в соответствии с принципами уголовного права (принцип оптимальности), сколько справедливое ее установление в интересах каждого потерпевшего. В свете изложенного представляется целесообразным включить в УК РФ самостоятельный состав преступления «Дискредитация», установив в ней ответственность за распространение заведомо ложных, неточных или искаженных сведений об индивидуальном предпринимателе или организации, либо об их деятельности.

Противоречие указанным принципам усматривается и в отсутствии уголовной ответственности за сговор между должностным лицом и представителями хозяйствующих субъектов. Предусматривая уголовную ответственность за картель как антиконкурентный сговор между представителями хозяйствующих субъектов, законодатель игнорирует антиконкурентный сговор с должностным лицом. Даже если основываться на принципе экономии уголовной репрессии и квалифицировать такие действия должностного лица по ст. 169, 285, 286 УК РФ, то возникает вопрос о том, есть ли основания полагать возможным не придавать уголовно-правовое значение факту договоренности об устранении конкуренции, достигнутой должностным лицом с одним или рядом хозяйствующих субъектов, при наличии таковой без участия должностного лица (ответственность за которую предусмотрена ст. 178 УК РФ)? Ведь таким образом ответственности избегают и представители хозяйствующих субъектов.

В контексте выделения видов антиконкурентных преступлений следует также отметить принцип универсальности при дифференциации ответственности, согласно которому невозможно не учитывать многогранность и разнообразие отношений, регулируемых законом [Рогова Е.В. Учение о дифференциации уголовной ответственности. С. 165]. Так, незаконный оборот объектов интеллектуальной собственности может быть как в сфере законной предпринимательской деятельности, так и осуществляться лицами, не имеющими статуса субъекта предпринимательской деятельности. И первое, и второе – опасные явления для экономики, требующие своей реакции государства. Следовательно, нужны разные подходы и в отношении криминализации таких деяний, и к дифференциации ответственности за их совершение. Преступления, объективная сторона которых связана с незаконным оборотом объектов интеллектуальной собственности, совершенные в предпринимательской деятельности, всегда имеют антиконкурентную направленность, так как таким образом виновные лица получают конкурентные преимущества, позволяющие извлекать прибыль. Отражение повышения уровня общественной опасности при таких противоправных деяниях может быть через признак цели недобросовестной конкуренции, которая заключается в получении преимуществ при осуществлении предпринимательской деятельности посредством незаконного использования чужих объектов интеллектуальной собственности. Включение данного

признака в состав преступлений, предусмотренных ст. 146, 147, 180, 183 УК РФ, позволило бы отграничить ответственность лиц, виновных в их совершении, которыми являются исключительно субъекты экономической деятельности, от ответственности лиц, ими не являющимися.

В учении о дифференциации уголовной ответственности выделяют основания [Лесниевски-Костарева Т.А. Дифференциация уголовной ответственности : дис. … д-ра юрид. наук. М., 1999. С. 69] или критерии [Рогова Е.В. Учение о дифференциации уголовной ответственности. С. 168–176], в соответствии с которыми происходит разделение мер уголовно-правового характера. Основываясь на позиции, согласно которой в качестве таковых определяются характер и степень общественной опасности преступления, личность виновного и форма вины, отметим, что их анализ в антиконкурентных преступлениях весьма определенно указывает на необходимость проведения дифференциации уголовной ответственности за их совершение и оценки существующего ее состояния.

Так, одним из дискуссионных вопросов является квалификация картеля при наличии признаков организованной группы, которая как квалифицирующий признак не предусмотрена действующей редакцией ст. 178 УК РФ, в то время как выявление в практике картелей, имеющих признаки организованной группы, не является редкостью. Особо актуальным является ответ на вопрос о возможности квалификации деяния, совершенного организованной группой, возникшей из деятельности организации, в частности, в форме ассоциации, координирующей экономическую деятельность в рамках картеля, которая запрещена п. 5 ст. 11 ФЗ «О защите конкуренции». Анализ антимонопольной практики показывает разностороннюю роль ассоциаций и модели их антиконкурентного поведения, имеющие различную степень и характер общественной опасности [5, с. 33-37].

Действия координатора, безусловно, придают устойчивость картелю, так как им контролируются все процессы, связанные с реализацией условий соглашения. С позиции уголовного права статус лица, координирующего экономическую деятельность хозяйствующих субъектов, подпадает под признаки организатора преступления.

Такая позиция может вызвать скептическую реакцию на предмет оценки деятельности участников ассоциации как членов организованной группы, ибо здесь имеет место некоммерческая организация (ассоциация, союз), которая в соответствии со ст. 123.8 ГК РФ создается в целях координации предпринимательской деятельности объединившихся в ней лиц. Однако гражданское право изначально направлено на регулирование добросовестного поведения. В противном случае нормы ГК РФ перестают действовать и возникает вопрос о том, как квалифицировать поведение физических лиц, нарушивших закон, в частности, договорившихся организованно ограничивать конкуренцию на товарном рынке вопреки запрету ФЗ «О защите конкуренции», используя для этого правомерно созданную ассоциацию, даже если значительная часть деятельности как самой ассоциации, так и ее членов находится в рамках правового поля. Представляется вполне логичным использовать в таких ситуациях те правовые механизмы, которые позволят в полной мере дать правовую оценку всем действиям, совершенным в нарушение установленного законом запрета и имеющим признаки состава преступления, включая квалифицирующие, под которые подпадают соответствующие акты поведения. То есть в подобных ситуациях следует понимать границы действия регулятивного закона, которые заканчиваются тогда, когда акт поведения невозможно «уложить» в его правовую норму и он «переносится» в сферу влияния другого закона.

Членство в коммерческой или некоммерческой организации, послужившее основой заключения картеля, руководство такой организацией и координация ее деятельности, в том числе в связи с заключением картеля, являются теми факторами, которые обусловливают в данном случае устойчивость и объединенность ее членов как участников организованной группы, возникшей из членства в такой организации.

Данная ситуация весьма показательно демонстрирует факт того, что картелю могут быть свойственны проявления организованной группы. Следовательно, такой квалифицирующий признак необходим в целях дифференциации уголовной ответственности за него как повышающий общественную опасность деяния.

Рассматривая критерии дифференциации уголовной ответственности за картель, отмечаются также следующие их аспекты.

Такой квалифицирующий признак картеля, как совершение преступления лицом с использованием своего служебного положения, давно вызывает заслуженную критику. В частности, Т.Д. Устинова [6, с. 115], П.С. Яни [7, с. 26], О.Е. Деревягина [Деревягина О.Е. Преступное ограничение конкуренции : теоретические и прикладные аспекты : дис. … канд. юрид. наук. Красноярск, 2021. С. 172–173] отмечают конкуренцию ч. 1 и п. «а» ч. 2 ст. 178 УК РФ из-за того, что субъектом картеля зачастую является должностное лицо организации, в связи с чем квалификация его действий должна осуществляться по ч. 2 ст. 178 УК РФ, которая усиливает ответственность при наличии такого признака, в то время как действия индивидуального предпринимателя – участника картеля – будут квалифицированы по ч. 1 той же статьи.

Одновременно с этим на практике возникают затруднения при квалификации деяний служащих организаций, которые не занимают должности, связанные с выполнением управленческих функций. В данном случае признак «с использованием своего служебного положения» несправедливо уравнивает в ответственности и руководителей, от которых зависит принятие решения о заключении антиконкурентного соглашения, и обычных служащих, исполняющих распоряжения.

Законопроект «О внесении изменений в статью 178 Уголовного кодекса Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации», внесенный на рассмотрение Государственной Думой РФ 29.11.2019 г., данный признак не предусматривает, но содержит сходный с ним по значению признак совершения преступления лицом, выполняющим функции единоличного исполнительного органа, члена совета директоров или иного коллегиального исполнительного органа в коммерческой или иной организации (далее – высшее должностное лицо организации), а также лицом, распоряжающимся более чем 50 % общего количества голосов, приходящихся на голосующие акции (доли) в уставном (складочном) капитале хозяйственного общества (товарищества, хозяйственного партнерства) [Законопроект № 848246-7 «О внесении изменений в статью 178 Уголовного кодекса Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации»// URL: https://sozd.duma.gov.ru/bill/848246-7 (дата обращения: 05.01.2024)].

Включение данного признака в ч. 2 ст. 178 УК РФ можно объяснить следующим: во-первых, особой ролью в организации высшего должностного лица организации, которое принимает юридически значимые решения или имеет возможность оказать решающее влияние на принятие таковых; во-вторых, более значимой ролью коммерческих организаций на товарном рынке, чем индивидуальных предпринимателей, которые зачастую являются субъектами малого и среднего бизнеса, а значит, такие организации

способны вызвать и более серьезные негативные изменения рынка в случае ограничения конкуренции. Таким образом, несмотря на замечание Верховного Суда РФ [Официальный отзыв на проект Федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации» // URL: https://sozd.duma.gov.ru/bill/848246-7 (дата обращения: 05.01.2024)] по поводу введения рассматриваемого признака, следует признать, что он действительно разграничивает ответственность индивидуального предпринимателя и высшего должностного лица организации как лиц, вносящих потенциально разный вклад в экономику, следовательно, способных своими противоправными действиями вызвать несопоставимые по масштабам последствия.

Представляется, что помимо изложенных доводов, в этом новом квалифицирующем признаке заключено предупреждение данным лицам об особом внимании государства в виде повышенной уголовной ответственности именно за их действия по заключению и реализации картеля: рассматриваемый признак переводит преступление в категорию тяжких, что обосновано официальным признанием картелей угрозой экономической и национальной безопасности.

В связи с вышеизложенным, а также с учетом сложившейся в уголовном праве традицией дифференцировать уголовную ответственность лиц, выполняющих управленческие функции в организации, и иных служащих организации, и имеющейся проблемы на практике, связанной с квалификацией деяний последних, представляется целесообразным указать в ч. 2 ст. 178 УК РФ в качестве специального субъекта этого преступления лицо, выполняющее управленческие функции в коммерческой или иной организации. Следует отметить, что лицо, распоряжающееся более чем 50 % общего количества голосов, приходящихся на голосующие акции (доли) в уставном (складочном) капитале хозяйственного общества (товарищества, хозяйственного партнерства), не входит в перечень лиц, которые согласно примечанию к ст. 201 УК РФ могут быть признаны лицами, выполняющими управленческие функции в коммерческой или иной организации, если только они не действуют по специальному полномочию. Однако указанное лицо может оказать ключевое влияние на принятие решения органом управления организации. Следовательно, в описании квалифицирующего признака преступления, предусмотренного ст. 178 УК РФ следует указать и лицо, выполняющее управленческие функции в организации, и лицо, распоряжающееся более чем 50 % общего количества голосов, приходящихся на голосующие акции (доли) в уставном (складочном) капитале хозяйственного общества (товарищества, хозяйственного партнерства).

Проведенное исследование также показало необходимость совершенствования такого признака преступления, предусмотренного п. «б» ч. 2 ст. 178 УК РФ, как уничтожение или повреждение чужого имущества либо угроза его уничтожения или повреждения, при отсутствии признаков вымогательства. Так, М.Х. Хакулов полагает, что эффективность использования ст. 178 УК могла бы быть существенно выше, если бы законодатель не ограничил перечень угроз только насилием и уничтожением или повреждением имущества. В ходе проведенного автором опроса предпринимателей было установлено, что респонденты получали угрозы иного рода – угрозу распространения порочащих сведений, угрозу дискредитации продукции посредством реализации ее недоброкачественных подделок, угрозу экономической блокады, угрозу неконкретизированными неприятностями [Хакулов М.Х. Преступления, посягающие на свободу и добросовестность конкуренции в сфере предпринимательской деятельности : дис. … докт. юрид. наук. М. 2009. С. 112-113]. При изучении приговоров, состоявшихся

по ст. 178 УК РФ, данный факт нашел свое подтверждение. Так, В., являясь заместителем начальника государственного учреждения – государственного заказчика, предложил нескольким руководителям коммерческих организаций заключить ограничивающее конкуренцию соглашение (картель), высказав в их адрес требование отказаться от участия в аукционе, подкрепленное угрозами о том, что в случае игнорирования его предложения и невыполнения его требований будут осуществлены препятствия в приёмке выполненных ими работ [Приговор Новгородского районного суда Новгородской области № 1-347/2014 от 22.04.2014 г. // Архив ФАС РФ].

Таким образом, включение в перечень квалифицирующих признаков угрозы препятствования в осуществлении экономической деятельности лица представляется рациональным предложением, так как в действительности угрозы лицам, отказавшимся вступить в картель, могут быть различными и нередко связанными именно с осуществлением предпринимательской деятельности.

При анализе основных и квалифицирующих признаков усматривается диссонанс в соотношении квалифицирующих признаков преступлений, предусматривающих ответственность за посягательства на разные объекты интеллектуальной собственности, права на которые имеют одинаковое значение в качестве конкурентного преимущества. Например, в ст. 147 УК РФ не предусмотрены такие квалифицирующие признаки, как совершение преступления лицом с использованием своего служебного положения, который назван в ч. 3 ст. 146 УК РФ. В то же время, в ходе изучения приговоров, состоявшихся по делам о преступлении, предусмотренном ст. 147 УК РФ, было установлено, что все преступления (количество таких невелико – всего было обнаружено и изучено 5 приговоров по ст. 147 УК РФ) совершены лицами с использованием служебного положения, а именно лицами, занимающими высшие управленческие должности в организации.

Как показало исследование, преступления, предусмотренные ст. 146, 147 УК РФ, имеют выраженную экономическую направленность, что является признанным фактом, отраженным в статистической отчетности состояния преступности согласно Указанию Генпрокуратуры России № 401/11, МВД России № 2 от 19.06.2023 г. «О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности». Исходя из этого вывода, есть основания признать необходимым предусмотреть признак совершения преступления лицом, выполняющим управленческие функции в коммерческой или иной организации, в качестве квалифицирующего в ст. 147 УК РФ, и заменить им в ст. 146 УК РФ признак совершения деяния лицом с использованием своего служебного положения. Обоснование данного предложения заключается в том, что на руководителе организации лежит обязанность обеспечить всем необходимым все ее структурные подразделения для осуществления правомерной экономической деятельности. Это в равной степени распространяется на контроль руководителя организации за своевременным заключением или продлением лицензионных и иных договоров на использование чужих исключительных прав на любые объекты интеллектуальной собственности. В силу специфичности права интеллектуальной собственности как подотрасли гражданского законодательства, далеко не всякий служащий организации владеет знаниями о нем. Соответственно, элементарная низкая правовая культура в данной сфере может стать причиной совершения преступления. И именно руководитель как лицо, осуществляющее управление всеми процессами, в первую очередь во внутренних служебных правоотношениях, функционально уполномочен на недопущение такой ситуации.

Изложенный подход к рассмотренному признаку в полной мере следует распространить и на преступления, предусмотренные ст. 180 и 183 УК РФ, чьи составы имеют признаки недобросовестной конкуренции.

В качестве другого недостатка дифференциации ответственности за незаконное использование объектов интеллектуальной собственности следует назвать то, что разные по степени и характеру общественной опасности формы соучастия – группа лиц по предварительному сговору и организованная группа – отнесены к одному квалифицирующему признаку преступлений, предусмотренных ст. 146 и 147 УК РФ. Таким образом, несмотря на их явное различие, уголовная ответственность за эти формы соучастия не дифференцируется.

В качестве непоименованных квалифицирующих признаков, отражающих новые тенденции совершения преступлений против добросовестной конкуренции, повышающих общественную опасность деяний, следует отметить совершение преступления в сети Интернет и в средствах массовой информации. Деяния, совершенные в сети Интернет, признаются особо опасными в некоторых зарубежных странах, которые установили в связи с этим повышенную ответственность [8, с. 30].

Так, в нарушение прав правообладателей, без заключения соответствующих договоров, в сети Интернет распространяются объекты авторских и смежных прав – программы для ЭВМ, аудиовизуальные произведения и их исполнения и т.п.; незаконное использование чужого товарного знака, знака обслуживания или сходных с ними обозначений для однородных товаров может быть совершено в форме применения указанных средств индивидуализации без разрешения правообладателя на товарах, этикетках, упаковках этих товаров, которые предлагаются к продаже в сети Интернет, при оказании услуг в сети Интернет, а также в доменном имени и при других способах адресации.

В предпринимательстве, в силу быстрого развития интернет-торговли, такие деяния могут привести к подрыву деловой репутации, фактическому ущербу хозяйствующим субъектам-правообладателям, другим серьезным неблагоприятным последствиям и не только для этих лиц. Общественная опасность противоправного использования чужих объектов интеллектуальной собственности в сети Интернет предопределена популярностью и массовостью потребления предлагаемых в сети товаров и услуг, доступностью объектов, размещенных в цифровом пространстве, наличием широких технических возможностей их получения (потребления), что охватывается умыслом виновного лица.

Аналогичная ситуация возникает и при распространении в сети Интернет или средствах массовой информации любой значимой информации. Будь то клевета, иная заведомо ложная информация либо охраняемая особым правовым режимом информация (коммерческая, налоговая, банковская тайна, инсайдерская информация) – распространение в сети Интернет или средствах массовой информации характеризуется невозможностью полностью контролировать этот процесс, а значит потребителями такой информации может стать широкий круг неопределенных лиц, в числе которых – конкуренты хозяйствующих субъектов – правообладателей, потребители товаров (работ, услуг), которые по-разному в своих интересах воспользуются такой информацией, что также приводит или может привести к нестабильности рыночной ситуации. Таким образом, признак незаконного использования объектов интеллектуальной собственности, распространение информации в сети Интернет или в средствах массовой информации влияет на степень общественной опасности деяния, а стало быть, может иметь значение критерия, усиливающего уголовную ответственность виновного лица.

Представляется целесообразным включить соответствующий квалифицирующий (особо квалифицирующий) признак в описание преступлений, предусмотренных ст. 146, 147, 180, 183 УК РФ.

Одной из задач дифференциации уголовной ответственности является построение системы мер уголовно-правового характера с учетом тяжести воздействия каждой отдельной меры и конкретизации оснований для ее применения. В этой связи актуальны вопросы категоризации преступлений. Называемая в науке основой дифференциации [Лесниевски-Костарева Т.А. Дифференциация уголовной ответственности. С. 60; Рогова Е. В. Учение о дифференциации уголовной ответственности. С. 197], категоризация должна быть внутренне согласованной: характер и степень общественной опасности деяния должны соответствовать мере наказания. Несоответствие описания признаков преступления мере наказания, следовательно, и категории преступления, а также меры наказания – общественной опасности деяния – подрывают сами основы уголовно-правовой политики в сфере охраны соответствующих отношений. Данный тезис в полной мере присущ отдельным преступлениям из исследуемой группы. В частности, заключение картеля, признанного угрозой экономической безопасности страны, являющееся групповым преступлением, относится к категории преступлений небольшой тяжести.

В ходе настоящего исследования, в целях изучения мнения специалистов об эффективности наказаний за антиконкурентные преступления, был проведен опрос 144 сотрудников антимонопольного органа и 310 сотрудников правоохранительных органов ряда субъектов Российской Федерации, которым был задан вопрос о том, какое наказание в качестве основного должно быть предусмотрено за картель и недобросовестную конкуренцию (таблица 1).

Таблица 1 - Основное наказание за картель и недобросовестную конкуренцию

	Лишение свободы	Штраф	Принудительные работы	Лишение права занимать определенные должности или заниматься определенной деятельностью	Арест
Сотрудники антимонопольного органа	***Картель***				
	29,5	70,5	13,6	59,1	6,8
	Недобросовестная конкуренция				
	2,3	90,9	13,6	38,6	0
Сотрудники правоохранительных органов	***Картель***				
	24,3	48,7	12,2	56,5	4,3
	Недобросовестная конкуренция				
	15,7	60	8,3	44,3	4,3

Результаты данного опроса, а также проведенное исследование отечественного и иностранного опыта, международных рекомендаций позволяют сделать вывод об обоснованности выделения в качестве основных видов наказания за преступления рассматриваемой группы лишение свободы, лишение права занимать определенные должности или заниматься определенной деятельностью и штраф.

При этом современное состояние перечисленных видов наказаний следующее. Лишение свободы как наиболее суровый вид наказания установлен далеко не для каждого основного состава преступлений рассматриваемой группы. Так, не предусмотрен такой вид наказания в отношении основных составов преступлений, закрепленных в ч. 1 ст. 128^1, ч. 1 ст. 146, ч. 1 ст. 169 УК РФ. Для других преступлений срок лишения свободы варьируется в рамках от 2 лет (ч. 2 ст. 146, ч. 1 ст. 147, ч. 1 ст. 180, ч. 1 ст. 183 УК РФ) до 4 лет (ч. 1 ст. 185^3 УК РФ, ч. 1 ст. 185^6, ч. 1 ст. 285, ч. 1 ст. 286 УК РФ). Из этого следует, что либо деяния не обладают действительно значительным уровнем общественной опасности, либо законодатель явно недооценил уровень общественной опасности многих деяний и, в частности, картеля, за который лишение свободы установлено на срок до 3 лет.

При установлении наказания в виде лишения свободы законодатель нередко допускает «перешагивание» категории преступления при установлении сроков лишения свободы. Так, преступление, предусмотренное ч. 1 ст. 178 УК РФ, относится к категории преступлений небольшой тяжести, в то время как деяние, зафиксированное в ч. 2 той же статьи, - к категории тяжких; согласно ч. 1 и ч. 2 ст. 146 УК РФ категория преступлений определяется как небольшая, ч. 3 – тяжкая; в ч. 1 ст. 200^4 УК РФ описано преступление небольшой тяжести, в ч. 2 – тяжкое.

Предел штрафа за совершение антиконкурентных преступлений, содержащих признаки основного состава, составляет 500 тыс. рублей. Такой максимальный размер штрафа установлен за разные по набору признаков в основных составах преступления, в частности, за клевету, воспрепятствование законной предпринимательской и иной деятельности, картель, незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну, манипулирование рынком и незаконное использование инсайдерской информации. Минимальный размер штрафа установлен в размере 80 тыс. руб. и предусмотрен за должностные преступления (ч. 1 ст. 285 и ч. 1 ст. 286 УК РФ). При этом в большинстве статей санкции не предусматривают низшего предела штрафа, например, в ч. 1 ст. 128^1, 146, 147, 183, 200^4, 285, 286 УК РФ, а значит суд, согласно ст. 46 УК РФ, может назначить штраф по своему усмотрению, что повышает риск назначения чрезмерно мягкого наказания. Низший предел штрафа имеют санкции преступлений, предусмотренных ч. 1 ст. 169, 178, 180, 185^3 и 185^6 УК РФ.

Лишение права занимать определенные должности или заниматься определенной деятельностью установлено в качестве дополнительного наказания, назначаемого по усмотрению суда за преступления, предусмотренные ч. 1 и 2 ст. 178, 185^3, 185^6, 200^4, ч. 2 ст. 285, ч. 2 ст. 285 УК РФ. Причем за заключение картеля, квалифицируемого по ч. 1 ст. 178 УК РФ, максимальный срок этого наказания составляет лишь 1 год. В обязательном порядке лишение права занимать определенные должности или заниматься определенной деятельностью как дополнительное наказание назначается лишь в случаях, предусмотренных ч. 1 ст. 169, ч. 3 ст. 178, ч. 2 и 3 ст. 183, ч. 3 ст. 285 УК РФ. И только при наличии признаков составов преступлений, предусмотренных ч. 2 ст. 169, ч. 1 ст. 285, ч. 1 ст. 286 УК РФ, лишение права занимать определенные должности или заниматься определенной деятельностью указано в качестве основного наказания (альтернативного). Не установлен данный вид наказания за совершение преступления, предусмотренного п. «г» ч. 3 ст. 146 УК РФ, лицом с использованием своего служебного положения, что следует признать явным пробелом.

Между тем построение санкций должно основываться на требовании согласованности и

соизмеримости суровости содержащихся в ней наказаний с тяжестью преступления. При этом строится система санкций с учетом иерархической значимости общественных отношений – объектов посягательства [Густова Э.В. Построение санкций в уголовном праве Российской Федерации : теоретический аспект : дис. … канд. юрид. наук. Воронеж, 2015. С. 143]. Соответственно преступления одной группы должны иметь непротиворечивую внутреннюю систему наказаний. Так, преступления, чья объективная сторона выражается в незаконном использовании экономически равноценных по стоимости исключительных прав на объекты интеллектуальной собственности, должны быть наказуемы одинаковыми видами наказания и их размерами. Однако существующие санкции преступлений, рассматриваемых как формы недобросовестной конкуренции, демонстрируют иную картину. Например, вызывают вопросы санкции за преступления, совершенные группой лиц по предварительному сговору и организованной группой: ч. 3 ст. 146 УК РФ предусматривает лишение свободы на срок до 6 лет, ч. 2 ст. 147 – на срок до 5 лет. Отсутствие квалифицирующего признака совершения деяния лицом с использованием своего служебного положения в ст. 147 УК РФ приводит к ненаказуемости такого деяния, в то время как аналогичное деяние, признаки которого описаны в смежном составе, предусмотренном п. «г» ч. 3 ст. 146 УК РФ, наказуемо лишением свободы сроком до 6 лет, но в то же время статья не предусматривает наказание в виде лишение права занимать определенные должности или заниматься определенной деятельностью, что было бы логично.

Еще одним примером несопоставимости отдельных наказаний являются санкции должностных преступлений, предусмотренных ст. 169, 285 и 286 УК РФ. Санкции, содержащиеся в ч. 1 ст. 285 и 286 УК РФ, идентичны по каждому виду и размеру наказания при сравнимых признаках обоих составов преступлений. В то же время, если рассматривать преступления, предусмотренные ст. 169, 285 и 286 УК РФ, как смежные деяния, субъектами которых являются должностные лица органов власти или местного самоуправления, посягающие на равнозначные охраняемые объекты, то их санкции никак нельзя назвать схожими. Так, санкция ч. 1 ст. 169 УК РФ, в отличие от санкций ч. 1 ст. 285 и ч. 1 ст. 286 УК РФ, не предусматривает наказания в виде лишения свободы, а по ч. 2 лишение свободы на год меньше санкции по ч. 1 ст. 285 и ч. 1 ст. 286 УК РФ. Размеры штрафов также несопоставимы: размер штрафа, предусмотренный санкцией ч. 1 ст. 169 УК РФ, значительно превышает размеры штрафов, содержащихся в санкциях ч. 1 ст. 285 и ч. 1 ст. 286 УК РФ.

Таким образом, проведенный анализ состояния санкций за совершение антиконкурентных преступлений демонстрирует набор различных возможностей дифференциации уголовной ответственности за эти преступления, не лишенных определенных недостатков. Основным среди них следует признать несоответствие санкций уровню общественной опасности преступлений - установленные максимальные пределы лишения свободы указывают на то, что преступления рассматриваемой группы отнесены, в основном, к категории преступлений небольшой тяжести, что нельзя признать обоснованным. Размеры штрафов также не соответствуют уровню опасности антиконкурентных преступлений. Представляется, что за совершение преступления, предусмотренного ст. 178 УК РФ, как наиболее опасного за экономики антиконкурентного деяния, размер штрафа следует существенно увеличить. Иное значение в целях справедливости наказания может иметь и такой его вид как лишение права занимать определенные должности или заниматься определенной деятельностью, которое необходимо установить в качестве основного (альтернативного) наказания за ряд антиконкурентных преступлений, в частности, в виде недобросовестной конкуренции и антиконкуретной деятельности должностных лиц органов государственной власти или

местного самоуправления. В целях дифференциации наказаний в сравнении с менее тяжким преступлением представляется важным определить низший предел всех видов наказания за совершение преступлений, имеющих признаки квалифицированного (особо квалифицированного) состава преступления.

Другой актуальной проблемой дифференциации ответственности является согласование иных мер уголовно-правового характера, в первую очередь конфискации, со степенью и характером общественной опасности деяний. Так, вызывает сомнение в объективности уголовно-правовой реакции на картель (ст. 178 УК РФ) отсутствие данного преступления в перечне деяний, на которые распространяются положения п. «а» ч. 1 ст. 104^1 УК РФ о конфискации, в то время как экономическая сущность картеля и заключается в получении сверхприбыли. Представляется целесообразным включить в указанный перечень ст. 104^1 УК РФ также преступления, предусмотренные ст. 180, 185^3 и 185^6 УК РФ, как преступления одной группы, целью совершения которых также является получение прибыли.

Весьма важным для целей дифференциации уголовной ответственности, в частности, за картель, является возможность воплощения принципа экономии уголовной репрессии в совершенствование программы освобождения от уголовной ответственности, предусмотренной в примечании к ст. 178 УК РФ, до уровня ее оптимального применения. Данный вопрос не является простым, и дело даже не в законодательной технике, конструировании правовых норм таким образом, чтобы в первую очередь возможность освобождения от уголовной ответственности не была фикцией, которой она является в настоящее время из-за явного несовершенства механизма, а в необходимости установления максимального баланса публичных и частных интересов.

В этой связи представляется важным отметить следующее. Условиями освобождения от ответственности виновного физического лица является ряд действий, которые оно обязано выполнить, а именно: лицо должно первым из числа соучастников преступления добровольно сообщить о преступлении, активно способствовать его раскрытию и (или) расследованию, возместить причиненный этим преступлением ущерб или иным образом загладить причиненный вред и если в его действиях не содержится иного состава преступления. Учитывая размеры ущерба, выявляемые при реализации картельных соглашений на практике, говорить о шансах отдельного физического лица быть освобожденным от уголовной ответственности по этому основанию, вероятнее всего, не приходится. Во всяком случае, практика не знает таких примеров.

В контексте данной проблемы видится целесообразным обратить внимание на такой общий аспект ответственности за нарушение антимонопольного законодательства, как совершение его группой лиц в понимании ст. 9 ФЗ «О защите конкуренции». В судебной практике сложилось представление о такой группе как о едином субъекте, в связи с чем в правоприменении и научной среде поднимается вопрос о правовых основаниях привлечения к индивидуальной ответственности участников группы [9; 10, с. 18-23] и порядке взыскания в федеральный бюджет дохода, полученного в связи с коллективным нарушением антимонопольного законодательства, которое предусмотрено ФЗ «О защите конкуренции» как мера антимонопольной ответственности.

Как указал в своем постановлении Конституционный Суд РФ [Постановление Конституционного Суда РФ от 24.06.2009 г. № 11-П «О проверке конституционности положений пунктов 2 и 4 ст. 12, ст. 22.1 и 23.1 Закона РСФСР «О конкуренции и ограничении монополистической деятельности на товарных рынках» и ст. 23, 37 и 51 ФЗ

«О защите конкуренции» в связи с жалобами ОАО «Газэнергосеть» и ОАО «Нижнекамскнефтехим»» // СПС «КонсультантПлюс»], индивидуальная ответственность каждого участника группы не исключается, а указанное обременение в виде взыскания в федеральный бюджет дохода, полученного в связи с нарушением антимонопольного законодательства группой хозяйствующих субъектов, возлагаемое на каждого из них, должно носить пропорциональный характер. Однако данное разъяснение порождает следующую проблему: каковы справедливые критерии такой пропорциональности?

Перечисленные вопросы перекликаются с проблемой уголовной ответственности за картели. Здесь возникает необходимость определить все аспекты участия каждого физического лица – представителя хозяйствующего субъекта, участника картеля – в преступлении, предусмотренном ст. 178 УК РФ, в частности, для применения правила освобождения от ответственности, предусмотренной в примечании к статье, или же согласно общему основанию по ст. 76^1 УК РФ. Указанные правила в качестве одного из обязательных действий содержат требование о возмещении ущерба или ином заглаживании вреда, причиненного преступлением, причем имеется в виду весь ущерб или вред, причиненный всеми членами картелями. Такое требование представляется несправедливым и не соответствующим целям индивидуализации уголовной ответственности за преступление, в том числе и тогда, когда речь идет об освобождении от нее.

Представляется, что перечисленные в вышеназванном постановлении Конституционного Суда РФ конституционные принципы справедливости, юридического равенства, пропорциональности соразмерности устанавливаемой ответственности должны в равной мере распространяться на все ее проявления. В целях применения программы смягчения ответственности за картель следует определять долю участия в картеле каждого хозяйствующего субъекта и в зависимости от этого устанавливать ту часть причиненного ущерба или иного вреда, которая корреспондирует его личному участию в качестве субъекта преступления, что и должно подлежать возмещению.

Однако, если ущерб как таковой возникает в результате деятельности юридического лица хотя и на основании решений, принимаемых конкретными физическими лицами – их представителями, то возможность освобождения от ответственности именно последнего не может быть связана только с возмещением им причиненного таким образом ущерба. Обратная ситуация противоречит не только вышеуказанным конституционным принципам, но и закрепленному в УК РФ отраслевому принципу справедливости. В этой связи представляется необходимым предусмотреть возможность возмещения причиненного таким образом ущерба самим юридическим лицом - хозяйствующим субъектом – участником картеля, аналогично тому, как может быть возмещен ущерб, причиненный преступлениями, предусмотренными ст. 199 и 199^1 УК РФ, согласно разъяснениям Верховного Суда РФ о применении примечания к ст. 199 [Постановление Пленума Верховного Суда РФ от 15.11.2016 г. № 48 (в ред. от 11.06.2020) «О практике применения судами законодательства, регламентирующего особенности уголовной ответственности за преступления в сфере предпринимательской и иной экономической деятельности»; постановление Пленума Верховного Суда РФ от 27.06.2013 г. № 19 «О применении судами законодательства, регламентирующего основания и порядок освобождения от уголовной ответственности» // Российская газета. 2013, № 145 (6121)].

Что касается проблемы уголовной ответственности второго, третьего лица, в действиях которого были установлены признаки заключения и исполнения картеля, то ее решение видится в дальнейшем совершенствовании этого института, в частности, путем

возможности смягчения наказания последовательно, в зависимости от очередности обращения в правоохранительные органы, согласно ст. 64 УК РФ.

Другой недостаток усматривается из сравнения институтов освобождения от уголовной ответственности по ст. 75–76^2 УК РФ и примечания к ст. 178 УК РФ, подкрепленного практикой применения аналогичного института «смягчения ответственности» в административном праве, и заключается в допущении возможности освобождения от уголовной ответственности за картель неоднократно. По аналогии с другими институтами условием освобождения от уголовной ответственности за картель должно быть совершение деяния впервые, иначе может возникнуть ситуация рецидивов заключения картелей, как это имеет место в административном производстве [11, с. 32]. Лицо, повторно совершившее преступление, не должно иметь возможности быть освобожденным от уголовной ответственности.

Следуя традициям уголовного и административного законодательства, необходимо предусмотреть невозможность применения правил об освобождении ответственности и смягчении наказания в отношении лица, которое явилось организатором преступления, предусмотренного ст. 178 УК РФ. Кроме этого, по аналогии с примечанием к ст. 14.32 КоАП, следует лишить такой возможности физическое лицо, виновное в совершении преступления, предусмотренного ст. 178 УК РФ, и допустившее принуждение иных лиц к совершению этого преступления либо к продолжению участия в ограничивающем конкуренцию соглашении.

Следует отметить, что в практике антимонопольного органа, программа «смягчения ответственности» активно применяется. Так, антимонопольным органом правила освобождения от административной ответственности были применены в 2015 г. – 46 раз, в 2016 г. – 91, в 2017 г. – 118, в 2018 г. – 89, в 2019 г. – 67, в 2020 г. – 146 раз [Доклады ФАС о состоянии конкуренции в Российской Федерации (2007–2020 гг.) // URL: https://fas.gov.ru/documents/type_of_documents/documenty_doklady (дата обращения: 11.01.2024)]. Представляется, что межотраслевая дифференциация ответственности при решении вопроса о применении программы освобождения от ответственности за картель, условия которого предусмотрены как в УК РФ, так и в КоАП, при условии совершенствования уголовно-правового механизма, могла бы способствовать повышению эффективности выявления картелей и их расследования.

Вышеизложенное приводит к выводу о том, что дифференциация уголовной ответственности за антиконкурентные преступления, основанная на принципах уголовного закона и предложенных в науке принципах самой дифференциации, и, как следствие, четкая и понятная система таких преступлений, построенная с учетом запретов отраслевого, антимонопольного законодательства, не допускающая пробелов в защите всех сопутствующих добросовестной конкуренции интересов и предусматривающая соответствующую степени и характеру опасности этих деяний, в том числе с учетом квалифицирующих и особо квалифицирующих признаков, систему наказаний и иных мер уголовно-правового характера является залогом эффективности всей уголовно-правовой политики в сфере охраны добросовестной конкуренции.

Достижение целей дифференциации ответственности за антиконкурентные преступления может иметь важное значение для развития уголовно-правовой политики в сфере охраны добросовестной конкуренции, ибо выделение антиконкурентных преступлений в связи с наличием общности групповых признаков позволило бы отграничить их от иных преступлений и вести официальный учет антиконкурентных преступлений при формирования статической отчетности по совершаемым преступлениям в структуре

преступлений экономической и коррупционной направленности. Такой учет позволит осуществлять своевременную оценку изменений состояния, структуры и динамики преступности в сфере добросовестной конкуренции и корректировать направления не только уголовно-правовой политики в сфере охраны добросовестной конкуренции, но и конкурентной политики. В этой связи целесообразны внести соответствующие изменения в Приказ Генеральной прокуратуры РФ, МВД РФ, МЧС РФ, Минюста РФ, ФСБ РФ Минэкономразвития РФ и Федеральной службы РФ по контролю за оборотом наркотиков от 29 декабря 2005 г. № 39/1070/1021/253/780/353/399 «О едином учете преступлений», а также в Указание Генпрокуратуры России № 401/11, МВД России № 2 от 19.06.2023 г. «О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности».

Библиография

1. Таганцев Н.С. Уложение о наказаниях уголовных и исправительных 1885 года / сост. Н.С. Таганцев. – 5-е изд., доп. – Санкт-Петербург : тип. М. Стасюлевича, 1886. [4].
2. Коробеев А.И. Уголовно-правовая политика России: от генезиса до кризиса : монография / А.И. Коробеев. – Москва : Юрлитинформ, 2019.
3. Даниловская А.В., Тенишев А.П.Об уголовной ответственности за сговоры на торгах // Актуальные проблемы российского права. 2019. № 1 (98). С. 119–131.
4. Даниловская А.В. Применение ст. 1281 УК РФ «Клевета» в сфере защиты добросовестной конкуренции // Уголовное право: стратегия развития в XXI веке : материалы XVIII Междунар. науч.-практ. конф., Москва, 21–22 янв. 2021 г. / Моск. гос. юрид. ун-т им. О.Е. Кутафина. – Москва : РГ-Пресс, 2021. – С. 550–555.
5. Тенишев А.П., Великанов А.П. Роль ассоциаций в антиконкурентных соглашениях : анализ практик антиконкурентного поведения и особенностей их пресечения // Конкурентное право. 2016. № 2. С. 33– 37.
6. Устинова Т.Д. Уголовно-правовая охрана свободы конкуренции в аспекте изменений и дополнений уголовного закона // Актуальные проблемы российского права. 2016. № 7 (68). С. 110–117.
7. Яни П.С. Проблемы уголовно-правовой охраны экономики от недобросовестной конкуренции // Российская юстиция. 2010. № 11. С. 22–26.
8. Даниловская А.В. Уголовно-правовая охраны конкуренции в ЕС, ФРГ, Великобритании и Франции // Юридические исследования. 2020. № 6. С. 21-35.
9. Кобаненко М., Денченкова О. Ответственность участников группы лиц за злоупотребление доминирующим положением // Конкуренция и право. 2011. № 5. С. 27–31.
10. Мартынова О.В.Группа лиц как самостоятельный субъект злоупотребления доминирующим положением // Современная конкуренция. 2013. № 5 (41). С. 18–23.
11. Алешин К.Н., Максимов С.В.Добровольное сообщение о заключении картеля: назревшие реформы // Российское конкурентное право и экономик. 2018. № 4 (16). С. 24–33.

Результаты процедуры рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов издательства можно ознакомиться здесь.

Предметом исследования в представленной на рецензирование статье является, как это следует из ее наименования, дифференциация уголовной ответственности как элемент уголовно-правовой политики в сфере охраны добросовестной конкуренции. Заявленные границы исследования соблюдены ученым.

Методология исследования в тексте статьи не раскрывается.

Актуальность избранной автором темы исследования не подлежит сомнению и обосновывается им следующим образом: "Дифференциация ответственности за совершение преступлений, посягающих на добросовестную конкуренцию (далее также - антиконкурентные преступления) является важным элементом современной уголовно-правовой политики в сфере охраны добросовестной конкуренции в силу значимости последней для обеспечения национальной, в том числе экономической безопасности страны. Отмеченные в указах Президента РФ от 13.05.2017 г. № 208 «О Стратегии экономической безопасности Российской Федерации на период до 2030 года» и от 2.07.2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» важные задачи, связанные с противодействием монополистической деятельности и антиконкурентным соглашениям, требуют проведения исследования вопросов дифференциации ответственности в отношении всей группы общественно-опасных деяний, посягающих на добросовестную конкуренцию, в целях выявления пробелов и противоречий в правовой защите добросовестной конкуренции. Данную группу образуют преступления, признаки которых прямо или косвенно соответствуют запретам ФЗ «О защите конкуренции» и предусмотрены ст. 1281,146, 147, 169, 178, 180, 183, 1853, 1856, 2004, 285 и 286 УК РФ, что нашло отражение в анализе правоприменения". Дополнительно автору необходимо перечислить фамилии ведущих специалистов, занимавшихся исследованием поднимаемых в статье проблем, а также раскрыть степень их изученности.

Научная новизна работы проявляется в следующих заключениях и предложениях ученого: "В этой связи следует отметить, что проблемы классификации преступлений однозначно выявляют и проблемы дифференциации уголовной ответственности за их совершение, а следовательно, и всей уголовно-правовой политики: отсутствие четких ориентиров относительно характера и степени общественной опасности группы деяний, имеющих один объект посягательства, нивелирует все попытки государства успешно противодействовать посягательствам на охраняемый объект, не позволяя расставить акценты согласно требованиям безопасности общества и государства. Сказанное имеет прямое отношение к проблеме классификации антиконкурентных преступлений, которая в современном уголовном законе представлена рассогласованной совокупностью таких деяний, расположенными в разных главах УК РФ, характеризующимися противоречивыми или спорными признаками и выпадающими элементами"; "Антиконкурентная деятельность должностных лиц органов власти и местного самоуправления, реализованная через сговор с хозяйствующими субъектами, представляет собой самостоятельный вид коррупционной деятельности, совершаемый в сфере экономической деятельности и имеющий направленность на ограничение конкуренции, а потому должна выделяться отдельным составом преступлений, входящих в одну группу антиконкурентных деяний"; "Одновременно с этим требуется ликвидация пробелов в уголовно-правовой защите отдельных благ, посягательства на которые хотя и образуют противоправное поведение согласно антимонопольному закону, но по непонятным причинам не нашли воплощения в уголовно-правовом запрете при одинаковой степени ценности с однородными объектами, поставленными под такую защиту. Речь идет, в частности, о защите деловой репутации юридического лица, прав на фирменное наименование, коммерческое обозначение, на топологию интегральных микросхем, селекционное достижение, обладание правами, на которые также может

составлять конкурентное преимущество хозяйствующих субъектов наряду с правами на иные, поименованные в УК РФ, объекты интеллектуальной собственности"; "В этой связи установление уголовной ответственности за дискредитацию означает не столько расширение и углубление сферы уголовной ответственности в соответствии с принципами уголовного права (принцип оптимальности), сколько справедливое ее установление в интересах каждого потерпевшего. В свете изложенного представляется целесообразным включить в УК РФ самостоятельный состав преступления «Дискредитация», установив в ней ответственность за распространение заведомо ложных, неточных или искаженных сведений об индивидуальном предпринимателе или организации, либо об их деятельности" и многих др. Таким образом, ученый выявляет проблемы дифференциации уголовной ответственности за совершение антиконкурентных преступлений и предлагает оригинальные пути их решения. Статья вносит определенный вклад в развитие отечественной правовой науки и, безусловно, заслуживает внимания потенциальных читателей.

Научный стиль исследования выдержан автором в полной мере.

Структура работы вполне логична. Во вводной части статьи ученый обосновывает актуальность избранной им темы исследования. В основной части работы автор на основании анализа нормативного, эмпирического и теоретического материалов выявляет основные проблемы дифференциации уголовной ответственности за совершение антиконкурентных преступлений, предлагая внесение соответствующих изменений и дополнений в действующее уголовное законодательство. В заключительной части статьи содержатся общие выводы по результатам проведенного исследования.

Содержание статьи полностью соответствует ее наименованию, но не лишено небольших недостатков формального характера.

Так, автор пишет: "В-третьих, необъяснимым выглядит придание разной степени общественной опасности деяний, направленных против имеющей одинаковое для всех хозяйствующих субъектов значение деловой репутации как одного из элементов своего конкурентного преимущества и успешности экономической деятельности [4, с. 550], когда за одно из них установлены меры уголовного наказания, а за другое нет" - "деяниям, направленным...".

Ученый отмечает: "Рассматривая критерии дифференциации уголовной ответственности за картель, отмечаются также следующие их аспекты" - "При рассмотрении критериев дифференциации уголовной ответственности за картель также выделяются следующие аспекты".

Таким образом, статья нуждается в дополнительном вычитывании - в ней встречаются стилистические погрешности.

Библиография исследования представлена 11 источниками (монографиями и научными статьями). Фактически их больше (в библиографическом списке не фигурирует ряд использованных диссертационных работ). С формальной и фактической точек зрения этого вполне достаточно. Характер и количество использованных при написании статьи источников позволили ученому раскрыть тему исследования с необходимой глубиной и полнотой. Работа выполнена на высоком академическом уровне.

Апелляция к оппонентам имеется, но носит общий характер в силу направленности исследования (в работе в основном анализируются действующие уголовно-правовые нормы, в которых устанавливается уголовная ответственность за совершение антиконкурентных преступлений). Научная дискуссия ведется автором корректно. Положения работы аргументированы в должной степени и проиллюстрированы примерами.

Выводы по результатам проведенного исследования имеются ("Вышеизложенное приводит к выводу о том, что дифференциация уголовной ответственности за

антиконкурентные преступления, основанная на принципах уголовного закона и предложенных в науке принципах самой дифференциации, и, как следствие, четкая и понятная система таких преступлений, построенная с учетом запретов отраслевого, антимонопольного законодательства, не допускающая пробелов в защите всех сопутствующих добросовестной конкуренции интересов и предусматривающая соответствующую степени и характеру опасности этих деяний, в том числе с учетом квалифицирующих и особо квалифицирующих признаков, систему наказаний и иных мер уголовно-правового характера является залогом эффективности всей уголовно-правовой политики в сфере охраны добросовестной конкуренции. Достижение целей дифференциации ответственности за антиконкурентные преступления может иметь важное значение для развития уголовно-правовой политики в сфере охраны добросовестной конкуренции, ибо выделение антиконкурентных преступлений в связи с наличием общности групповых признаков позволило бы отграничить их от иных преступлений и вести официальный учет антиконкурентных преступлений при формирования статической отчетности по совершаемым преступлениям в структуре преступлений экономической и коррупционной направленности. Такой учет позволит осуществлять своевременную оценку изменений состояния, структуры и динамики преступности в сфере добросовестной конкуренции и корректировать направления не только уголовно-правовой политики в сфере охраны добросовестной конкуренции, но и конкурентной политики. В этой связи целесообразны внести соответствующие изменения в Приказ Генеральной прокуратуры РФ, МВД РФ, МЧС РФ, Минюста РФ, ФСБ РФ Минэкономразвития РФ и Федеральной службы РФ по контролю за оборотом наркотиков от 29 декабря 2005 г. № 39/1070/1021/253/780/353/399 «О едином учете преступлений», а также в Указание Генпрокуратуры России № 401/11, МВД России № 2 от 19.06.2023 г. «О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности»), обладают свойствами достоверности, обоснованности и, несомненно, заслуживают внимания научного сообщества.

Интерес читательской аудитории к представленной на рецензирование статье может быть проявлен прежде всего со стороны специалистов в сфере уголовного права при условии ее доработки: раскрытии методологии исследования, дополнительном обосновании актуальности его темы (в рамках сделанного замечания), устранении нарушений в оформлении работы.

Вопросы безопасности
Правильная ссылка на статью:
Николаев Н.В., Ильин В.В., Некрасов М.И. Актуальные вопросы противодействия современным автономным беспилотным летательным аппаратам и FPV-дронам // Вопросы безопасности. 2024. № 1. DOI: 10.25136/2409-7543.2024.1.68860 EDN: TNFGJG URL: https://nbpublish.com/library_read_article.php?id=68860

Актуальные вопросы противодействия современным автономным беспилотным летательным аппаратам и FPV-дронам

Николаев Николай Владимирович

кандидат экономических наук

Сотрудник, Академия ФСО России

302015, Россия, Орловская область, г. Орёл, ул. Приборостроительная, 35

nnv85Nikolas@list.ru

Ильин Владимир Викторович

кандидат технических наук

Сотрудник, Академия ФСО России

302015, Россия, Орловская область, г. Орёл, ул. Приборостроительная, 35

w.ilin82@yandex.ru

Некрасов Максим Игоревич

кандидат технических наук

Сотрудник, Академия ФСО России

302015, Россия, Орловская область, г. Орёл, ул. Приборостроительная, 35

nekr-maks@yandex.ru

Статья из рубрики "Технологии и методология в системах безопасности"

DOI:

10.25136/2409-7543.2024.1.68860

EDN:

TNFGJG

Дата направления статьи в редакцию:

01-11-2023

Аннотация: Высокий уровень развития беспилотной авиации предопределил

Аннотация: Высокий уровень развития беспилотной авиации предопределил возможность ее использования для решения широкого перечня задач. При этом следует констатировать, что достижения в данной сфере не всегда используются в мирных целях. Результаты анализа практики применения беспилотных летательных аппаратов (БПЛА) в современных военных конфликтах и сведений о террористических актах с их использованием позволяют сделать вывод, что наиболее сложными целями, устойчивыми к различным методам воздействия, являются современные автономные БПЛА и FPV-дроны с взрывными устройствами. Поэтому актуальным направлением исследований представляется поиск эффективных путей противодействия им. Целью работы является формирование направлений эффективного противодействия современным автономным БПЛА и FPV-дронам средствами электромагнитного, лазерного и механического воздействия. В работе применяются методы системного анализа. В статье отмечен возрастающий уровень угроз, связанных с массовым применением автономных БПЛА и FPV-дронов, представлены результаты «ревизии» и критического анализа основных методов противодействия современным БПЛА, отражающие их характеристику, достоинства и недостатки. На основе полученных результатов проведен сравнительный анализ методов противодействия автономным БПЛА и FPV-дронам. Сделан вывод, что наиболее действенными из них являются методы электромагнитного, лазерного и механического воздействия. Представлены требуемые параметры эффективного применения указанных видов воздействия на современные автономные БПЛА и FPV-дроны.Результаты исследований могут быть использованы в качестве исходных данных для создания новых и совершенствования существующих средств противодействия БПЛА в составе систем физической защиты (СФЗ). Научная новизна работы заключается в развитии научно-методического аппарата обоснования СФЗ объектов в части учета особенностей функционирования и уязвимостей современных автономных БПЛА и FPV-дронов, а также определения путей совершенствования систем противодействия им на основе применения средств электромагнитного, лазерного и механического воздействия.

Ключевые слова:

Угрозы безопасности, система физической защиты, беспилотный летательный аппарат, БПЛА, автономные БПЛА, FPV-дроны, методы противодействия БПЛА, электромагнитное воздействие, лазерное воздействие, механическое воздействие

Введение

В настоящее время развитию систем физической защиты (СФЗ) важных объектов уделяется значительное внимание [1–3]. Это обусловлено в том числе появлением новых средств реализации угроз безопасности – современных беспилотных летательных аппаратов (БПЛА) с взрывными устройствами. Так, автономные БПЛА, осуществляющие полет по загруженной программе, не излучают радиосигналы и, как следствие, не обнаруживаются специализированными средствами радиотехнической разведки из состава объектовых СФЗ. В свою очередь, БПЛА, управляемые пилотами по видео с курсовых камер в режиме «от первого лица» (далее – FPV-дроны), характеризуются малыми размерами, высокой скоростью и маневренностью, наличием оригинальных параметров каналов управления и передачи данных. Указанные летательные аппараты являются «неудобными» целями с высоким потенциалом к преодолению существующих систем безопасности. При этом автономные БПЛА и FPV-дроны обладают приемлемыми техническими параметрами (скоростью и продолжительностью полета,

грузоподъемностью) для применения в противоправных целях, например, для совершения террористических и диверсионных актов.

Для нейтрализации указанных угроз в настоящее время проводятся исследования, направленные на поиск эффективных методов противодействия таким средствам [1, 4]. Выбор метода противодействия современным БПЛА является сложной научно-технической задачей, решение которой требует учета многих факторов, например, места расположения и конфигурации объекта, особенности прилегающей территории, необходимости обеспечения электромагнитной совместимости радиоэлектронных средств и других [3, 4]. Указанное обусловливает актуальность темы данного исследования.

С учетом отмеченного целью настоящей статьи является выявление эффективных методов противодействия современным автономными БПЛА и FPV-дронами в интересах развития научно-методического аппарата обоснования СФЗ объектов.

В этой связи для достижения цели исследования оценим возможности современных БПЛА, изучим практику их применения для выявления ключевых особенностей. Проведем критический анализ основных методов противодействия БПЛА и на его основе представим их краткую характеристику, определим достоинства и недостатки. Кроме того, по результатам исследования предложим направления развития средств противодействия современным автономным БПЛА и FPV-дронам.

1. Особенности современных беспилотных летательных аппаратах

Результаты анализа возможностей и практики применения современных БПЛА [1, 4–12] позволили выделить их ключевые особенности:

– современные БПЛА обеспечивают возможность осуществления полетов в автономном режиме, при котором радиосигналы управления и передачи данных не излучаются, что делает такие летательные аппараты невидимыми для основных средств обнаружения – средств радиотехнической разведки;

– отдельные типы современных автономных БПЛА предоставляют возможность автоматического выявления и идентификации целей, а также совершения в их отношении различных действий в соответствии с заложенными алгоритмами (наблюдения, сопровождения, атаки) за счет размещения на их борту высокопроизводительных средств обработки информации для функционирования алгоритмов искусственного интеллекта;

– современные БПЛА имеют возможность изменения версии программного обеспечения, а также внедрения дополнительных каскадов усиления сигналов на борт БПЛА или наземную станцию управления (НСУ), что придает им сравнительно большую устойчивость к радиоэлектронному воздействию относительно их базовой модификации;

– широкое распространение получили высокоманевренные самодельные FPV-дроны, собранные из готовых компонентов (имеющихся в свободной продаже), которые не всегда могут быть идентифицированы средствами радиотехнической разведки по характерным параметрам радиосигналов управления и передачи данных ввиду возможности применения в их составе нетиповых схемотехнических решений и приемо-передающих устройств, работающих в уникальных частотных диапазонах;

– отдельные типы современных БПЛА, использующие для организации каналов управления и передачи данных ресурсы сетей сотовой связи, не поддаются выявлению

среди множества других абонентов имеющимися средствами радиотехнической разведки.

Проведенный анализ возможностей современных БПЛА и практики их применения в ходе специальной военной операции на Украине, а также результаты исследования существующих средств обнаружения и противодействия им позволили заключить, что наиболее сложными целями, обладающими высоким потенциалом к преодолению существующих СФЗ, выступают автономные БПЛА и FPV-дроны с взрывными устройствами. В этой связи актуальной задачей является поиск эффективных методов противодействия таким средствам.

С этой целью проведем критический анализ основных методов противодействия современным БПЛА в контексте оценки возможности их применения для борьбы с автономными БПЛА и FPV-дронами.

2. Критический анализ основных методов противодействия беспилотным летательным аппаратам

Проведенный анализ публикаций [4–15] показал отсутствие единой общепринятой классификации методов противодействия БПЛА. Вместе с тем в работах по данной тематике рассматривают следующие методы воздействия [5, 13–15]:

– радиоэлектронное;

– информационно-техническое;

– электромагнитное;

– лазерное;

– акустическое;

– механическое.

Радиоэлектронное воздействие (радиоэлектронное подавление каналов управления, передачи данных и навигации) – это метод противодействия БПЛА, при котором осуществляется генерация и излучение помеховых сигналов для затруднения (блокирования, срыва) функционирования систем БПЛА и НСУ[13]. Технические изделия, реализующие данный метод, как правило, используют заградительную шумовую помеху на типовых частотах каналов управления, передачи данных и навигации БПЛА, которая обеспечивает неприемлемое соотношение сигнал/шум в полосе пропускания радиоприемного тракта БПЛА или НСУ.

Выделяют следующие разновидности метода радиоэлектронного воздействия [5, 13]:

– подавление каналов управления и передачи данных БПЛА;

– подавление средств спутниковой радионавигации (GPS, ГЛОНАСС, Galileo, BeiDou и др.);

– комбинирование разновидностей метода радиоэлектронного воздействия.

Метод радиоэлектронного воздействия БПЛА обладает следующими основными достоинствами [4, 5]:

– расходуется только возобновляемый ресурс – электроэнергия, а не средства поражения;

– избирательное воздействие осуществляется как на определенные типы БПЛА с заданными параметрами, так и на их отдельные бортовые системы;

– воздействие обеспечивается сразу на несколько БПЛА.

Вместе с тем использование данного метода сопряжено с рядом недостатков [4, 5, 7, 13].

– возможность воздействия на каналы управления и навигации БПЛА только при условии соблюдения электромагнитной доступности, поскольку эффективность их подавления убывает пропорционально квадрату расстояния до цели;

– неспособность противодействия БПЛА, осуществляющих полет в автономном режиме (в режиме «радиомолчания») по заранее загруженной программе с использованием инерциальных или помехозащищенных навигационных систем;

– средства радиоэлектронного подавления не обеспечивают эффективное противодействие БПЛА, использующим уникальные протоколы информационного обмена и диапазоны частот для организации каналов управления и передачи данных;

– средства радиоэлектронного подавления имеют ограничения по применению, обусловленные необходимостью выполнения требований по электромагнитной совместимости с другими радиоэлектронными средствами;

– относительно невысокая эффективность противодействия БПЛА, использующим широкополосные сигналы для организации каналов управления и передачи данных;

– электромагнитное излучение средств радиоэлектронного подавления оказывает негативное влияние на операторов и другие технические средства;

– имеются правовые ограничения на применение средств подавления спутниковой радионавигации.

Важно отметить, что в настоящее время метод радиоэлектронного воздействия (подавления) является основным методом противодействия БПЛА. Однако развитие современных БПЛА в направлении повышения их помехоустойчивости для успешного функционирования в условиях сложной радиоэлектронной обстановки, а также широкое распространение самодельных FPV-дронов, работающих в уникальных частотных диапазонах, существенно снижает эффективность данного вида воздействия.

Информационно-техническое воздействие (перехват управления, спуфинг, ddos-атаки) – это метод противодействия БПЛА, при котором воздействие осуществляется путем перехвата управления, навязывания некорректных режимов функционирования бортовым системам и специальному программному обеспечению на БПЛА и/или НСУ. Для реализации указанного метода технические средства противодействия должны получить информацию об используемых протоколах управления и доступ к каналам управления и телеметрии с целью формирования и последующей передачи подменных команд или данных.

Выделяют следующие разновидности метода информационно-технического воздействия [5, 14]:

– нарушение радиообмена между БПЛА и НСУ;

– нарушение информационного обмена между БПЛА и НСУ;

– изменение специального программного обеспечения на БПЛА и/или НСУ;

– подмена сигналов спутниковой радионавигации (GPS, ГЛОНАСС, Galileo, BeiDou и др.).

Нарушение радиообмена между БПЛА и НСУ предусматривает [5, 14]:

– срыв синхронизации и/или процедуры установления связи;

– навязывание некорректных режимов функционирования в канальных или сетевых протоколах радиосети;

– переполнение входного буфера путем DOS или DDOS-атак;

– нарушение функционирования программного обеспечения микроконтроллера управления средствами радиообмена.

Нарушение информационного обмена между БПЛА и НСУ включает [5, 14]:

– перехват управления БПЛА путем подмены пульта оператора;

– подмену управляющих команд с целью перевода БПЛА в некорректный режим полета, выключения двигателей, электропитания бортовой аппаратуры и полезной нагрузки;

– подмену данных телеметрии на НСУ.

Изменение специального программного обеспечения на БПЛА и/или НСУ предполагает несанкционированное внедрение [5, 14]:

– компьютерных вирусов в специальное программное обеспечение БПЛА;

– программных закладок в БПЛА, обеспечивающих прием и выполнение команд от сторонних источников.

Подмена сигналов спутниковой радионавигации (GPS, ГЛОНАСС, Galileo, BeiDou и др.) подразумевает создание ложного радионавигационного поля (GPS-spoofing) [14].

Метод информационно-технического воздействия на БПЛА обладает следующими достоинствами [7, 9, 14]:

– расходуются не средства поражения, а только возобновляемый ресурс – электроэнергия;

– полученная информация о формате и структуре используемых протоколов управления и обмена данными позволяет установить тип БПЛА, его координаты (на основе данных от бортовой навигационной аппаратуры) и координаты НСУ, статус (состояние) систем летательного аппарата, последовательность управляющих команд, параметры и настройки программного обеспечения и др.

– информационно-техническое воздействие характеризуется скрытностью, что существенно затрудняет для оператора своевременное и адекватное принятие мер противодействия;

– подмена радионавигационного поля позволяет существенно снизить эффективность применения некоторых типов автономных БПЛА.

Выделяют следующие недостатки данного метода [4, 5, 7]:

– перехват управления БПЛА представляется весьма нетривиальной научно-технической задачей, требующей от специалистов создания и постоянного пополнения базы данных о сигнальных, форматных, потоковых и сетевых параметрах каналов радиоуправления;

– невысокая эффективность подмены отдельных команд низкоуровневого управления и данных телеметрии, поскольку каждая последующая команда от НСУ и данные телеметрии от БПЛА делают неактуальными все предыдущие;

– эффективное информационно-техническое воздействие на БПЛА требует интеграции средств радио-и радиотехнической разведки, сетевой компьютерной разведки и др. в единый комплекс;

– использование аппаратуры криптографической защиты информации, а также широкополосных сигналов в канале связи между БПЛА и НСУ существенно затрудняет информационно-техническое воздействие на БПЛА;

– имеются правовые ограничения на применение средств подмены сигналов спутниковой радионавигации.

Следует отметить, что метод информационно-технического воздействия на БПЛА активно развивается. В настоящее время наибольшее распространение получили технические решения, обеспечивающие подмену сигналов спутниковой радионавигации.

Электромагнитное воздействие (функциональное поражение СВЧ излучением) – это метод противодействия БПЛА, основанный на дистанционном выведении из строя бортовой электроники электромагнитным излучением большой мощности [4]. Технические изделия (микроволновые излучатели, СВЧ-пушки) используют узконаправленное излучение, способное изменить электрофизические параметры полупроводниковых элементов радиоэлектронных систем путем их перегрева или пробоя с целью нарушения работы бортовых систем БПЛА. Эффективность функционального поражения электромагнитным оружием зависит от таких факторов, как напряженность электрического поля в точке нахождения цели, ее конструкции, а также частоты излучения.

Достоинствами метода электромагнитного воздействия являются следующие [7, 8]:

– расходуются не средства поражения, а только возобновляемый ресурс – электромагнитная энергия;

– средства электромагнитного воздействия обладают «площадным эффектом», что обеспечивает возможность поражения одиночных и групповых целей;

– способность воздействия практически на все типы БПЛА, в том числе автономные и FPV-дроны;

– средствам электромагнитного воздействия не требуется точное целеуказание и сведения о режимах работы БПЛА;

– погодные условия (дым, дождь, туман) не оказывают существенного влияния на дальность поражения.

К недостаткам метода следует отнести [4, 7, 8]:

– средства электромагнитного воздействия не обеспечивают избирательность в отношении поражаемых целей в зоне действия;

– имеет ограничения на применение в случаях нахождения в зоне поражения различных радиоэлектронных систем (например, в условиях городской застройки, при наличии объектов инфраструктуры и др.);

– требует больших энергетических затрат;

– для существенного снижения эффективности электромагнитного воздействия достаточно применить простые схемотехнические решения, направленные на уменьшение силы наведенных токов, а также экранировать электронные компоненты БПЛА (например, с помощью «клетки Фарадея»);

– излучение средств электромагнитного воздействия оказывает негативное влияние на операторов и других лиц в зоне их действия.

Необходимо отметить, что электромагнитное воздействие является эффективным методом противодействия БПЛА, который в настоящее время активно развивается в направлении обеспечения избирательного воздействия на цели.

Лазерное воздействие (функциональное поражение лазерным излучением) – это метод противодействия БПЛА, при котором воздействие на объект осуществляется узконаправленным высокоэнергетическим электромагнитным излучением в оптическом диапазоне волн.

В зависимости от плотности потока лазерного излучения выделяют следующие основные разновидности метода [4, 7]:

– термомеханическое воздействие на элементы БПЛА (разрушение, расплавление, испарение);

– поражение оптико-электронных приборов БПЛА (матриц приемников оптико-электронных систем);

– оптическое воздействие на оптико-электронные приборы БПЛА (ослепление).

Достоинствами метода лазерного воздействия являются следующие [6–8, 10, 15]:

– расходуются не средства поражения, а только возобновляемый ресурс – электроэнергия;

– термомеханическое воздействие (разрушение, расплавление) лазерных средств характеризуется скрытностью, что существенно затрудняет для оператора своевременное и адекватное принятие мер противодействия;

– лазерные средства обладают высокой избирательностью, поскольку требуют высокой точности наведения лазерного луча на цель;

– лазерные средства могут применяться по автономным БПЛА, осуществляющим полет в режиме «радиомолчания», и FPV-дронам;

– отсутствие механической инерции, обусловливающее способность лазерного луча поражать высокоманевренные цели;

– возможность регулировки степени воздействия на объект путем изменения мощности лазерного луча (от «ослепления» оптоэлектронных систем БПЛА до его физического разрушения).

Вместе с тем существует ряд недостатков метода лазерного воздействия [4, 6–8, 15]:

– высокие требования к качеству целеуказания для средств лазерного поражения;

– высокие требования к системам наведения лазера, обусловленные необходимой точностью и продолжительностью непрерывного воздействия (0,5-15 с) на БПЛА для расплавления их элементов в условиях активного маневрирования;

– существующие лазерные установки имеют значительный интервал между сериями «выстрелов», который может достигать десятков секунд, что негативно сказывается на возможности отражения групповой атаки БПЛА;

– на эффективность лазерного воздействия существенное влияние оказывают метеоусловия (дым, дождь, туман и др.), поскольку в газах атмосферы происходит затухание лазерного луча;

– высокая технологичность обслуживания и высокое энергопотребление;

– лазерные средства (химического типа) обладают значительными массогабаритными характеристиками и высоким тепловыделением;

– для снижения эффективности лазерного воздействия достаточно применить на БПЛА специальное покрытие, способствующее рассеиванию (отражению) лазерного излучения, а также оснастить летательный аппарат распылителем аэрозолей типа «дымовая завеса»;

– высокая стоимость лазерных систем.

Следует отметить, что лазерное воздействие является перспективным методом противодействия БПЛА. Данный метод активно развивается в направлении поиска новых конструктивных решений, обеспечивающих устранение его основных недостатков.

Акустическое воздействие (акустическое подавление автономной навигационной системы) – это метод противодействия БПЛА, при котором происходит воздействие на гироскоп БПЛА акустическими колебаниями. Подобранное по частоте акустическое воздействие негативно влияет на работу гироскопических датчиков из-за эффекта резонанса. Это может приводить к дестабилизации летательного аппарата в пространстве и последующей аварии [4].

Данный метод характеризуется следующими достоинствами [4, 5]:

– расходуется только возобновляемый ресурс – электроэнергия, а не средства поражения;

– относительно невысокая стоимость технической реализации метода;

– акустические средства могут воздействовать на гироскопы автономных БПЛА, осуществляющих полет в режиме «радиомолчания».

Основные недостатки метода акустического воздействия [4, 5, 7, 8]:

– малая дальность действия существующих технических средств (до 40 м) и интенсивное звуковое воздействие мощностью порядка 140 дБ;

– сложность подбора резонансной частоты разных моделей гироскопов БПЛА для

создания аварийной ситуации;

– низкая эффективность метода противодействия БПЛА, обусловленная конструкцией гироскопов (в некоторых из них резонанс оказывает влияние только на канал ориентации по горизонтальной оси) и наличием магнитометров, дублирующих ориентацию БПЛА в горизонтальной плоскости;

– простым способом снижения эффективности данного воздействия является акустическая защита гироскопа вспененным материалом;

– требуется проработка вопросов обеспечения экологической безопасности таких средств, поскольку акустическое колебание на уровне 120-140 дБ соответствует болевому порогу и может привести к контузии оператора.

Необходимо отметить, что проведенные исследования и эксперименты выявили низкую эффективность данного метода по причине ограниченной дальности действия и требуемой высокой мощности акустического воздействия. В этой связи его применение для противодействия БПЛА считается нецелесообразным.

Механическое воздействие – это метод противодействия БПЛА, при котором происходит огневое поражение объекта (кинетическое воздействие) или его физический перехват (физическое воздействие) [4]. Огневое поражение направлено на разрушение (повреждение) БПЛА путем передачи ему кинетической энергии поражающего элемента. Физический перехват предполагает воздействие на БПЛА, приводящее к принудительной остановке и/или ограничению подвижности его конструктивных элементов.

В публикациях [4, 5, 7–12] выделены следующие основные разновидности метода механического воздействия:

– огневое поражение БПЛА средствами артиллерийского вооружения (зенитными артиллерийскими установками (ЗАУ), зенитными пулеметными установками (ЗПУ), зенитными ракетно-пушечными комплексами (ЗРПК)), управляемым ракетным вооружением (зенитно-ракетными комплексами (ЗРК), переносными зенитно-ракетными комплексами (ПЗРК)), стрелковым оружием (пулеметами, автоматами и т.д.) и БПЛА-камикадзе с взрывными устройствами;

– кинетическое воздействие БПЛА-перехватчиками таранного типа;

– применение БПЛА-перехватчиков с установленными средствами огневого поражения;

– применение систем метания объемных сетей, нитей или лент из высокопрочных материалов, клейких (вязких) и горючих аэрозолей, которые могут размещаться как на «земле» в виде ручных (портативных), мобильных и стационарных установок, так и на БПЛА-перехватчиках;

– применение специально тренированных птиц для перехвата БПЛА.

К основным достоинствам метода механического воздействия можно отнести следующие [7–11]:

– захват малогабаритных БПЛА сетью является наиболее простым в реализации и достаточно эффективным методом;

– обеспечивает возможность поражения всех типов БПЛА;

– сравнительно невысокая стоимость средств поражения (кроме управляемого ракетного вооружения) и физического перехвата;

– для средств огневого поражения БПЛА метеоусловия (дым, дождь, туман и др.) не оказывают существенного влияния.

Основными недостатками метода механического воздействия являются [7, 9, 10, 12]:

– эффективное применение средств огневого (кинетического) воздействия требует задействования высокоточных комплексов целеуказания, производительных вычислителей баллистических данных и углов упреждения, а также автоматических средств наведения;

– при огневом поражении БПЛА средствами артиллерийского вооружения (ЗАУ, ЗПУ, ЗРПК) и стрелковым оружием происходит большой расход боеприпасов;

– применение средств огневого (кинетического) воздействия сопряжено с возможностью нанесения сопутствующего ущерба жизни и здоровью людей, элементам инфраструктуры и другим материальным ценностям;

– применение БПЛА-перехватчиков таранного типа или БПЛА-камикадзе зачастую приводит к их безвозвратной потере;

– применение БПЛА-перехватчиков не является эффективным методом противодействия в случае отражения групповой атаки малогабаритных маневренных БПЛА;

– применение клейких (вязких) и горючих аэрозолей сопряжено со следующими проблемными вопросами: сильной зависимостью от метеоусловий; ограничениями на использование в городских условиях; сложностью процесса образования аэрозольного облака с требуемым уровнем концентрации действующего вещества в заданном месте; небольшим «сроком жизни» аэрозольного облака; низкой эффективностью против активно маневрирующих БПЛА и др.;

– применение наземных систем метания объемных сетей ограничено дальностью действия не более 200-300 м;

– использование хищных птиц сопряжено с большими сроками их обучения, влиянием внешних раздражителей и психо-физиологических особенностей животных на эффективность перехвата БПЛА.

Следует отметить, что механическое воздействие является сравнительно простым в реализации методом противодействия БПЛА с определенными ограничениями по применению технических средств и комплексов. При этом средства огневого поражения или физического перехвата в совокупности с системами обнаружения, целеуказания и автоматического наведения обладают достаточным потенциалом для противодействия современным БПЛА.

3. Сравнительный анализ методов противодействия автономным беспилотным летательным аппаратам и FPV-дронам

Физические основы различных методов противодействия БПЛА характеризуют теоретическую возможность воздействия на современные БПЛА или их отдельные системы. Вместе с тем достигнутый высокий уровень развития беспилотной авиации, а также современный уровень развития науки и техники в области противодействия БПЛА в совокупности накладывают существенные ограничения на возможность применения

рассмотренных методов на практике. В этой связи представим результаты сравнительного анализа методов противодействия с учетом теоретической и практической возможности воздействия на автономные БПЛА и FPV-дроны на современном этапе их развития (таблица 1).

Таблица 1 – Результаты оценки основных методов воздействия для борьбы с автономными БПЛА и FPV-дронами

Наименование метода (разновидности метода) противодействия БПЛА	Возможность воздействия на БПЛА			
	Автономные		FPV-дроны	
	Теоретическая	Практическая	Теоретическая	Практическая
1 Радиоэлектронное воздействие				
Подавление радиолинии управления и радиолинии передачи данных БПЛА	Нет	–	Есть	Имеется с ограничениями
Подавление средств спутниковой радионавигации	Есть	Имеется	Нет	–
Комбинирование разновидностей методов радиоэлектронного воздействия	Есть	Имеется	Есть	Имеется с ограничениями
2 Информационно-техническое воздействие				
Нарушение радиообмена между БПЛА и НСУ	Нет	–	Есть	Не имеется
Нарушение информационного обмена между БПЛА и НСУ (перехват управления)	Нет	–	Есть	Не имеется
Нарушение специального программного обеспечения на БПЛА и/или НСУ (перехват управления)	Нет	–	Есть	Не имеется
Подмена сигналов спутниковой радионавигации (спуфинг)	Есть	Имеется	Нет	–
3				

Электромагнитное воздействие	Есть	Имеется	Есть	Имеется
4 Лазерное воздействие				
Термомеханическое воздействие на элементы БПЛА	Есть	Имеется	Есть	Имеется
Поражение оптико-электронных приборов БПЛА	Есть	Имеется	Есть	Имеется
Оптическое воздействие на оптико-электронные приборы БПЛА	Есть	Имеется	Есть	Имеется
5 Акустическое воздействие	Есть	Не имеется	Нет	–
6 Механическое воздействие				
Огневое поражение БПЛА средствами артиллерийского вооружения, управляемым ракетным вооружением, стрелковым оружием и БПЛА-камикадзе с взрывным устройством	Есть	Имеется	Есть	Имеется
Кинетическое воздействие БПЛА-перехватчиками таранного типа	Есть	Имеется с ограничениями	Есть	Не имеется
Применение БПЛА-перехватчиков с установленными средствами огневого поражения	Есть	Имеется с ограничениями	Есть	Не имеется
Применение систем метания объемных сетей, нитей или лент из высокопрочных материалов, клейких (вязких) и горючих аэрозолей	Есть	Имеется с ограничениями	Есть	Не имеется
Применение специально тренированных птиц для перехвата БПЛА	Есть	Не имеется	Нет	–

Результаты сравнительного анализа методов противодействия автономным БПЛА и FPV-

дронам позволили сделать вывод, что наиболее действенными из них являются:

– электромагнитное воздействие;

– лазерное воздействие;

– некоторые методы механического воздействия.

Рассмотрим требуемые параметры эффективного применения указанных методов противодействия автономным БПЛА и FPV-дронам.

Результаты исследования, посвященные вопросам оценки эффективности электромагнитного воздействия на БПЛА, показывают, что при использовании СВЧ-импульсов длительностью 200-270 пс с шириной спектра 2-3 ГГц возникают разного рода отказы летательных аппаратов [16]. Так, при формировании на поверхности БПЛА напряженности электрического поля [7]:

– 0,05-0,07 кВ/м происходят обратимые эффекты: сбои при маневрировании БПЛА, в питании электродвигателей и бортовой полезной нагрузки, нарушения работы приемо-передающих устройств и т.д.;

– 1,4 кВ/м наблюдается необратимое нарушение функционирования БПЛА – потеря управления из-за отказа отдельных систем;

– от 3 кВ/м и выше происходит выведение из строя элементной базы бортовых систем БПЛА.

Для разрушения микроволновых диодов и интегральных схем требуется обеспечить мощность СВЧ-сигнала на входе радиоэлектронных элементов БПЛА от 0,006 до 0,4 Вт, коммутирующих диодов и маломощных транзисторов – 0,06-9,5 Вт, микроволновых диодов и микросхем – от 6,125 до 125 Вт, коммутирующих диодов и маломощных транзисторов – от 62 Вт [7].

Следует отметить, что существующие недостатки средств электромагнитного воздействия, обусловленные отсутствием избирательности поражаемых радиоэлектронных систем в зоне их действия, накладывают ограничения на область применения таких средств для отражения атак автономных БПЛА и FPV-дронов.

Результаты исследования, посвященные вопросам оценки эффективности лазерного воздействия на БПЛА, показывают [6, 7]:

1. Для термомеханического воздействия на элементы БПЛА путем их разрушения (расплавления, испарения) требуется удержание на элементах конструкции летательного аппарата лазерного луча мощностью 2 кВт в течение 10–15 с, а луча 20–50 кВт – 0,5–5 с. При этом на удалении 2 км угловая точность наведения лазерного луча должна быть не ниже 0,00145º.

2. Для поражения оптико-электронных приборов БПЛА необходимо создать плотность энергии лазерного излучения:

– 0,005–0,01 Дж/см² (длительность импульсов 0,3 с) на наружной поверхности фильтра объектива камеры (отвечающего за улучшения света, уменьшение отражения и защиту линзы) для превышения температуры плавления его поверхностного слоя;

– 0,01 Дж/см² на входном зрачке оптико-электронного средства для быстрого нагрева

приемника излучения до высокой температуры с последующим выходом из строя.

3. Для оптического воздействия на оптико-электронные приборы БПЛА (ослепления) требуется плотность энергии лазерного излучения менее 0,005 Дж/см².

Уровни облучения для термомеханического воздействия на элементы БПЛА и поражения их оптико-электронных приборов могут быть созданы лазерным источником с энергией излучения в импульсе 200–300 Дж на дальности 5 км [7].

Следует отметить, что поскольку автономные БПЛА и FPV-дроны находятся в движении и маневрируют, то фактическая точность ориентации лазерного луча для получения эффекта поражения БПЛА на дистанции 2 км должна быть порядка 0,001–0,002º. Данное условие характеризует высокие требования к системе наведения комплекса лазерного поражения, что существенно увеличивает его стоимость и технологичность производства.

Более перспективной и сравнительно недорогой разновидностью метода противодействия автономным БПЛА, использующим курсовую камеру для геопозиционирования или обнаружения и идентификации объектов, а также FPV-дронам является оптическое воздействие на оптико-электронные приборы БПЛА. Проведенное исследование [6, 7] показывает, что для оптического (ослепляющего) воздействия достаточно относительно низкой плотности потока лазерного излучения и малой продолжительности воздействия. Указанные факторы позволяют даже при сравнительно невысокой мощности источника лазерного излучения увеличить диаметр оптического пучка, тем самым существенно снизить требования к точности его наведения. В этой связи данный разновидность метода имеет большой потенциал для развития.

Результаты исследования, посвященные вопросам оценки эффективности механического воздействия, показывают, что [4, 7, 8]:

1. Применение стрелкового оружия для эффективного поражения маневрирующих малоразмерных целей требует задействования автоматизированных систем наведения и управления огнем. Вместе с тем даже при условно идеальном прицеливании вероятность поражения зависит от кучности боя оружия (например, для 7,62-мм пулемета Калашникова нормальная кучность боя характеризуется попаданием четырех пуль в круг диаметром 15 см на дистанции 100 м), расстояния до цели и других факторов. В этой связи гарантированное поражение таких целей требует производства нескольких серий выстрелов, а эффективная дальность стрельбы не превышает 200 м.

2. Средства артиллерийского вооружения (ЗАУ, ЗПУ, ЗРПК и т.п.) обладают высокой скорострельностью. Гарантированное поражение маневрирующих малоразмерных целей этими средствами требует значительного расхода боеприпасов даже при задействовании автоматизированных систем наведения и управления огнем. Указанное существенно снижает эффективность данной разновидности метода в части противодействия автономным БПЛА и FPV-дронам. Для устранения этого недостатка в настоящее время ведутся работы по созданию снарядов с программируемым временем подрыва. Их применение обеспечит создание облака поражающих элементов в заданной точке пространства, что снизит требования к точности наведения на цель и существенно уменьшит время поражения целей и расход боеприпасов.

3. Управляемое ракетное вооружение (ЗРК, ПЗРК) в части поражения рассматриваемых в статье БПЛА характеризуется избыточным боевым могуществом и существенно более высокой стоимостью средств поражения относительно стоимости целей. В этой связи их

массовое применение против автономных БПЛА и FPV-дронов с экономической точки зрения считается нецелесообразным. Необходимо отметить, что в настоящее время проводятся работы по созданию недорогих малогабаритных управляемых ракет ближнего радиуса действия (до 2 км) для поражения БПЛА. В качестве их боевой части используются распространенные штатные боеприпасы, например, выстрелы с осколочной гранатой, ручные гранаты и т.д.

4. Применение БПЛА-перехватчиков (камикадзе) всех типов с ручным или автоматизированным управлением не обеспечивает эффективное поражение маневрирующих малоразмерных целей вследствие недостаточной скорости реакции оператора. Между тем ведутся разработки систем автоматического наведения данных средств поражения на цель, а также беспилотных платформ с требуемыми летно-техническими характеристиками. Наиболее перспективным направлением в данной предметной области представляется внедрение алгоритмов обработки видеоданных с курсовой камеры БПЛА-перехватчика (камикадзе) для автоматического распознавания, захвата и наведения на цель. При этом исполнение указанных алгоритмов должно осуществляться на вычислительных ресурсах НСУ.

Следует отметить, что существующие недостатки средств механического воздействия, обусловленные малой эффективной дальностью поражения стрелковым оружием, значительным расходом боеприпасов средств артиллерийского вооружения, высокой стоимостью управляемого ракетного вооружения, а также сложностью наведения таких средств на малоразмерные маневрирующие цели существенно ограничивают возможность их применения для противодействия автономным БПЛА и FPV-дронам. Кроме того, использование средств механического воздействия сопряжено с возможностью нанесения сопутствующего ущерба жизни и здоровью людей, повреждения элементов инфраструктуры и других материальных ценностей.

Таким образом, результаты анализа требуемых параметров эффективного применения методов электромагнитного, лазерного и механического воздействия для поражения автономных БПЛА и FPV-дронов позволяют заключить, что оптическое (ослепляющее) воздействие на оптико-электронные приборы БПЛА представляется наиболее перспективным направлением развития методов борьбы с такими целями. Указанный подход обеспечивает возможность использования сравнительно дешевых, компактных лазерных установок с широким пучком излучения, не требующим его точного наведения и длительного удержания на цели.

Вывод

Развитие робототехнических технологий предопределило появление новых средств реализации угроз безопасности важных объектов – автономных БПЛА и FPV-дронов с взрывными устройствами. Для противодействия такого рода угрозам необходимо непрерывно совершенствовать СФЗ объектов в направлении противодействия современным БПЛА.

В статье отмечены основные особенности современных БПЛА, сделан вывод о том, что наиболее сложными целями, обладающими высоким потенциалом к преодолению существующих систем безопасности, являются современные автономные БПЛА и FPV-дроны. Приведена характеристика основных методов противодействия современным БПЛА, выделены их достоинства и недостатки. Представлены результаты сравнительного анализа данных методов, отражающие подверженность автономных БПЛА и FPV-дронов разного рода воздействию.

Кроме того, в работе приведены требуемые параметры эффективного применения методов электромагнитного, лазерного и механического воздействия для поражения автономных БПЛА и FPV-дронов, позволяющие заключить, что наиболее перспективным является оптическое воздействие на оптико-электронные приборы данных летательных аппаратов.

Полученные результаты могут быть положены в основу исследований, направленных на разработку технических решений и их применение в составе СФЗ, обеспечивающих защиту важных объектов от атак современных БПЛА.

Библиография

1. Егурнов В. О., Соколов А. М., Некрасов М. И. Модель универсальной управляющей платформы системы противодействия робототехническим комплексам // Наукоемкие технологии в космических исследованиях Земли. 2020. Т. 12. № 2. С. 79–87.
2. Егурнов В. О., Николаев Н. В., Некрасов М. И. К вопросу обоснования облика системы противодействия робототехническим комплексам на защищаемых объектах // Вооружение и экономика. 2021. № 4(58). С. 121–134.
3. Ильин В. В., Николаев Н. В., Некрасов М. И., Соколов А. М. Подход к оценке эффективности систем противодействия робототехническим комплексам на важных объектах // Вопросы безопасности. 2023. № 4. С. 15–26.
4. Егурнов В. О., Ильин В. В., Некрасов М. И., Сосунов В. Г. Анализ способов противодействия беспилотным летательным аппаратам для обеспечения безопасности защищаемых объектов // Вопросы оборонной техники. Научно-технический журнал. Серия 16. Технические средства противодействия терроризму. 2018. № 115–116. С. 51–58.
5. Беспилотные летательные аппараты военного назначения: монография, ч. 1 / В.А. Аладинский, С.В. Богдановский, В.М. Клименко, В.А. Ромашов. – Череповец: РИО ВВИУРЭ, 2019. – 613 с.
6. Ростопчин В. В. Ударные беспилотные летательные аппараты и противовоздушная оборона – проблемы и перспективы противостояния // Беспилотная авиация [Электронный ресурс]. 2019. – URL: https://www.researchgate.net/publication/331772628_udarnye_bespilotnye_letatelnye_apparaty_i_protivovozdusnaa_oborona_-problemy_i_perspektivy_protivostoania (дата обращения 19.09.2023).
7. Макаренко С. И. Противодействие беспилотным летательным аппаратам. – СПб.: Наукоемкие технологии, 2020. – 204 с.
8. Тазетдинов М. Н., Хахалев А. И., Духнов С. В. Средства и способы противодействия беспилотным летательным аппаратам // Наука ЮУрГУ: материалы 73-й научной конференции (Челябинск, 20–22 апреля 2021 г.). – Челябинск: Издательский центр ЮУрГУ, 2021. – С. 624–632.
9. Семенец В. О., Трухин М. П. Способы противодействия беспилотным летательным аппаратам // Наукоемкие технологии в космических исследованиях Земли. – 2018. Т. 10. № 3. С. 4–12.
10. Скиба В. А., Кузьмин А. А. Анализ методов и средств противодействия беспилотным летательным аппаратам в интересах Ракетных войск стратегического назначения // Военная мысль. 2021. № 11. С. 104–114.
11. Теодорович Н. Н., Строганова С. М., Абрамов П. С. Способы обнаружения и борьбы с малогабаритными беспилотными летательными аппаратами // Интернет журнал «Науковедение». 2017. Т. 9. № 1. С. 1–7.
12. Галкин Д. В., Степанов А. В. Борьба с беспилотными летательными аппаратами:

методы и средства иностранных армий // Военная мысль. 2021. № 6. С. 142–151.
13. Способы противодействия беспилотным летательным аппаратам. Часть 1 // Сайт Sky X [Электронный ресурс]. 05.09.2023. – URL: https://sky-x.pro/blog/sposoby-protivodeystviya-bespilotnym-letatelnym-apparatam (дата обращения: 15.09.2023).
14. Информационно-техническое воздействие на БПЛА. Часть 2 // Сайт Sky X [Электронный ресурс]. 05.09.2023. – URL: https://sky-x.pro/blog/informatsionno-tehnicheskoe-vozdeystvie-na-bpla (дата обращения: 15.09.2023).
15. Механическое, лазерное и микроволновое противодействие БПЛА коммерческого типа. Часть 4 // Сайт Sky X [Электронный ресурс]. 05.09.2023. – URL: https://sky-x.pro/blog/mehanicheskoe--lazernoe-i-mikrovolnovoe-protivodeys-tvie-bpla-kommercheskogo-tipa (дата обращения: 15.09.2023).
16. Sakharov K. Yu., Sukhov A. V., Ugolev V. L., Gurevich Yu. M. Study of UWB Electromagnetic Pulse Impact on Commercial Unmanned Aerial Vehicle // Proceedings of the 2018 International Symposium on Electromagnetic Compatibility (EMC Europe 2018), Amsterdam, The Netherlands, August 27–30, 2018.

Результаты процедуры рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов издательства можно ознакомиться здесь.

РЕЦЕНЗИЯ
на статью на тему «Актуальные вопросы противодействия современным автономным беспилотным летательным аппаратам и FPV-дронам».

Предмет исследования.
Предложенная на рецензирование статья посвящена актуальным вопросам противодействия современным автономным беспилотным летательным аппаратам и FPV-дронам. Автором выявляются сущностные особенности данных объектов, рассматривается проблема использования этих особенностей для целей регулирования, предлагаются механизмы совершенствования процедуры противодействия современным автономным беспилотным летательным аппаратам и FPV-дронам в нынешних условиях. В качестве непосредственного предмета исследования выступили, прежде всего, мнения ученых, а также технические характеристики рассматриваемых объектов.

Методология исследования.
Цель исследования прямо в статье заявлена: «целью настоящей статьи является выявление эффективных методов противодействия современным автономными БПЛА и FPV-дронами в интересах развития научно-методического аппарата обоснования СФЗ объектов». Исходя из поставленных цели и задач, автором выбрана методологическая основа исследования. В частности, в статье указано, что «В этой связи для достижения цели исследования оценим возможности современных БПЛА, изучим практику их применения для выявления ключевых особенностей. Проведем критический анализ основных методов противодействия БПЛА и на его основе представим их краткую характеристику, определим достоинства и недостатки. Кроме того, по результатам исследования предложим направления развития средств противодействия современным автономным БПЛА и FPV-дронам».
В частности, автором используется совокупность общенаучных методов познания: анализ, синтез, аналогия, дедукция, индукция, другие. В частности, методы анализа и

синтеза позволили обобщить и разделить выводы различных научных подходов к предложенной тематике, а также сделать конкретные выводы из доктринальной литературы.

Также автором активно использовались технические данные, которые позволили, среди прочего, провести сравнительный анализ методов противодействия автономным беспилотным летательным аппаратам и FPV-дронам. Ввиду этого был сделан, например, следующий вывод: «Применение стрелкового оружия для эффективного поражения маневрирующих малоразмерных целей требует задействования автоматизированных систем наведения и управления огнем. Вместе с тем даже при условно идеальном прицеливании вероятность поражения зависит от кучности боя оружия (например, для 7,62-мм пулемета Калашникова нормальная кучность боя характеризуется попаданием четырех пуль в круг диаметром 15 см на дистанции 100 м), расстояния до цели и других факторов. В этой связи гарантированное поражение таких целей требует производства нескольких серий выстрелов, а эффективная дальность стрельбы не превышает 200 м».

Таким образом, выбранная автором методология в полной мере адекватна цели исследования, позволяет изучить все аспекты темы в ее совокупности.

Актуальность.

Актуальность заявленной проблематики не вызывает сомнений. Имеется как теоретический, так и практический аспекты значимости предложенной темы. С точки зрения теории тема противодействия современным автономным беспилотным летательным аппаратам и FPV-дронам. Сказанное подтверждается практикой, которая свидетельствует об активном использовании указанных объектов в целях совершения различных преступлений, в том числе направленных на нарушение общественной безопасности. Сложно спорить с автором в том, что «В настоящее время развитию систем физической защиты (СФЗ) важных объектов уделяется значительное внимание [1–3]. Это обусловлено в том числе появлением новых средств реализации угроз безопасности – современных беспилотных летательных аппаратов (БПЛА) с взрывными устройствами. Так, автономные БПЛА, осуществляющие полет по загруженной программе, не излучают радиосигналы и, как следствие, не обнаруживаются специализированными средствами радиотехнической разведки из состава объектовых СФЗ. В свою очередь, БПЛА, управляемые пилотами по видео с курсовых камер в режиме «от первого лица» (далее – FPV-дроны), характеризуются малыми размерами, высокой скоростью и маневренностью, наличием оригинальных параметров каналов управления и передачи данных. Указанные летательные аппараты являются «неудобными» целями с высоким потенциалом к преодолению существующих систем безопасности. При этом автономные БПЛА и FPV-дроны обладают приемлемыми техническими параметрами (скоростью и продолжительностью полета, грузоподъемностью) для применения в противоправных целях, например, для совершения террористических и диверсионных актов».

Тем самым, научные изыскания в предложенной области стоит только поприветствовать.

Научная новизна.

Научная новизна предложенной статьи не вызывает сомнений. Во-первых, она выражается в конкретных выводах автора. Среди них, например, такой вывод:

«Развитие робототехнических технологий предопределило появление новых средств реализации угроз безопасности важных объектов – автономных БПЛА и FPV-дронов с взрывными устройствами. Для противодействия такого рода угрозам необходимо непрерывно совершенствовать СФЗ объектов в направлении противодействия современным БПЛА. В статье отмечены основные особенности современных БПЛА, сделан вывод о том, что наиболее сложными целями, обладающими высоким

потенциалом к преодолению существующих систем безопасности, являются современные автономные БПЛА и FPV-дроны. Приведена характеристика основных методов противодействия современным БПЛА, выделены их достоинства и недостатки. Представлены результаты сравнительного анализа данных методов, отражающие подверженность автономных БПЛА и FPV-дронов разного рода воздействию».

Указанный и иные теоретические выводы могут быть использованы в дальнейших научных исследованиях.

Во-вторых, автором предложены различные технические обобщения, которые могут быть полезны специалистам по рассматриваемой в статье тематике. В частности, указано следующее: «Управляемое ракетное вооружение (ЗРК, ПЗРК) в части поражения рассматриваемых в статье БПЛА характеризуется избыточным боевым могуществом и существенно более высокой стоимостью средств поражения относительно стоимости целей. В этой связи их массовое применение против автономных БПЛА и FPV-дронов с экономической точки зрения считается нецелесообразным. Необходимо отметить, что в настоящее время проводятся работы по созданию недорогих малогабаритных управляемых ракет ближнего радиуса действия (до 2 км) для поражения БПЛА. В качестве их боевой части используются распространенные штатные боеприпасы, например, выстрелы с осколочной гранатой, ручные гранаты и т.д».

Таким образом, материалы статьи могут иметь определенных интерес для научного сообщества с точки зрения развития вклада в развитие науки.

Стиль, структура, содержание.

Тематика статьи соответствует специализации журнала «Вопросы безопасности», так как она посвящена правовым проблемам, связанным с противодействием современным автономным беспилотным летательным аппаратам и FPV-дронам.

Содержание статьи в полной мере соответствует названию, так как автор рассмотрел заявленные проблемы, достиг цели исследования.

Качество представления исследования и его результатов следует признать в полной мере положительным. Из текста статьи прямо следуют предмет, задачи, методология и основные результаты исследования.

Оформление работы в целом соответствует требованиям, предъявляемым к подобного рода работам. Существенных нарушений данных требований не обнаружено.

Библиография.

Следует не очень высоко оценить качество использованной литературы. Автором активно использована литература, представленная авторами из России (Егурнов В.О., Соколов А.М., Некрасов М.И., Тазетдинов М.Н., Хахалев А.И., Духнов С.В. и др.).

Таким образом, труды приведенных авторов соответствуют теме исследования, но не обладают признаком достаточности, не способствуют раскрытию различных аспектов темы.

Апелляция к оппонентам.

Автор провел серьезный анализ текущего состояния исследуемой проблемы. Все цитаты ученых сопровождаются авторскими комментариями. То есть автор показывает разные точки зрения на проблему и пытается аргументировать более правильную по его мнению.

Выводы, интерес читательской аудитории.

Статья может быть интересна читательской аудитории в плане наличия в ней систематизированных позиций автора применительно к вопросам совершенствования правовых и технических механизмов противодействия современным автономным беспилотным летательным аппаратам и FPV-дронам.

На основании изложенного, суммируя все положительные и отрицательные стороны статьи

«Рекомендую опубликовать»

Security Issues
Правильная ссылка на статью:
Camara A. The Role of Cognitive-Information Technologies in Cybersecurity: Threat Detection and Adaptive Defense Systems // Вопросы безопасности. 2024. № 1. DOI: 10.25136/2409-7543.2024.1.69882 EDN: TMESCK URL: https://nbpublish.com/library_read_article.php?id=69882

The Role of Cognitive-Information Technologies in Cybersecurity: Threat Detection and Adaptive Defense Systems / Роль когнитивно-информационных технологий в кибербезопасности: обнаружение угроз и адаптивные системы защиты

Камара Амаду Сара

магистр, кафедра Прикладная математика и информатика, Российский университет дружбы народов

117198, Россия, Москва область, г. Москва, ул. Миклухо-Маклая, 21, кв. 803А

leosarah109@gmail.com

Статья из рубрики "Технологии и методология в системах безопасности"

DOI:

10.25136/2409-7543.2024.1.69882

EDN:

TMESCK

Дата направления статьи в редакцию:

17-02-2024

Аннотация: Предметом исследования является влияние развития машинного обучения и искусственного интеллекта на обеспечение кибербезопасности в программно-ориентированных системах. Автор подробно рассматривает такие аспекты темы, как моделирование когнитивных информационных технологий и их влияние на анализ данных, обучение и принятие решений в системах. Особое внимание уделяется угрозам кибербезопасности, с которыми сталкиваются системы искусственного интеллекта, таким как кибератаки. Автор предлагает компоненты адаптивной обороны для преодоления этих угроз, включая анализ поведенческой биометрии, автоматизированный инцидентный ответ, аналитику поведения пользователей и сущностей, а также управление уязвимостями. Эти компоненты выделяются в контексте разработки стратегий кибербезопасности в современной цифровой среде, что имеет критическое значение для обеспечения защиты чувствительной информации и инфраструктуры.

Методология исследования включает анализ существующих угроз кибербезопасности и выявление их воздействия на системы искусственного интеллекта. Применяются методы аналитики данных и моделирования с учетом специфики информационных технологий. Исследование также основывается на анализе современных методов адаптивной киберзащиты. Основными выводами проведенного исследования является не только выявление угроз кибербезопасности для систем искусственного интеллекта, но и предложение компонентов адаптивной обороны для их эффективного преодоления. Новизна исследования заключается в анализе влияния когнитивно-информационных технологий на стратегии кибербезопасности и предложении инновационных подходов к защите данных и инфраструктуры в современной цифровой среде. Особым вкладом автора в исследование темы является системный анализ различных угроз и разработка комплексных рекомендаций по обеспечению кибербезопасности. В рамках исследования также выявлены перспективы развития киберзащиты в контексте быстро меняющейся киберугрозы, что открывает новые горизонты для дальнейших исследований и разработок в данной области. Полученные выводы представляют собой значимый вклад в понимание и обеспечение безопасности в цифровой среде.

Ключевые слова:

Когнитивно-информационные технологии, Кибербезопасность, Обнаружение угроз, Адаптивные системы защиты, Искусственный интеллект, Машинное обучение, Уязвимости, Компьютерная безопасность, Анализ угроз, Поведенческая биометрия

Introduction

In the digital age, cybersecurity has become a paramount concern for individuals, businesses, and governments alike. The ever-evolving landscape of cyber threats necessitates innovative approaches to safeguard sensitive information and infrastructure. As the complexity and scale of cyberattacks increase, traditional security measures alone may no longer suffice. Enter cognitive-information technologies – a cutting-edge paradigm that leverages the power of artificial intelligence, machine learning, and big data to enhance threat detection and create adaptive defense systems. Due to its ability to evaluate security threats in real-time and take appropriate action, artificial intelligence has emerged as a key component of cyber security. Threat detection and prevention are the focus of AI's role in cybersecurity. AI can be used to prevent attacks. AI also can recognize potential threats before they occur and take action to avoid them by assessing past attacks and detecting similarities. Creating automated incident response systems is another important function of artificial intelligence in cybersecurity. Because of its ability to analyze vast volumes of data in real time and automate incident response, AI is swiftly becoming into a key tool for efficient cybersecurity in today's digital environment [1]. In this article, we explore the pivotal role of cognitive-information technologies in bolstering cybersecurity efforts.

Understanding Cognitive-Information Technologies

Cognitive-information technologies refer to a set of advanced computing solutions that simulate human-like thinking processes, allowing systems to learn, adapt, and make decisions based on data analysis. These technologies rely on artificial intelligence (AI) and machine learning (ML) algorithms to process vast amounts of information, enabling them to recognize patterns, anomalies, and trends that could indicate potential cybersecurity

threats [2].

Some examples of cognitive-information technologies that rely on artificial intelligence (AI) and machine learning (ML).

Natural Language Processing (NLP): NLP enables computers to understand, interpret, and generate human language. It is the technology behind virtual assistants like Siri and chatbots that can engage in human-like conversations. NLP is crucial for processing unstructured data, such as text from social media, emails, or documents, to derive valuable insights [3].

Image and Video Recognition: AI and ML algorithms can be trained to recognize patterns, objects, and even human faces in images and videos. This technology is used in various applications, including facial recognition for security purposes, content moderation on social media, and autonomous vehicles' visual perception systems [4].

Speech Recognition: Speech recognition technology converts spoken language into text, enabling voice-activated assistants and dictation systems. It finds applications in voice-controlled devices, transcription services, and interactive voice response (IVR) systems [5].

Predictive Analytics: AI and ML can analyze historical data to identify patterns and trends and make predictions about future events. Businesses use predictive analytics for various purposes, such as forecasting customer behavior, optimizing supply chain management, and anticipating equipment failures [6].

Recommendation Systems: These systems are prevalent in online platforms like e-commerce websites and streaming services. AI algorithms analyze user behavior and preferences to provide personalized recommendations, suggesting products, movies, music, or content that users are likely to be interested in [7].

Healthcare Diagnostics: AI and ML are employed in medical imaging to assist in diagnosing diseases and conditions by analyzing X-rays, MRI scans, and other medical images. These technologies can help identify abnormalities and assist medical professionals in providing more accurate diagnoses [8].

Virtual Assistants and Chatbots: Virtual assistants like Google Assistant and Amazon Alexa, as well as chatbots used in customer support, employ NLP and other AI techniques to understand user queries and respond appropriately [9].

These are just a few examples of how cognitive-information technologies, driven by AI and ML, are transforming various industries, and enhancing the way we process information and make decisions. The capabilities of these technologies continue to evolve, and they are expected to play an increasingly significant role in our daily lives and businesses in the future.

Threat Detection - Staying Ahead of the Game

Cybersecurity intelligence is conducted to develop information on four levels: Strategic, Operational, Tactical, and Asymmetrical. Strategic intelligence should be developed for the board of directors, senior management, and the CRG committee. Operational intelligence should be designed to provide security professionals with an understanding of threats and operational environment vulnerabilities. Tactical intelligence must provide directional guidance for offensive and defensive security strategies. Asymmetrical intelligence

strategies include monitoring the cyber black market and other market intelligence from law enforcement and other means as possible. In the realm of cybersecurity, early detection of threats is crucial. Traditional security solutions typically employ rule-based approaches, which rely on predefined signatures to identify known threats. However, these methods fall short when dealing with novel, zero-day attacks. Cognitive-information technologies offer a significant advantage in this regard, as they excel at identifying emerging threats without relying on preconceived notions [10].

Machine learning algorithms can analyze historical and real-time data, enabling systems to recognize subtle deviations from normal behavior and raise red flags when anomalies occur. This proactive approach allows cybersecurity teams to stay one step ahead of cybercriminals, identifying potential threats even before they materialize into full-fledged attacks [11].

Cognitive information technologies based on artificial intelligence (AI) and machine learning (ML), which play a crucial role in strengthening cybersecurity efforts.

Anomaly Detection: Anomaly detection involves identifying unusual patterns or behaviors in data that might indicate potential threats. This technology is crucial for early detection of emerging threats and suspicious activities that do not match typical patterns [12, 13].

Threat Intelligence Analysis: Threat intelligence analysis utilizes AI and ML to process and analyze vast amounts of data from various sources to identify and understand potential threats. This helps organizations stay informed about the latest cyber threats and trends, enabling them to proactively defend against new attack vectors [14].

Phishing Detection and Email Security: AI-powered phishing detection systems can analyze email content, sender behavior, and patterns to identify phishing attempts and malicious emails. Staying ahead of phishing attacks is critical as they remain one of the most common attack vectors used by cybercriminals. Phishing intends to deceive users and can be used as a technique to steal information or gain unauthorized access to a network [15, 16, 17].

Next-Generation Firewalls: Next-generation firewalls (NGFWs) incorporate AI and ML to analyze network traffic in real-time and detect potential threats. These advanced firewalls can identify and block sophisticated attacks, including those attempting to exploit application vulnerabilities [18].

Network Traffic Analysis: Network traffic analysis with AI capabilities allows for the identification of suspicious patterns and potential cyber threats traversing the network. This technology is essential for detecting and mitigating threats before they cause significant damage [19, 20].

Adaptive Defense Systems - The Power of Dynamic Responses

Cybersecurity is no longer a reactive endeavor. Attackers have become more sophisticated, capable of adapting their strategies to bypass conventional security measures. As such, businesses and organizations must adopt a dynamic defense strategy that can evolve in response to new threats. Cognitive-information technologies lay the foundation for such adaptive defense systems.

Through continuous learning and pattern recognition, AI-driven cybersecurity systems can

adjust their response mechanisms based on the changing threat landscape. These systems can autonomously adapt their defenses, swiftly identifying and neutralizing new threats. This adaptability significantly reduces response times and minimizes the damage caused by potential breaches, enhancing overall cybersecurity resilience [21].

Behavioral Biometrics: Behavioral biometrics provides an adaptive defense mechanism by continuously monitoring and authenticating users based on their behavioral patterns. It helps in identifying unauthorized access attempts and potential account compromises [22, 23, 24].

Automated Incident Response: Automated incident response systems use AI and ML to detect and respond to certain types of cyber threats without human intervention. This adaptive defense approach ensures swift and efficient mitigation of known threats [25].

User and Entity Behavior Analytics (UEBA): UEBA solutions help in building adaptive defense systems by monitoring and analyzing user and entity behavior within an organization's network. Any deviations from normal behavior trigger alerts, allowing for proactive defense against insider threats and anomalies [26].

Vulnerability Management: Vulnerability management with AI capabilities allows for adaptive prioritization of security patches based on risk and potential impact. This ensures that critical vulnerabilities are addressed promptly to reduce the attack surface [27].

In summary, both for "Threat Detection" and "Adaptive Defense Systems," the mentioned technologies are instrumental and crucial because they provide essential capabilities to detect, analyze, and respond to cyber threats effectively, ensuring a higher level of security for organizations and staying ahead of evolving cyber risks.

Cybersecurity trends

In this article, Jim Boehm, Dennis Dias, Charlie Lewis, Kathleen Li, and Daniel Wallance explore cybersecurity trends and emphasize the importance of being prepared for accelerated digitization and understanding the cybersecurity implications of technology investments in the future. They highlight defensive capabilities that organizations can develop to mitigate future cyber threats, emphasizing the need for over-the-horizon defensive capabilities in the face of digital disruption. [30].

Big Data and Cognitive Insights

The rise of big data has transformed the way organizations approach cybersecurity. The vast amounts of data generated daily can overwhelm conventional security analysts, making it challenging to identify relevant patterns or derive meaningful insights manually. Cognitive-information technologies come to the rescue by processing and analyzing big data more efficiently. AI algorithms can process massive datasets to uncover hidden patterns and relationships between various data points. By identifying relevant signals from the noise, cognitive-information technologies help security analysts focus their efforts on high-priority threats, streamlining the decision-making process and maximizing the effectiveness of security measures [28].

Challenges and Ethical Considerations

While cognitive-information technologies hold immense promise for revolutionizing cybersecurity, they also come with their fair share of challenges and ethical considerations. One significant concern is the potential for bias in AI algorithms, which can lead to false positives or negatives in threat detection. Additionally, ensuring data privacy and security is of paramount importance when dealing with sensitive information. Moreover, the increasing sophistication of AI-driven attacks presents a Catch-22 situation where AI is both a tool for defense and an instrument for potential attacks. Striking the right balance between innovation and safety requires a collaborative effort from governments, businesses, and researchers to establish ethical frameworks and regulations [29].

Conclusion

In an ever-evolving cyber landscape, cognitive-information technologies offer a promising path towards robust cybersecurity. The integration of AI, machine learning, and big data analytics empowers organizations to detect threats in real-time, adapt defenses dynamically, and gain valuable insights from vast amounts of data. However, as we harness the power of these technologies, we must also address ethical concerns and ensure the responsible use of AI in safeguarding our digital world. By leveraging cognitive-information technologies responsibly, we can foster a safer and more secure digital future for everyone. This article sheds light on the different types of cybersecurity attacks and their

corresponding defense mechanisms in a detailed and comprehensive manner. Growing threats and attacks in emerging technologies, often manifest in different forms. It is worth noting that it is challenging to capture all patterns of threats and attacks. Therefore, this article attempted to capture a common set of general threat and attack patterns that are specifically targeted towards AI/ML systems.

Библиография

1. Ризви, В. (2023). Усиление кибербезопасности: сила искусственного интеллекта в обнаружении и предотвращении угроз. Международный журнал передовых исследований в инженерии и науке (IJAERS), 10(5), май 2023. https://dx.doi.org/10.22161/ijaers.105.8
2. Цзян, Й., и Атиф И. (2021). Селективная ансамблевая модель для когнитивного анализа кибербезопасности. Журнал компьютерных и сетевых приложений, 193, ноябрь 2021, 103210. https://doi.org/10.1016/j.jnca.2021.103210
3. Чэн, С., Си, Х., и Тао, С. (2022). Видение, статус и исследовательские темы обработки естественного языка. Журнал обработки естественного языка, 1, 2022, 100001. https://doi.org/10.1016/j.nlp.2022.100001
4. Динг, И., и Лю, И. (2022). Новый метод распознавания действий с небольшим числом обучающих примеров: временные реляционные кросс-трансформеры на основе пирамиды различий изображений. IEEE Access, 10, 94536 – 94544. 10.1109/ACCESS.2022.3204404
5. Ке, Х., Луо, Ф., и Ши, М. (2023). Проектирование модели распознавания эмоций речи. Труды по инженерии, 38(1), 86. https://doi.org/10.3390/engproc2023038086
6. Эгвим, С. Н., Алака, Х., Ториола-Кокер, Л. О., Балогун, Х., и Сунмола, Ф. (2021). Применение искусственного интеллекта для прогнозирования задержек в строительных проектах. Машинное обучение с приложениями, 6, 15 декабря 2021, 100166. https://doi.org/10.1016/j.mlwa.2021.100166
7. Ислек, И., и Огудучу, С. Г. (2022). Иерархическая система рекомендаций для электронной коммерции с использованием онлайн-отзывов пользователей. Исследования и приложения в области электронной коммерции, 52, март–апрель 2022, 101131. https://doi.org/10.1016/j.elerap.2022.101131
8. Хабуза, Т., Наваз, А. Н., Хашим, Ф., Альнаджар, Ф., Заки, Н., Серхани, М. А., и Статсенко, Й. (2021). Применение искусственного интеллекта в робототехнике, анализе диагностических изображений и медицине точности: текущие ограничения, будущие тенденции, рекомендации по системам компьютерной помощи в медицине. Информатика в медицине (Informatics in Medicine Unlocked), 24, 2021, 100596. https://doi.org/10.1016/j.imu.2021.100596
9. Гкинко, Л., и Эльбанна, А. (2023). Аппроприация разговорного искусственного интеллекта на рабочем месте: таксономия пользователей чат-ботов с искусственным интеллектом. Международный журнал управления информацией, 69, апрель 2023, 102568. https://doi.org/10.1016/j.ijinfomgt.2022.102568
10. Бон, Дж. (2017). Когнитивный хак: новое поле битвы в кибербезопасности ... Человеческий разум. Издательство Auerbach. С. 156-160.
11. Chio, C., & Freeman, D. (2018). Машинное обучение и безопасность: Защита систем с использованием данных и алгоритмов (1-е издание). O'Reilly Media. С. 25-45.
12. Ахмад, Р., Алсмади, И., Альхамдани, В., & Тавальбех, Л. (2023). Обнаружение атак нулевого дня: систематический обзор литературы. Обзор искусственного интеллекта. https://doi.org/10.1007/s10462-023-10437-z

13. Кандхро, И. А., Аланази, С. М., Али, Ф., Кехар, А., Фатима, К., Уддин, М., & Каруппайа, С. (2023). Обнаружение в реальном времени злонамеренных вторжений и атак в кибербезопасных инфраструктурах, оснащенных интернетом вещей. IEEE Access, 11, стр. 9136-9148. 10.1109/ACCESS.2023.3238664
14. Эйнсли, С., Томпсон, Д., Мейнард, С., & Ахмад, А. (2023). Кибер-разведка: обзор и исследовательская программа для практики принятия решений в области безопасности. Компьютеры и безопасность, 132, 103352. https://doi.org/10.1016/j.cose.2023.103352
15. Дьюис, М., & Виана, Т. (2022). Phish Responder: гибридный метод машинного обучения для обнаружения фишинга и спам-писем. Прикладные системные инновации, 5(4), 73. https://doi.org/10.3390/asi5040073
16. Хуаньес-Мартино, Ф., Алаиз-Родригес, Р., Гонсалес-Кастро, В., Фидалго, Е., & Алегре, Е. (2023). Обзор обнаружения спама в электронной почте: анализ стратегий спамеров и проблемы сдвига набора данных. Обзор искусственного интеллекта, 56, 1145–1173. https://doi.org/10.1007/s10462-022-10195-4
17. Мугхайд, А., АльЗу'би, С., Хнаиф, А., Таамне, С., Альнаджар, А., & Абу Элсоуд, Э. (2022). Интеллектуальная система обнаружения фишинга в кибербезопасности с использованием техник глубокого обучения. Кластерные вычисления, 25, 3819–3828. https://doi.org/10.1007/s10586-022-03604-4
18. Неупане, К., Хаддад, Р., & Чен, Л. (2018). Брандмауэр следующего поколения для сетевой безопасности: обзор. Доклад представлен на SoutheastCon 2018, Санкт-Петербург, Флорида, США, стр. 1-6. IEEE. 10.1109/SECON.2018.8478973.
19. Ким, Дж., & Сим, А. (2019). Новый подход к мультивариативному анализу сетевого трафика. Журнал по компьютерным наукам и технологиям, 34, 388–402. https://doi.org/10.1007/s11390-019-1915-y
20. Аббаси, М., Шахраки, А., & Тахеркорди, А. (2021). Глубокое обучение для мониторинга и анализа сетевого трафика (NTMA): обзор. Компьютерные коммуникации, 170, 19-41. https://doi.org/10.1016/j.comcom.2021.01.021
21. Алотаиби, А., & Рассам, М. А. (2023). Атаки на обучение соперничеством машинного обучения на системы обнаружения вторжений: обзор стратегий и защиты. Будущий интернет, 15, 62. https://doi.org/10.3390/fi15020062
22. Баиг, А. Ф., Эскеланд, С., & Янг, Б. (2023). Сохранение конфиденциальности непрерывной аутентификации с использованием поведенческой биометрии. Международный журнал информационной безопасности, 1-10. https://doi.org/10.1007/s10207-023-00721-y
23. Траоре, И., Воунганг, И., Обайдат, М. С., Наккаби, Й., & Лай, И. (2014). Онлайн аутентификация на основе рисков с использованием поведенческой биометрии. Мультимедийные инструменты и приложения, 71, 575–605. https://doi.org/10.1007/s11042-013-1518-5
24. Шалини П., & Шанкараия. (2022). Социальный поведенческий биометрический мультимодальный союз для предотвращения создания поддельных аккаунтов в Facebook. Мультимедийные инструменты и приложения, 81, 39715–39751. https://doi.org/10.1007/s11042-022-13104-7
25. Бан, Т., Такахаши, Т., Ндичу, С., & Иноуэ, Д. (2023). Преодоление усталости от тревоги: ИИ-помощник в рамках системы мониторинга информационной безопасности для эффективного реагирования на инциденты. Прикладные науки, 13, 6610. https://doi.org/10.3390/app13116610
26. Ренгараджан, Р., & Шекар Бабу. (2021). Обнаружение аномалий с использованием

аналитики поведения субъектов и визуализации данных. VIII Международная конференция IEEE по вычислительной технике для устойчивого глобального развития (INDIACom), Нью-Дели, Индия, стр. 842-847. https://ieeexplore.ieee.org/document/9441226

27. Малик, А. А., & Тош, Д. К. (2023). Динамическая классификация уязвимостей для улучшенного киберситуационного осведомленности. Конференция IEEE по системам (SysCon), Ванкувер, Британская Колумбия, Канада, 2023, стр. 1-8. 10.1109/SysCon53073.2023.10131235.
28. Андраде, Р., Торрес, Ж., & Телло-Окендо, Л. (2018). Задачи когнитивной безопасности с использованием инструментов Big Data. Международная конференция по вычислительным наукам и вычислительному интеллекту (CSCI), Лас-Вегас, Невада, США, стр. 100-105. 10.1109/CSCI46756.2018.00026.
29. Лоренц, Б., & Киккас, К. (2020). Педагогические вызовы и этические соображения при развитии критического мышления в кибербезопасности. 20-я международная конференция по передовым технологиям обучения (ICALT) IEEE, Тарту, Эстония, 2020, стр. 262-263. 10.1109/ICALT49669.2020.00085.
30. Бём, Дж., Диас, Д., Льюис, К., Ли, К., & Уоллэнс, Д. (2022). Тенденции кибербезопасности: взгляд в будущее. McKinsey & Company. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizo

Результаты процедуры рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов издательства можно ознакомиться здесь.

Рецензируемая статья посвящена исследованию ключевой роли когнитивно-информационных технологий в укреплении кибербезопасности.
Методология исследования базируется на обобщении научных публикаций зарубежных и отечественных ученых по рассматриваемой в статье проблематике, применении общенаучных методов.
Актуальность работы авторы связывают с тем, что, в цифровую эпоху кибербезопасность превращается в одну из первостепенных проблем как для частных лиц, так и для предприятий и правительств, а постоянно меняющийся ландшафт киберугроз требует инновационных подходов к защите конфиденциальной информации и инфраструктуры, поскольку одних только традиционных мер безопасности может быть недостаточно.
Научная новизна работы, по мнению рецензента, заключается в выводах о том, что когнитивно-информационные технологии могут найти применение в борьбе с различными типами кибератак и разработке соответствующих механизмов защиты.
В тексте публикации структурно выделены следующие разделы: Введение, Понятие когнитивно-информационных технологий, Обнаружение угроз: быть на шаг впереди, Адаптивные системы защиты – сила динамического реагирования, Тенденции кибербезопасности, Большие данные и когнитивная аналитика, Этические проблемы, Заключение, Библиография.
Когнитивно-информационные технологии рассматриваются в статье как передовая парадигма, которая использует возможности искусственного интеллекта, машинного обучения и больших данных для улучшения обнаружения угроз и создания адаптивных систем защиты. Когнитивно-информационные технологии относятся к набору передовых вычислительных решений, которые имитируют процессы человеческого мышления,

позволяя системам обучаться, адаптироваться и принимать решения на основе анализа данных. Эти технологии используют алгоритмы машинного обучения и искусственного интеллекта для обработки огромных объемов информации, что позволяет им распознавать закономерности, аномалии и тенденции, которые могут указывать на потенциальные угрозы кибербезопасности. В публикации приведены примеры успешного применения когнитивно-информационных технологий в различных сферах: обработка естественного языка, распознавание изображений и видео, распознавание речи, предиктивная аналитика, рекомендательные системы, диагностика в здравоохранении, виртуальные помощники и чат-боты, а также предпринята попытка их адаптации к решению проблем обеспечения кибербехопасности. В частности, авторы уделяют внимание обнаружению аномалий, аналитике угроз, обнаружению фишинга и защита электронной почты, межсетевым экранам нового поколения для анализа сетевого трафика в режиме реального времени и обнаружения потенциальных угроз. Отмечено, что разведка кибербезопасности проводится для получения информации на четырех уровнях: стратегическом, оперативном, тактическом и асимметричном, а кибербезопасность больше не является реактивной деятельностью, поскольку динамическая стратегия защиты может развиваться и самообучаться в ответ на новые угрозы, и таким образом, когнитивно-информационные технологии закладывают основу для адаптивных защитных систем.

Библиографический список включает 30 источников – научные публикации на русском и английском языках по рассматриваемой теме. В тексте публикации имеются адресные отсылки к списку литературы, подтверждающие наличие апелляции к оппонентам.

Из резервов улучшения статьи следует отметить, что, последние три раздела статьи, предшествующие Заключению, представляют собой краткое изложение в нескольких предложениях материала какого-то одного источника, чего вряд ли достаточно.

Тема статьи актуальна, материал отражает результаты проведенного авторами исследования, соответствует тематике журнала «Вопросы безопасности», может быть опубликована после устранения отмеченной выше недоработки.

Вопросы безопасности
Правильная ссылка на статью:
Перелыгин И.М. Анализ программных продуктов и изучение автоматизации процессов в сфере мониторинга закупок и товаров // Вопросы безопасности. 2024. № 1. DOI: 10.25136/2409-7543.2024.1.69887 EDN: VLWPDM URL: https://nbpublish.com/library_read_article.php?id=69887

Анализ программных продуктов и изучение автоматизации процессов в сфере мониторинга закупок и товаров

Перелыгин Иван Михайлович

студент, кафедра индустриального программирования, МИРЭА - Российский технологический университет

119454, Россия, Московская область, г. Москва, ул. Проспект Вернадского, 78

iv_perelygin@mail.ru

Статья из рубрики "Технологии и методология в системах безопасности"

DOI:

10.25136/2409-7543.2024.1.69887

EDN:

VLWPDM

Дата направления статьи в редакцию:

17-02-2024

Аннотация: Предметом исследования данной работы является сравнительный анализ программных продуктов и исследование преимуществ и недостатков в области оптимизации закупок и мониторинга товаров. В рамках данного исследования были поставлены следующие задачи: изучение существующих программных решений для оптимизации процессов закупок, анализ их функционала и эффективности, а также исследование бизнес-процессов компаний в сфере мониторинга товаров. В результате данной работы была представлена таблица сравнения различных программных продуктов, были выявлены их преимущества и недостатки, а также проанализированы текущие бизнес-процессы и выявлены возможности и потенциал для оптимизации. Полученные результаты и выводы могут быть использованы для разработки рекомендаций по улучшению процессов закупок и мониторинга товаров в организациях. Методология исследования базировалась на сравнительном анализе функциональности, эффективности и стоимости программ, а также изучении отзывов пользователей и экспертов в отрасли. Результаты позволили выявить основные преимущества и

недостатки каждого рассмотренного программного обеспечения. Исследование основных характеристик и функциональности систем управления закупками представляет значимый вклад в область информационных технологий и управления бизнес-процессами. Анализ сравнительных характеристик ERM-систем, их интеграционных возможностей и соответствия потребностям бизнеса позволяет выявить ключевые факторы успешной автоматизации закупочных процессов. Это исследование не только расширяет научное понимание в области автоматизации закупок, но также предоставляет практические рекомендации для выбора оптимальной системы управления закупками. Выводы работы подчеркивают важность индивидуальной настройки программного обеспечения под уникальные потребности организации для достижения оптимальной эффективности и результативности в управлении закупками. Представленная в заключительной части таблица сравнения недостатков ERM-систем по ключевым параметрам позволяет выделить основные преимущества и недостатки каждого программного продукта, что является важным шагом в выборе наиболее подходящего решения для конкретного бизнеса. Таким образом, данное исследование не только способствует развитию научного знания в области управления закупками, но также предоставляет ценные практические рекомендации для бизнес-сообщества, помогая повысить эффективность и результативность закупочных процессов в современной деловой среде.

Ключевые слова:

автоматизация, закупки, мониторинг, оптимизация, интеграция, бизнес-процесс, модульность, ERM-система, адаптация, гибкость

1 ОПИСАНИЕ ERM-СИСТЕМ

1.1 Comindware – система управления закупками

Система разработана на основе опыта, полученного при реализации множества проектов по автоматизации закупок. Она особенно эффективна для программ импортозамещения в нефтегазовой промышленности. Comindware не только заменяет функциональность решений, созданных на базе Oracle и SAP, но также обеспечивает полный контроль над процессом закупок, от планирования до выполнения.

Comindware предлагает комплексный подход к автоматизации процесса закупок. Она может быть успешно применена в программах импортозамещения в нефтегазовой промышленности. Благодаря своей функциональности, система заменяет решения, созданные на базе Oracle и SAP, и обеспечивает полный контроль и управление различными процессами закупок.

Система автоматизирует 5 основных этапов процесса закупок – планирование, подготовку закупок, выполнение закупок, заключение контрактов и доставку. Она способствует эффективному и прозрачному управлению всеми этапами процесса закупок.

Кроме того, Comindware обеспечивает контролируемый доступ ко всей связанной информации, такой как номенклатурные справочники, реестры поставщиков, контракты, статусы задач и заявки. Это позволяет пользователям быстро и удобно получать необходимую информацию и выполнять требуемые действия.

Заявленные сроки внедрения системы варьируются от 2 до 7 дней, что позволяет быстро развернуть систему и использовать ее преимущества. Кроме того, систему можно постоянно улучшать, используя инструменты разработки с низким кодом, унаследованные от платформы приложений Comindware. Это позволяет постепенно масштабировать систему и внедрять ее в бизнес-процессы других организаций [1].

У Comindware есть много преимуществ, которые делают ее привлекательным решением для компаний. Некоторые из них включают в себя:

- управление закупками на всем цикле от планирования до доставки;

- высокий уровень прозрачности процесса;

- быстрое развертывание системы;

- низкая стоимость настройки и обслуживания;

- расширенные возможности управления задачами;

- тщательный процесс квалификации подрядчиков;

- готовый портал поставщика для сбора предложений и проведения закрытых тендеров;

- подготовка лотов для загрузки на электронные торговые площадки;

- поддержка работы тендерного комитета;

- поддержка полного цикла электронного документооборота (EDI).

Система управления закупками Comindware использует набор сложных алгоритмов для оптимизации и улучшения процесса закупок. Эти алгоритмы являются ключевыми для нескольких основных функциональностей системы [2]:

1. *алгоритмы оценки поставщиков*: система использует алгоритмы многокритериального принятия решений (МКПР) для оценки поставщиков. Это могут быть алгоритмы аналитической иерархии (АИ) или модели взвешенной оценки (МВО), где различные факторы, такие как цена, качество, сроки поставки и прошлые результаты, получают вес в соответствии с их важностью;

2 . *алгоритмы оптимизации планирования закупок*: Comindware может использовать линейное программирование (ЛП) для оптимизации планирования закупок, минимизируя затраты при соблюдении потребностей в закупках;

3. *алгоритмы обогащения и валидации данных*: для обогащения данных система может использовать алгоритмы нечеткого сопоставления, чтобы связывать и объединять данные, вероятно, относящиеся к одним и тем же объектам в различных наборах данных;

4. *коллаборативная фильтрация для выбора поставщиков*: система может использовать техники коллаборативной фильтрации, подобные тем, которые используются в системах рекомендаций, для предложения поставщиков на основе истории закупок и предпочтений аналогичных задач по закупкам.

Дополнительные функции [3]:

1. *динамическая отчетность*: система обеспечивает возможность создания динамических

и адаптивных отчетов, позволяющих пользователям генерировать настраиваемые отчеты с использованием различных данных. Например, можно использовать запросы, подобные SQL, для извлечения данных в режиме реального времени или использовать инструменты для бизнес-аналитики для визуализации трендов;

2 . *управление доступом на основе ролей (RBAC)*: это обеспечивает доступ пользователей только к информации и функциональности, необходимым для выполнения их ролей, улучшая безопасность и операционную эффективность;

3 . *возможности интеграции*: Comindware может быть интегрирована с существующими системами управления предприятием (ERP) с помощью API или веб-сервисов, чтобы обеспечить непрерывность потока данных и сохранить целостность данных между платформами.

Преимущества автоматизации [4]:

Процесс закупок, то есть процесс сбора материалов и ресурсов, является одной из самых важных частей любого бизнеса. Это позволяет вам предоставлять своим клиентам или заказчикам своевременное и надежное обслуживание. Автоматизированные процессы делают весь этот процесс более эффективным и упорядоченным. Программное обеспечение, которое предоставляет панель инструментов для всех заинтересованных сотрудников, позволяет всем сторонам видеть, на каком этапе находится одобрение контракта. Они могут получить важную информацию о процессах и использовать эту информацию для стратегического планирования и бизнес-целей в будущем.

Сегодня прозрачность имеет огромное значение в любом бизнесе. Вам необходимо иметь возможность документировать весь процесс заключения контракта или закупки. С помощью панели инструментов вы можете видеть, на каком этапе находится контракт и на чьем столе он лежит. Это позволяет вам знать, кого контактировать, если вам нужно ускорить процесс.

Прозрачность не только помогает руководить процессом одобрения и ускоряет его. Она также позволяет проводить аудит. Большинство процессов имеют место для улучшения, и возможность отслеживать контракт от начала до утверждения может дать вам представление о том, где вы можете улучшить эффективность и надежность.

У многих пакетов программного обеспечения есть функции перетаскивания и удаления, которые делают весь процесс визуальным и позволяют сторонам видеть, как работает процесс утверждения. Визуальное представление процесса дает всем заинтересованным сторонам возможность видеть, как работает каждый шаг. Это упрощает понимание того, на каком этапе утверждения находится данный контракт. Это также может дать администраторам и другим идеи о том, как улучшить эффективность и сократить время, необходимое для утверждения закупочных контрактов.

Внедряя эти сложные алгоритмические подходы, управление закупками Comindware может автоматизировать сложные задачи по закупкам, тем самым сокращая ручную работу, повышая точность и обеспечивая принятие решений по закупкам на основе данных и их соответствие организационным целям.

1.2 AGORA – платформа автоматизации закупок

В быстротемповом цифровом мире эффективные системы закупок являются неотъемлемой частью успеха бизнеса. AGORA выступает в качестве ведущего игрока в этой сфере, стремясь упростить и улучшить процесс закупок.

AGORA – это передовая платформа для автоматизации закупок, разработанная для усовершенствования способа обработки закупочных процессов бизнеса. Благодаря более чем 200 модульным функциональностям, она обещает решение для почти 90 процентов задач, связанных с закупками. Интересно, что гибкость платформы проявляется в ее цикле разработки: от MVP (минимально жизнеспособного продукта) продолжительностью всего 2 недели до более полного цикла в 2 месяца [5].

Кроме того, AGORA – это не просто автоматизация закупок. Это универсальная платформа, на которой бизнесы могут создавать как надежную систему управления закупками, так и целый электронный торговый платформу.

Преимущества AGORA [6]:

1 . *индивидуальные решения для автоматизации*: каждый бизнес имеет уникальные потребности. Признавая это, AGORA предоставляет инструменты для разработки индивидуальных решений, обеспечивая возможность точно настроить систему закупок под свои нужды;

2 . *создание электронной торговой платформы*: AGORA выделяется тем, что является одним из немногих продуктов на рынке, позволяющих создавать персонализированные электронные торговые платформы (ETP);

3. *управление качеством и подрядчиками*: обеспечение надежности подрядчиков имеет важное значение. Специализированные модули AGORA помогают бизнесам управлять качеством и даже оценивать своих подрядчиков, обеспечивая прозрачность и доверие;

4. *разнообразный выбор поставщиков*: с помощью AGORA бизнесы могут оптимизировать процесс выбора поставщиков, категоризируя их по различным типам торговых процедур, тем самым обеспечивая наилучшее соответствие конкретным потребностям;

5. *корпоративный веб-сайт для закупок*: бизнесы могут улучшить свои процессы закупок, интегрируя их в корпоративный веб-сайт для закупок, что можно осуществить в рамках платформы AGORA.

Структурное и алгоритмическое основание AGORA:

1. *модульная архитектура*: архитектура AGORA является модульной, то есть она состоит из отдельных взаимозаменяемых компонентов или модулей, которые могут быть индивидуально настроены или заменены. Такой дизайн позволяет обширную настройку для удовлетворения конкретных потребностей бизнеса и облегчает обновления и обслуживание;

2 . *поток данных и интеграция бизнес-процессов*: в основе дизайна AGORA лежит безупречная архитектура потока данных, интегрированная с бизнес-процессами. Эта интеграция обеспечивает систематическое сбор, обработку и передачу данных через каждый модуль, обеспечивая плавный переход от одного бизнес-процесса к другому;

3 . *алгоритмические стратегии для улучшения закупок*: AGORA использует ряд алгоритмических стратегий для автоматизации и оптимизации задач по закупкам. Это может включать:

- *прогностическая аналитика*: использование исторических данных для прогнозирования будущих потребностей и тенденций в закупках;

- *эвристические алгоритмы*: для процессов принятия решений, таких как выбор поставщика, эвристические алгоритмы могут быть применены для быстрого нахождения удовлетворительных решений в случаях, когда исчерпывающий поиск невозможен;

- *оптимизация на основе ограничений*: для планирования и распределения ресурсов в задачах по закупкам, обеспечивая соблюдение всех ограничений при оптимизации по стоимости или эффективности.

4. *разработка электронных торговых платформ (ETP)*: структура AGORA разработана для поддержки создания электронных торговых платформ, предлагая не только управление закупками, но и возможность запуска собственных торговых платформ бизнесами. Может использоваться стандарт обмена данными, такой как EDIFACT или XML для обмена документами и упрощения транзакций.

Интеграция бизнес-процессов и управление данными [7]:

AGORA интегрируется с различными бизнес-процессами, такими как управление поставщиками, управление контрактами и операции по закупкам. Система разработана для эффективного управления данными и предоставляет следующие возможности:

- синхронизацию данных в режиме реального времени между модулями;

- автоматизированную проверку данных для обеспечения целостности информации;

- безопасные протоколы передачи данных для поддержания конфиденциальности и соответствия нормам.

Исследуемые преимущества [7]:

1 . *пользовательские решения по закупкам*: благодаря модульному подходу AGORA предлагает бизнесам гибкость настройки системы закупок под их уникальные процессы и рабочие процедуры;

2 . *управление качеством*: платформа включает функциональности управления качеством, которые помогают поддерживать высокие стандарты на протяжении цикла закупок;

3. *управление поставщиками и разнообразность*: возможности управления поставщиками в AGORA обеспечивают комплексный подход к управлению отношениями с поставщиками, поощрению разнообразия и оптимизации выбора поставщика.

Критическая оценка:

1 . *сложность модульности*: хотя модульный подход обеспечивает гибкость, он также вводит сложность в начальной настройке и настройке под конкретные требования, требуя больше времени и ресурсов;

2 . *верификация поставщика*: существующая структура agora может требовать дополнительного совершенствования для полноценных процессов верификации поставщика, что является важным аспектом целостности закупок.

Отсутствие указанных цен на веб-сайте AGORA указывает на индивидуальную модель ценообразования, вероятно, зависящую от конкретных модулей и функциональности, выбранных бизнесом. Отсутствие поддержки low-code говорит о возможных дополнительных затратах на разработку и внедрение, так как для настройки и

поддержания системы может потребоваться специализированный технический персонал.

1.3 Программное обеспечение NaumenSRM/GPMS

Разработанная известной российской компанией, система Naumen SRM/GPMS была тщательно спроектирована для решения широкого спектра задач, связанных с закупочной деятельностью. Этот обширный комплекс охватывает полный жизненный цикл закупок, начиная с начальной фазы сбора заявок и заканчивая детальными нюансами управления заказами, организации торгов и обеспечения регистрации и соблюдения контрактов.

Основные функции и преимущества Naumen SRM/GPMS [8]:

1 . *комплексная обработка жалоб*: программа не только позволяет пользователям зарегистрировать жалобы, но и поддерживает систематический реестр для проверок. Это гарантирует своевременное рассмотрение всех жалоб и наличие прозрачного аудита для проверок;

2 . *эффективное управление бюджетом*: в системе реализована надежная механизм управления бюджетными ограничениями, обеспечивающая соответствие расходов организационным пределам и приоритетам;

3. *автоматизация на высшем уровне*: одна из основных возможностей - автоматическое генерирование заказов вместе с необходимой документацией. Это сокращает ручные работы, минимизирует ошибки и ускоряет процесс закупок;

4. *детализированный реестр контрактов*: каждый контракт, введенный в систему, может быть отслежен на предмет изменений или дополнений. Это не только гарантирует выполнение всех контрактных обязательств, но и обеспечивает заинтересованным сторонам полную прозрачность.

Точная цена касательно приобретения системы для личного или коммерческого использования не указана на официальном сайте разработчика, однако стоит отметить, что программа может потребовать настройки, особенно для частных предприятий. Такие настройки могут повлиять на общую стоимость. Потенциальные пользователи, особенно из частного сектора, должны рассматривать аспекты ценообразования с гибкостью, учитывая потенциальные дополнительные затраты, связанные с настройкой системы под конкретные потребности.

Программное обеспечение Naumen SRM/GPMS представляет собой сложное решение от ведущего российского разработчика, направленное на оптимизацию процессов закупок для организаций. Эта система построена для эффективного управления всем жизненным циклом закупок и особенно соответствует требованиям государственных закупок.

Структура системы и поток данных Naumen SRM/GPMS [9]:

1. *централизованная база данных*: в основе Naumen SRM/GPMS лежит централизованная база данных, в которой хранятся все данные, связанные с закупками. Это гарантирует согласованность информации и легкий доступ к ней из разных модулей системы;

2 . *автоматизированный механизм рабочего процесса*: программа использует автоматизированный механизм рабочего процесса, который управляет закупочными операциями от инициации до завершения. Этот механизм отвечает за запуск действий, отправку уведомлений и управление потоком данных на протяжении всего процесса

закупок;

3 . *возможности интеграции*: Naumen SRM/GPMS спроектирована с возможностью интеграции с другими системами, такими как финансовое и складское программное обеспечение. Эта интеграция облегчает обмен данными и оптимизирует процессы закупок в различных бизнес-функциях.

Бизнес-процессы в Naumen SRM/GPMS [10]:

1 . *управление жалобами и проверками*: в системе есть отдельный процесс обработки жалоб, их регистрации и управления последующими проверками. Этот процесс обеспечивает ответственность и прозрачность в закупочной деятельности;

2 . *контроль бюджета и финансовое планирование*: включает финансовые контроли, которые помогают управлять и контролировать бюджеты на закупки, обеспечивая соответствие расходов политикам и ограничениям организации;

3 . *управление заказами*: процесс управления заказами автоматизирован для эффективного создания заказов и связанной документации. Это помогает снизить ручные нагрузки и повысить скорость и точность закупочных операций;

4 . *управление контрактами и соблюдение требований*: существует детальный процесс управления контрактами, который отслеживает статусы контрактов, их изменения и соблюдение, предоставляя заинтересованным сторонам прозрачное представление о всех контрактных обязательствах.

Алгоритмы и функциональность Naumen SRM/GPMS [10]:

1 . *алгоритм реестра жалоб*: программное обеспечение использует алгоритм для категоризации, приоритизации и маршрутизации жалоб к соответствующему персоналу, обеспечивая их своевременное разрешение;

2 . *алгоритм оптимизации бюджета*: для эффективного управления бюджетами, Naumen SRM/GPMS может использовать оптимизационные алгоритмы, которые распределяют ресурсы на основе заранее определенных критериев и ограничений;

3 . *алгоритм генерации документов*: для автоматического создания заказов и документации, программное обеспечение, вероятно, использует набор алгоритмов на основе правил, которые извлекают данные из центральной базы данных и применяют бизнес-логику для создания точных документов.

Цена Naumen SRM/GPMS может значительно варьироваться в зависимости от уровня необходимой настройки, чтобы соответствовать конкретным потребностям организации, особенно если требуется адаптация стандартной ориентации на государственные закупки для использования в частном секторе.

1.4 Norbit’s – платформа эффективных закупок

Программное обеспечение Norbit's представляет собой комплексный и инновационный подход к преобразованию стратегий закупок в различных организационных средах. Основанный на обширном опыте и понимании, это программное обеспечение разработано для удовлетворения сложных потребностей правительственных учреждений, государственных предприятий и коммерческих организаций разных размеров.

Ключевые особенности и преимущества [11]:

1. унифицированная система закупок:

- *централизованная платформа*: программное обеспечение Norbit's предлагает централизованную платформу для всех закупочных деятельностей, обеспечивая стандартизированный подход от выбора поставщика до завершения контракта;

- *соответствие стратегическим целям*: унифицированная система повышает эффективность и выстраивает закупочные деятельности в соответствии со стратегическими целями организации.

2. плавное интегрирование этапов закупок:

- *связанные фазы*: решение акцентирует на плавной связи между различными этапами закупок, такими как привлечение поставщиков, переговоры и исполнение контракта;

- *безошибочный процесс*: интеграция обеспечивает гибкий и безошибочный процесс закупок.

3. продвинутый набор оптимизационных инструментов:

- *гибкость и адаптивность*: Norbit’s предоставляет пользователям инструменты, разработанные для оптимизации закупочных деятельностей, обеспечивая организации постоянное получение наилучшей стоимости за свои расходы;

- *стратегическое принятие решений*: набор инструментов поддерживает стратегическое принятие решений в динамичном закупочном ландшафте.

4. гибкость в удовлетворении потребностей различных секторов:

- *настроенная функциональность*: программное обеспечение Norbit's адаптируется к тонким различиям между государственными и частными закупками, проявляя гибкость в своей функциональности;

- *компетентность в различных отраслях*: оно удовлетворяет разнообразные потребности коммерческих конгломератов и государственных органов.

Ценообразование и особенности внедрения:

1 . *детали ценообразования*: хотя конкретные детали ценообразования не указаны на веб-сайте разработчика, потенциальные клиенты должны учитывать операционные соображения;

2 . *длительность внедрения*: отсутствие поддержки инструментов для создания кода низкой сложности может увеличить длительность внедрения;

3 . *общая стоимость владения*: учет как прямых затрат (лицензирование), так и косвенных затрат (сроки внедрения, поддержка) является важным для полного понимания общей стоимости владения.

Для более глубокого исследования потенциальные клиенты могут получить пользу от прямого контакта с компанией Norbit’s, изучения кейс-стадии, а также поискать отзывы пользователей. Кроме того, исследование отзывов и анализов отрасли может предоставить ценные сведения о производительности программного обеспечения и его влиянии на процессы закупок.

Расширенные возможности и инновации [12]:

1. *принятие решений на основе искусственного интеллекта*:

- «Effective Procurement» от Norbit's интегрирует искусственный интеллект (ИИ) для предоставления поддержки принятия решений. Это включает предиктивный анализ для прогнозирования спроса, анализ производительности поставщиков и оперативные показатели, что позволяет организациям принимать обоснованные и стратегические решения в сфере закупок.

2. *динамическое управление рисками*:

- программное обеспечение включает инструменты динамического управления рисками, использующие данные в режиме реального времени и прогностическое моделирование для выявления и снижения потенциальных рисков в процессе закупок. Эта функция повышает устойчивость и обеспечивает активное снижение рисков.

3. *совместные рабочие процессы в сфере закупок*:

- Norbit's облегчает совместные рабочие процессы, позволяя сотрудничать между отделами и функциональными областями в процессе закупок. Это обеспечивает возможность вклада и рассмотрения закупочных деятельностей заинтересованными сторонами из различных областей, способствуя прозрачности и ответственности.

4. *мобильная доступность*:

- учитывая важность мобильности, программное обеспечение от Norbit's предлагает мобильную доступность, позволяя пользователям осуществлять закупочные операции в любом месте. Эта функция повышает гибкость и оперативность пользователей, особенно в быстро меняющейся деловой среде.

Соблюдение регулирования и безопасность [13]:

1. *модули соответствия нормативным требованиям*:

- решение от Norbit's включает модули соответствия, настроенные под различные нормативные фреймворки. Это обеспечивает возможность организациям соблюдать специфические закупочные нормы, соответствующие их отрасли и географическому положению.

2. *меры безопасности данных*:

- внедрены надежные меры безопасности данных для защиты конфиденциальной информации о закупках. Это включает протоколы шифрования, контроль доступа и регулярные обновления безопасности для защиты от возможных киберугроз.

Norbit's проводит регулярные обновления и улучшения, чтобы программа «Effective Procurement» развивалась в соответствии с изменяющейся динамикой отрасли и технологическими достижениями. Это стремление к инновациям позволяет программному обеспечению быть долгосрочным решением для меняющихся потребностей в сфере закупок.

Разработчик активно взаимодействует с пользовательским сообществом, поощряя обратную связь и предложения. Такой коллективный подход обеспечивает непрерывное улучшение и гарантирует соответствие программного обеспечения ожиданиям пользователей и трендам отрасли.

1.5 О программном обеспечении ITenderSRM

Программное обеспечение ITender SRM, разработанное российской компанией FogSoft, является результатом передового программирования и глубокого понимания области закупок. Это комплексная платформа, основанная на модульной структуре, которая предлагает специализированные инструменты и функциональность для управления различными этапами закупочного цикла и развития отношений с поставщиками. Гордясь своим отечественным происхождением, ITender SRM имеет внушительную историю успеха, с более чем 70 успешно реализованными проектами в странах Содружества Независимых Государств (СНГ) [14].

Основные особенности и преимущества ITender SRM [15]:

1. *проверенный опыт успеха*: нельзя недооценить важность надежного опыта при выборе корпоративного программного обеспечения. ITender SRM выделяется множеством успешно реализованных проектов, многие из которых обслуживают ведущие корпорации. Эта история не только подтверждает его надежность, но и его приспособляемость к различным бизнес-потребностям;

2. *продвинутые инструменты сотрудничества с поставщиками*: признавая важную роль отношений с поставщиками в сфере закупок, ITender SRM оснащен сложно спроектированными инструментами. Эти функциональные возможности направлены на упрощение процессов коммуникации, переговоров и сотрудничества с поставщиками, обеспечивая гармоничное и продуктивное партнерство;

3. *посвящение повышению возврата инвестиций*: философия программного обеспечения заключается в увеличении возврата инвестиций (ROI) в закупочную деятельность. Благодаря своим инновационным функциям и стратегическим идеям, ITender SRM помогает компаниям оптимизировать свои расходы, что приводит к улучшению прибыльности;

4. *интеграция внутренней ЭТП*: уникальное предложение в комплекте ITender SRM - возможность создания и интеграции внутренней электронной торговой платформы (ЭТП). Это позволяет компаниям создать централизованную цифровую торговую площадку для своих закупочных активностей, обеспечивая прозрачность, эффективность и контроль.

Расширенные возможности и инновации [16]:

1. модульная платформа для масштабируемости:

- модульная платформа ITender SRM позволяет достичь масштабируемости, позволяя организациям настраивать систему под свои потребности в сфере закупок. Такая гибкость обеспечивает возможность развития программного обеспечения вместе с бизнесом, учитывая растущую сложность и расширение сети поставщиков.

2. аналитика и отчетность в реальном времени:

- программное обеспечение включает надежные инструменты для аналитики и отчетности, предоставляя пользователям актуальную информацию о производительности закупок. Эта функция позволяет организациям принимать решения на основе данных, выявлять области для улучшения и оптимизировать стратегии закупок.

3. автоматизированное управление рабочим процессом:

- ITender SRM оптимизирует процессы закупок с помощью автоматизированного управления рабочим процессом. Это включает автоматизированное согласование рабочих процессов, назначение задач и уведомлений, что снижает необходимость вручную вмешиваться и повышает эффективность процесса.

4. мониторинг производительности поставщика:

- платформа включает инструменты для мониторинга и оценки производительности поставщика. Можно отслеживать ключевые показатели эффективности (KPI), чтобы оценить надежность поставщика, соблюдение сроков поставки и общее соблюдение контрактных соглашений, что способствует стратегическому управлению отношениями с поставщиками.

Пользовательский опыт и сотрудничество [15]:

1. интуитивный пользовательский интерфейс и доступность:

- ITender SRM уделяет внимание пользовательскому опыту с помощью интуитивного интерфейса, что делает его удобным как для профессионалов в сфере закупок, так и для других заинтересованных сторон. Доступность системы гарантирует эффективное использование ее функций.

2. совместные рабочие пространства:

- программное обеспечение способствует сотрудничеству, предоставляя отдельные рабочие пространства для команд по закупкам и поставщиков. Эта совместная среда способствует прозрачной коммуникации, обмену документами и совместному принятию решений, укрепляя отношения между покупателем и поставщиком.

Меры соответствия и безопасности [16]:

1. инструменты соблюдения правил и нормативов:

- ITender SRM интегрирует инструменты соблюдения правил, чтобы помочь организациям соблюдать региональные и отраслевые нормативы в сфере закупок. Это гарантирует, что закупочная деятельность осуществляется в рамках законодательных рамок, снижая риски соблюдения нормативов.

2. шифрование данных и защищенные контроли доступа:

- для обеспечения безопасности платформа использует надежные методы шифрования данных и защищенные контроли доступа. Это обеспечивает защиту от несанкционированного доступа к конфиденциальным данным о закупках и потенциальных киберугроз, обеспечивая целостность и конфиденциальность данных.

Развитие и поддержка в будущем [16]:

1. постоянные обновления программного обеспечения:

- FogSoft обязуется постоянно обновлять программное обеспечение, чтобы ITender SRM оставался технологически актуальным и соответствовал лучшим практикам в отрасли. Постоянное развитие отражает стремление к решению возникающих проблем и внедрению отзывов пользователей.

2. комплексная поддержка клиентов:

- FogSoft предоставляет комплексные услуги поддержки клиентов, включая документацию, обучающие ресурсы и отзывчивые каналы поддержки. Это обеспечивает улучшение пользовательского опыта и гарантирует, что организации смогут максимально использовать преимущества ITender SRM.

Рекомендуется проводить глубокие оценки, пилотные внедрения и взаимодействие с командами поддержки и разработки FogSoft для организаций, рассматривающих внедрение ITender SRM. Кроме того, изучение кейс-стади и поиск отзывов текущих пользователей могут предоставить ценную информацию о практическом применении программного обеспечения и его влиянии на процессы закупок.

2 РАЗВИТИЕ ИДЕАЛЬНОЙ ERM-СИСТЕМЫ

2.1 Недостатки текущих ERM-систем

Недостатки Comindware:

К сожалению, у Comindware также есть некоторые недостатки, которые следует учитывать при рассмотрении этого решения. Некоторые из них включают в себя:

- процесс контроля доставки потребует интеграции с системами учета;

- интеграция с электронными торговыми площадками находится в разработке.

Недостатки AGORA:

Хотя Agora предлагает множество преимуществ, важно учесть некоторые из его ограничений:

1 . *модульная система*: AGORA не предлагает готового решения "включи и работай". Вместо этого она предоставляет ряд модулей, из которых бизнесы должны собрать свою систему. Такой модульный подход, хотя и гибкий, может потребовать больше начальной настройки и конфигурации;

2. *процесс проверки поставщиков*: одной из сложностей закупок является обеспечение надежности поставщиков. На данный момент AGORA не имеет установленного всестороннего процесса для этого важного этапа, что может привести к необходимости разработки собственных методов проверки бизнесами.

Возможные недостатки Naumen SRM/GPMS:

1 . *фокус на государственных закупках*: из-за своей концепции, программа сильно ориентирована на удовлетворение потребностей государственных закупок. В результате некоторые из ее функций могут показаться излишними или ненужными для частных предприятий;

2. *ограниченный каталог товаров*: отсутствие специального каталога товаров может быть недостатком для некоторых организаций. Кроме того, хотя и предоставляются функции управления бюджетом, они могут оказаться недостаточными для некоторых сложных организационных потребностей.

Возможные ограничения Norbit’s:

1. *проблемы интеграции*: специализированный портал поставщика, хотя и стратегически важен, может вызывать проблемы с интеграцией для некоторых организаций;

2 . *ограничения гибкости аукционов*: исключительная зависимость от внешних электронных торговых площадок для проведения аукционов может ограничивать гибкость для некоторых предприятий.

Возможные проблемы с ITender SRM:

1. *зависимость от экосистемы Microsoft*: зависимость платформы от компонентов Microsoft может быть двусмысленной. Хотя инструменты Microsoft глобально признаны своей эффективностью и надежностью, геополитическая обстановка и потенциальные санкции против России могут представлять операционные риски для компаний, полагающихся на ITender SRM;

2 . *финансовые соображения для ITender SRM*: хотя FogSoft остается сдержанным в отношении точной цены на своем официальном веб-сайте, ясно, что общая инвестиция в ITender SRM будет зависеть от конкретных потребностей, масштаба и требований к настройке проекта. Организации, рассматривающие принятие ITender SRM, должны непосредственно общаться с командой FogSoft, чтобы провести всестороннюю оценку и получить более точную финансовую оценку.

Ниже представлена таблица 2.1 для сравнения различных недостатков систем управления закупками.

Такая таблица может быть использована для лучшего понимания преимуществ и недостатков каждой системы и поможет при принятии решения о выборе или разработке подходящей системы управления закупками.

Таблица 2.1 – Сравнение недостатков ERM-систем

Недостатки системы	**Comindware**	**AGORA**	**Naumen SRM/GPMS**	**Norbit's**	
Интеграция с учетными системами	Требует интеграции	Модульный подход	Ограниченное управление каталогом	Проблемы интеграции с порталом поставщика	З
Электронные торговые площадки	В разработке	Неопределенный процесс	Не полностью применимы в частном секторе	Ограниченная гибкость аукционов	
Модульная система	-	Требует конфигурации	Не полностью применимы в частном секторе	Ограниченная гибкость аукционов	З
Процесс проверки поставщиков	-	Отсутствует установленный процесс	Не полностью применимы в частном секторе	Ограниченная гибкость аукционов	ге
Ориентация на государственный сектор	-	-	Адаптированы для государственных закупок	-	С
Ограниченное управление каталогом	-	-	Ограниченное управление каталогом	-	Не
Зависимость от экосистемы	-	-	-	-	с

Microsoft					

2.2 Требования к разрабатываемой системе

Разрабатываемая система управления закупками (СЗ) должна стремиться к обеспечению полного цикла управления закупками, начиная от планирования и заканчивая исполнением контракта. Для минимизации недостатков текущих систем ERM, будущая СЗ должна включать следующие ключевые функциональности:

1. *интеграция с учетными системами*: обеспечение плавной интеграции с различными системами учета для контроля доставки и финансового учета;

2. *электронные торговые площадки*: полная поддержка электронных торговых площадок с целью обеспечения максимальной конкуренции и эффективности в процессе закупок;

3. *модульность с простой настройкой*: гибкая модульная система с простым процессом настройки, чтобы упростить внедрение и адаптацию системы к специфическим потребностям предприятия;

4. *всесторонний процесс проверки поставщиков*: реализация всестороннего и автоматизированного процесса проверки поставщиков для обеспечения надежности и качества предлагаемых товаров и услуг;

5. *ориентация на обе сферы – государственный и частный сектор*: адаптированные функции для удовлетворения как строгих требований государственных закупок, так и бизнес-требований частного сектора;

6. *расширенное управление каталогом*: расширенная функциональность управления каталогом продуктов для удовлетворения разнообразных бизнес-требований;

7. *надежность и гибкость тендеров*: обеспечение надежности процесса проведения тендеров с гибкостью в зависимости от потребностей предприятия;

8. *система проверки безопасности*: внедрение системы проверки безопасности для защиты конфиденциальных данных и предотвращения несанкционированного доступа.

Библиография

1. Comindware procurement management (tadviser.com). URL: https://tadviser.com/index.php/Product:Comindware_Procurement_Management#:~:text=Comindware%20Procurement%20Management%20was%20developed,to%20the%20specified%20business%20logic (дата обращения: 20.10.2023).
2. Procurement management software market outlook 2022 to 2031 – Supply chain council of European Union | scceu.org. URL: https://scceu.org/procurement-management-software-market-outlook-2022-to-2031/ (дата обращения: 21.10.2023).
3. Procurement contract approval process – BPI – The destination for everything processes related (businessprocessincubator.com). URL: https://www.businessprocessincubator.com/content/procurement-contract-approval-process/ (дата обращения: 21.10.2023).
4. Автоматизация бизнес-процесса согласования договоров – Comindware. URL: https://www.comindware.ru/usecases/document-approval-business-process/ (дата обращения: 22.10.2023).
5. Agora.ru – B2C и B2B E-commerce платформа для цифровизации бизнеса. URL: https://www.agora.ru/?ysclid=lovz0vvkq9695817461 (дата обращения: 22.10.2023).

6. Construction ERP Software | AGORA | Simpro business solutions. URL: https://simpro.co.in/construction-erp-software-agora/ (дата обращения: 23.10.2023).
7. AGORA: Разработка онлайн-решений для автоматизации закупочной деятельности (ocs.ru). URL: https://www.ocs.ru/agora-razrabotka-onlajn-reshenij-dlya-avtomatizaczii-zakupochnoj-deyatelnosti/?ysclid=lovzgbwbo9129914734 (дата обращения: 23.10.2023).
8. Naumen SRM/GPMS | автоматизация закупочной деятельности. URL: https://naumensrm.ru/srm-sistema/?ysclid=lovzzfaa303290434 (дата обращения: 23.10.2023).
9. Naumen SRM/GPMS | автоматизация закупочной деятельности. URL: https://softfinder.ru/service/naumen-srmgpms?ysclid=lsqp6djt7d226861212 (дата обращения: 23.10.2023).
10. Naumen SRM/GPMS – система автоматизации закупочной деятельности (softfinder.ru). URL: https://tadviser.com/index.php/Product:Naumen_GPMS_%E2%80%93_Purchase_management?ysclid=low06isokp673800220 (дата обращения: 23.10.2023).
11. Норбит: эффективные закупки (norbit.ru). URL: https://products.norbit.ru/effektivnye-zakupki/?ysclid=low1n3id4f104510856 (дата обращения: 23.10.2023).
12. Norbit business trade (NBT) (tadviser.com). URL: https://tadviser.com/index.php/Product:Norbit_Business_Trade_(NBT)?ysclid=low1nagqio924137887 (дата обращения: 23.10.2023).
13. Norbit SRM: эффективная цифровизация закупок (norbit-srm.com). URL: https://norbit-srm.com/news-and-events/norbit-srm-effektivnaya-tsifrovizatsiya-zakupok/?ysclid=low1nfc75t624810865 (дата обращения: 23.10.2023).
14. Система управления закупками ITender SRM: планирование, контроль - ай тендер фогсофт (fogsoft.ru). URL: https://fogsoft.ru/solutions/itender-srm/?ysclid=low0rjouqt552056949 (дата обращения: 23.10.2023).
15. Разработка компании Фогсофт – ITender SRM (itender-online.ru). URL: https://itender-online.ru/solutions/itender-srm/?ysclid=low0nkld1j406386270 (дата обращения: 23.10.2023).
16. ITender девелопмент – полноценная SRM для застройщиков (bizneslab.com). URL: https://bizneslab.com/itender-development/?ysclid=low0nwc8r523448463 (дата обращения: 23.10.2023).

Результаты процедуры рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов издательства можно ознакомиться здесь.

Предмет исследования: в статье рассматриваются вопросы анализа и сравнения различных программных продуктов для автоматизации процессов в сфере мониторинга закупок и управления поставками (ERM-систем).
Методология исследования: исследование проведено методом сравнительного анализа основных характеристик и функциональных возможностей пяти ERM-систем – Comindware, AGORA, Naumen SRM/GPMS, Norbit's и ITender SRM. Comindware - комплексное решение для управления закупками, особенно эффективно в программах импортозамещения в нефтегазовой сфере. Обеспечивает контроль на всех этапах процесса закупок. AGORA - передовая модульная платформа для автоматизации

закупок. Позволяет создавать персонализированные системы управления закупками и электронные торговые площадки. Naumen SRM/GPMS – комплексное решение российской разработки для автоматизации закупок с акцентом на госсектор. Обеспечивает контроль бюджета, обработку жалоб и управление контрактами. Norbit's – платформа "Эффективные закупки" с расширенным набором оптимизационных инструментов. Ориентирована как на государственный, так и на частный сектор. ITender SRM – решение российской компании FogSoft, ориентированное на управление отношениями с поставщиками и повышение ROI от закупочной деятельности. Для каждой системы приведено подробное описание, выделены ключевые преимущества, рассмотрены алгоритмические и технические основы. Также проведен анализ возможных недостатков и даны рекомендации по их устранению в рамках создания идеальной ERM-системы.

Актуальность темы не вызывает сомнений, поскольку эффективность систем мониторинга и управления закупками является важным фактором оптимизации расходов и повышения конкурентоспособности организаций.

Научная новизна заключается в структурированном анализе возможностей современных ERM-систем и разработке требований к идеальной системе с учетом выявленных недостатков текущих решений.

Стиль изложения научный, язык четкий и лаконичный. Структура логична и последовательна. Содержание соответствует заявленной теме и раскрывает ее достаточно полно.

Библиография представлена 16 наименованиями отечественных и зарубежных источников, оформлена по ГОСТ.

Апелляция к оппонентам отсутствует, однако автор(ы) демонстрирует(ют) критический подход при анализе ERM-систем, выделяя их недостатки.

В заключение делаются конкретные выводы о требованиях к идеальной ERM-системе на основе проведенного анализа.

Статья представляет несомненный интерес для специалистов в области анализа и разработки систем мониторинга и управления закупками, а также для практиков, принимающих решения о выборе и внедрении таких систем.

Предложения по развитию данной работы в будущем:

1. Расширить анализ за счет включения ещё 2-3 ERM-систем. Это позволит сделать сравнение более полным и объективным.
2. Провести анкетирование или интервьюирование компаний, использующих рассмотренные ERM-системы. Это даст более глубокое понимание реального опыта применения этих систем.
3. Дополнить теоретический анализ практическим кейсом выбора и внедрения ERM-системы для конкретной компании. Это приблизит работу к потребностям бизнеса.
4. Разработать экономическое обоснование эффективности внедрения ERM-системы с расчетом окупаемости инвестиций. Это важно для принятия решений на практике.
5. Предложить проект технического задания на разработку собственной идеальной ERM-системы с учетом выявленных недостатков и потребностей бизнеса.

Реализация этих предложений позволит значительно расширить и углубить проведенное исследование.

Вопросы безопасности
Правильная ссылка на статью:
Садеков Р.Р. Актуальные аспекты и проблемные вопросы применения полиграфа на государственной службе в современных условиях // Вопросы безопасности. 2024. № 1. DOI: 10.25136/2409-7543.2024.1.69634 EDN: VOGSDD URL: https://nbpublish.com/library_read_article.php?id=69634

Актуальные аспекты и проблемные вопросы применения полиграфа на государственной службе в современных условиях

Садеков Рустем Рафекович

ORCID: 0000-0002-2739-5490

кандидат педагогических наук

Доцент кафедры психолого-педагогического и медицинского обеспечения деятельности ОВД, ВИПК МВД России

142007, Россия, Московская область, г. Домодедово, ул. Пихтовая, 3

vipk10kafedra@yandex.ru

Статья из рубрики "Кадровое обеспечение национальной безопасности"

DOI:

10.25136/2409-7543.2024.1.69634

EDN:

VOGSDD

Дата направления статьи в редакцию:

20-01-2024

Аннотация: В работе автором рассматриваются проблемные вопросы, связанные с изучением особенностей организации и правового регулирования применения полиграфа на государственной службе. В статье затрагиваются различные аспекты применения полиграфа в государственной сфере, включая юридические аспекты, психолого-педагогические особенности, физиологические и этические вопросы, а также защиту прав граждан. Кроме того, в ней рассматривается опыт использования полиграфа в различных условиях, когда осуществляется процедура получения, выявления, обработки, сохранения и надежности данных, а как следствие, возникает необходимость компетентным специалистам государственного сектора постоянно уделять особое внимание безопасности хранения и использования полученной конфиденциальной информации. В целях анализа эффективности применения полиграфа, в работе описываются задачи, стоящие перед специалистами, рассмотрены

алгоритмы и приемы, используемые при оценке достоверности получаемых сведений. При подготовке материала статьи использовались следующие методы : системный подход, сравнительный анализ и синтез, индукция и дедукция, приемы логического мышления, классифицирование. Основными выводами проведенного автором исследования являются организационные аспекты, направленные на соблюдение прав и свобод граждан, которым по тем или иным основаниям предстоит пройти процедуру тестирования на полиграфном устройстве. Обязательным условием выступает то обстоятельство, что правовое регулирование применения полиграфа на госслужбе требует четкого формулирования, обеспечения прозрачности и объективности процедур, своевременного разъяснения предстоящих нюансов обследования на полиграфе, связанных с этим возможных ограничениях, но при этом соблюдения гарантий для сотрудников и работников, которые подвергаются тестированию. Данная тема, по своему содержанию и смыслу носит актуальный характер, в связи с чем на сегодняшний день является востребованным разработка правовых и методических механизмов применения полиграфа в государственной сфере, основанной на научных разработках ведущих ученых и практиков в этой области знаний.

Ключевые слова:

полиграф, система, специалист, особенность, законодательство, качество, психология, право, обеспечение, гражданин

На сегодняшний день в нашем государстве современные информационные, компьютерные, инновационные кадровые и психолого-педагогические технологии являются неотъемлемыми стратегическими составляющими в организации работы системы государственных органов. Актуальной задачей сотрудников, отвечающих за отбор кандидатов на работу и службу в государственный сектор, является применение комплекса специальных мер, направленных на недопущение проникновения в государственные структуры лиц, которые могут нанести ущерб интересам страны и общества. Следует отметить тот факт, что сложность и достаточно большие объемы обнаруживаемой и поступающей информации вызывают необходимость компетентным специалистам государственного сектора постоянно уделять особое внимание безопасности получения, выявления, обработки, сохранения и надежности данных. При этом необходимо также учитывать, что в каждом случае, недостоверная, искаженная, некорректная информация, ошибочно интерпретированная специалистами, отвечающими за кадровую политику и безопасность, может повлечь за собой серьезные юридические правовые последствия, ущерб от которых может нанести серьезный вред интересам службы и создать реальную угрозу национальной безопасности страны.

Проблемами правового регулирования, организационными аспектами, вопросами повышения эффективности специальных психофизиологических исследований с применением полиграфа в своих исследованиях занимались ученые Богаевский В.А., Печенкова Е.А., Дашко М.Н., Виноградов М.В., Ульянина О.А., Деулин Д.В., Паршутин И.А., Андриянова О.Ю., Ерошенков Н.В., Юрина О.И., Лаврентьева И.В. и ряд других авторов. В частности анализу были подвергнуты актуальные вопросы применения полиграфа в отношении кандидатов поступающих на службу в органы внутренних дел Российской Федерации, эффективность такой процедуры, процессуальные возможности полиграфа при расследовании уголовных дел, в оперативно-разыскной деятельности и уголовном судопроизводстве. Таким образом, актуальность выбранной нами темы

исследования является достаточно высокой.

Однозначно в целях изучения выбранной темы, мы считаем, что в рамках качественного обеспечения функционирования государственной службы, достоверность, оперативность и точность получаемой информации является одним из фундаментов для принятия кадровых и управленческих решений, дальнейшего построения государственной политики в вопросах обеспечения безопасности. А значит актуальным остается вопрос обоснованного и законного применения современных технологий, в том числе и полиграфа, связанных с получением исчерпывающих сведений о лицах, претендующих на работу в государственной сфере.

Кадровые риски, которые могут причинить критический ущерб интересам государственной службы достаточно объёмные, и в их число входит наличие таких факторов, как связи с преступным миром, коррупционные правонарушения, наличие в истории кандидата тщательно скрываемых им криминальных фактах биографии и т.д. Список этот достаточно широкий, в связи с чем специалистам-полиграфологам, руководителям кадрового звена, HR-директорам необходимо четко знать свои полномочия, быть компетентными, грамотными и главное осуществлять свою работу в строгом соответствии с требованиями законодательства.

Можно остановиться на одном из примеров, когда наличие достоверных данных позволяет сделать четкие выводы при рассмотрении вопросов в антикоррупционной сфере. Авторами Головиным А. Ю., Бугаевской Н. В. в своем исследовании изучены особенности расследования коррупционных преступлений, в ходе которого они отмечают, что коррупция охватывает любые злоупотребления должностных лиц, совершенные с корыстной целью [1].

Таким образом, по данному направлению, входящему в область обеспечения кадровой безопасности организации, предприятия, подразделения, проверка ответственными специалистами личных данных граждан и доступ к конфиденциальной информации, выполняют важную роль в деле предотвращения наступления неблагоприятных последствий, а возможно административных нарушений и преступлений, что, несомненно, является важным обстоятельством.

Развивая тему нашей работы, для специалистов государственных служб будет полезным мнение исследователей. В частности автором Красинской Е.С.[2] отмечается, что благодаря полиграфу, в результате его применения, возможно решение, кроме прочих, следующих задач и достижение целей:

- установление причастности подозреваемого к совершению преступления, возможных соучастников, их роли;

- установление мест сокрытия имущества, добытого преступным путем, оружия, наркотических средств и т.д.;

- установление реальности события преступления при опросе потерпевшего;

- установление уровня осведомленности свидетелей о деталях рассматриваемого события [3].

Таким образом, можно сделать вывод о том, что всё вышесказанное говорит о ключевой роли комплексного подхода обеспечения безопасности и проверки информации в деятельности государственных органов и подчеркивает необходимость непрерывного

усовершенствования методов, методик и технологий в этой сфере, одним из рабочих звеньев которого является применение полиграфа.

Однако следует отметить что в отечественном законодательстве пока нет исчерпывающих нормативных правовых актов, позволяющих с помощью полиграфа обезопасить государственные органы от проникновения в них ненадёжных элементов, поэтому работодателю приходится ставить под угрозу сферу субъективных прав сотрудников и работников, что вызывает определенные правовые проблемы.

Правовое регулирование в сфере трудового законодательства не регламентируют надлежащим образом применение полиграфа при приёме на работу и не представляет законных оснований в случае наличия выводов полиграфолога о нецелесообразности продолжения трудовых отношений с работником по результатам тестирования, для увольнения в установленном порядке по дискредитирующим обстоятельствам.

Конечно, можно отметить, что в ряде статей Трудового кодекса Российской Федерации содержатся понятия трудового распорядка, и, в нашем случае можно толковать применение полиграфа в части дополнительного инструмента для руководителя кадровой службы регулировать выполнение подчинёнными надлежащим образом трудового распорядка организации.

Кадровые работники и юристы зачастую включают в трудовые соглашения требования о том, что сотрудники государственных организаций должны следовать чёткому соблюдению правил предприятий и вменяют в должностные инструкции пункт о прохождении полиграфа в случае необходимости. В части 4 статьи 29 Конституции Российской Федерации определены права каждого [4] свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Перечень сведений составляющих государственную тайну определяется Федеральным Законом [5].

В свою очередь применение полиграфа на государственной службе не должно противоречить конституционным требованиям. А пока однозначной правовой позиции и регламентации по отношению к полиграфу не выработано. Отметим также, что существует и множество методических проблем связанных с подходами к проверкам испытуемых на полиграфных устройствах. Пока прослеживается в динамике и позиция судейского корпуса, которая пока не в полной мере поддерживает работодателя в коллизионных вопросах, сопряженных с применением полиграфа

Говоря о полиграфе, следует отметить, что это специальное высокотехнологичное оборудование, которое точно отслеживает динамику психофизиологических реакций обследуемого лица в ответ на предъявленные стимулы (заданные вопросы, связанные непосредственно с событием или фактом, который подлежит проверке), путем регистрации физиологических показателей деятельности органов дыхания, сердечно-сосудистой системы, секреции потовых желез [6].

Как мы отмечали ранее, характер решаемых полиграфологами задач носит специфический характер и связан обеспечением безопасности государственных структур, принятием решений в рамках проведения скрининговых исследований и уголовного судопроизводства[7].

К примеру, специалистом-полиграфологом в ходе инструментальной детекции лжи может быть исследовано следующее:

1. Кровяное давление: во время теста полиграф измеряет изменения кровяного давления. Рост кровяного давления может свидетельствовать о стрессе или нервозности человека. Это также может быть признаком попыток скрыть правду или же обман. Кровяное давление замеряется с помощью манжеты, которая надевается на руку испытуемого и соединяется с датчиком, либо более совершенным способом, техническая возможность которого заложена в модель современного полиграфного устройства.

2. Пульс: «детектор лжи» также контролирует изменения в частоте сердечных сокращений испытуемого. Повышение частоты сердечных сокращений может означать стресс, волнительное состояние или попытку скрыть те или иные сведения. Для измерения частоты пульса используются особые датчики, которые можно расположить в соответствии с инструкцией к полиграфу.

3. Дыхание: частота и глубина дыхания также могут измеряться полиграфом. Изменения в дыхании могут указывать на напряжение и попытку скрыть нежелательную для обследуемого лица информацию. Для регистрации изменений в дыхательной деятельности используются специальный алгоритм полиграфного устройства.

4. Электрическая активность кожи: полиграф измеряет уровень электрической активности кожи, который может изменяться в ответ на возникновение эмоционального возбуждения. Это может ассоциироваться с попыткой скрыть информацию или совершить обман. Замеры производятся с помощью электродов, которые размещаются на теле испытуемого в установленном порядке.

Иными словами, исходя из вышеизложенного, на основании проведенного полиграфного исследования специалист осуществляет анализ физиологических показателей во время опроса, чтобы установить вероятность того, что человек говорил правду или лгал. Казалось бы, очевидна же польза от этой процедуры, которая носит добровольный характер и не наносит какой либо физический вред обследуемому лицу.

Тем не менее, его использование на госслужбе все же вызывает некоторые юридические и этические вопросы, обусловленные несовершенством данного метода. Полиграфолог не всегда бывает точным и может выдавать ошибочные суждения, что может повлечь за собой неверные выводы о причастности или непричастности человека к тому или иному фактору.

Несомненно, если рассматривать применение полиграфа на государственной службе с юридической точки зрения, то оно должно иметь четкое законодательное закрепление. Это значит, что должны быть установлены четкие правовые механизмы, которые определят условия и процедуры применения полиграфа. Эти правила должны содержать формулирование отдельных случаев, когда использование полиграфа допускается, например, в правоохранительной сфере:

1. Расследование преступлений:

- При расследовании тяжких и особо тяжких преступлений, применение полиграфа может оказаться оправданным. С помощью этой технологии правоохранительным органам предоставляется возможным собрать дополнительные данные по существу обстоятельств преступлений.

- В рамках уголовного расследования полиграф может быть использован для проверки достоверности показаний подозреваемых или свидетелей.

2. Вопросы, важные для обеспечения национальной безопасности:

- Полиграф можно использовать при трудоустройстве или проверке сотрудников, которые работают с конфиденциальной информацией или имеют доступ к различным формам государственной тайны. Это дает возможность убедиться в их преданности, лояльности и благонадежности.

- При расследовании утечек информации и шпионажа полиграф может быть применен для выявления возможных преступников.

Применение полиграфа в этих аспектах должно быть строго регламентировано и проводиться в соответствии с законодательством, чтобы обеспечить защиту прав и свобод граждан и соблюдение верховенства закона.

Рассуждая о правовом регулировании применения полиграфа на госслужбе мы должны придерживаться позиций об ограничениях и гарантиях для работников, которые подвергаются тестированию.

В.И. Миронов выделяет основные признаки, характеризующие гарантии работников. Так, к ним можно отнести: установленные в нормативных правовых актах, соглашениях, коллективных и трудовых договорах средства, способы и условия, обеспечивающие осуществление прав граждан в отношениях, входящих в предмет трудового права; непосредственное обеспечение предусмотренных в законодательстве трудовых прав; обеспечение осуществления как неимущественных, так и имущественных прав работников в сфере труда.[8]

Приженникова А.Н. отмечает, что защита работника как наиболее слабой (в экономическом смысле) стороны трудового правоотношения реализуется, в установлении принципов правового регулирования трудовых и иных непосредственно связанных с ними отношений (ст. 2 ТК РФ) [9].

Чтобы обеспечить справедливость и защиту прав сотрудников, ограничения и гарантии должны быть четко определены. Ряд из них успешно претворяются на практике.

Прежде всего, необходимо обязательное оповещение сотрудников о планируемом тестировании на полиграфе, которое должно включать в себя подробное информирование о процедуре, целях и последствиях проведения тестирования. Сотрудники в обязательном порядке должны быть уведомлены соответствующими специалистами о том, что тестирование на полиграфе входит в процедуру подтверждения правдивости их заявлений или действий в ходе выполнения ими своих должностных обязанностей.

Также сотрудникам должна быть дана дополнительная возможность заранее изучить правила и процедуры проведения тестирования на полиграфе, чтобы они были готовы к процессу и понимали, что от них потребуется. Это позволит избежать недоразумений и конфликтных ситуаций в ходе тестирования.

Очень важно, чтобы у работников была такая возможность - задавать вопросы и получать разъяснения у специалистов по проверке на детекторе лжи до того, как начнется процедура.

Подобный подход к делу позволит обеспечить сотрудникам прозрачность и понимание ими всех аспектов тестирования, что, в свою очередь, поспособствует созданию атмосферы доверия и справедливости в рамках процесса применения полиграфа на государственной службе.

Кроме того, сотрудники должны иметь право не проходить полиграф без негативных последствий для своей профессиональной деятельности. Это подразумевает, что на работников не должно быть оказано давление или угроз со стороны их работодателя или администрации, если они не согласятся пройти тестирование.

Во избежание возможных злоупотреблений или нарушений прав сотрудников важно также на уровне кадрового аппарата государственного предприятия разработать четкие правила и порядок проведения проверок на полиграфе. К примеру, возможно, рассмотреть включение в участие в процедуре тестирования независимого наблюдателя для повышения объективности процесса, с разработкой соответствующих инструкций и правил.

И наконец, как мы отмечали ранее, конфиденциальность полученных результатов проверки на полиграфе играет важную роль в законодательном регулировании его применения на государственной службе. В результатах проверки на полиграфе содержится важная информация о личной жизни и деятельности сотрудника, поэтому она подлежат рассмотрению в таком формате, как конфиденциальная информация. Эти сведения не могут быть раскрыты без прямого письменного разрешения сотрудника, прошедшего проверку.

Сохранение конфиденциальности полученных результатов тестирования на детекторе лжи помогает обеспечить защиту частной и личной жизни сотрудника. Обнародование такой информации без его разрешения может привести к отрицательным последствиям для его деловой репутации, а также к ущемлению его прав на защиту личных данных.

Автор Абрамова А.В. приводит такой важный аспект, что при получении информации от участников уголовного производства следователь, дознаватель, суд обязаны гарантировать ее сохранность, и несут ответственность за разглашение такой информации [10].

В связи с этим важно, чтобы в законодательстве были четко определены требования к соблюдению конфиденциальности сведений о результатах тестирования на полиграфе и предусмотрена ответственность за их незаконное разглашение.

Таким образом, эти ограничения и гарантии являются необходимыми для того, чтобы обеспечить объективность и защиту прав сотрудников при применении полиграфа на государственной службе.

Поэтому стоит отметить, что такой взгляд обеспечит соблюдение прав и свободы работников, охрану их личной жизни и предотвращение возможного злоупотребления при применении полиграфа на госслужбе.

При обсуждении актуальных вопросов применения полиграфа на государственной службе важную роль также играют этические вопросы. Следует учитывать следующие принципы:

1. Принцип справедливости: Согласно этому принципу, применение полиграфа на государственной службе не должно противоречить закону и должно быть справедливым и равноправным. Это говорит о том, что никто не может подвергаться дискриминации или злоупотреблению служебным положением по признаку расы, пола, религии, национальности или других личных качеств.

2. Принцип конфиденциальности: Согласно этому принципу, сведения, полученные с помощью полиграфа, должны считаться конфиденциальными и не должны разглашаться

без получения согласия испытуемого. Это необходимо для защиты частной жизни и конфиденциальности граждан.

3. Принцип личного достоинства: Согласно этому принципу, при использовании полиграфа следует уважать и защищать достоинство всех тестируемых лиц. Это указывает на то, что процедуры тестирования должны проходить с учетом уважения к человеку и без нарушения его прав, свобод и интересов.

При этом на наш взгляд всегда важно обеспечить надежную защиту прав граждан от возможных злоупотреблений со стороны государственных органов при использовании полиграфа. А для этого, мы считаем, должны быть соблюдены неотъемлемые обязательные этапы и процедуры применения полиграфа.

Они включают в себя:

- Обязательное согласие испытуемого: это подразумевает, что перед началом тестирования на полиграфе от лица, в отношении которого будет проводиться проверка, должно быть получено письменное согласие. Это позволяет гарантировать, что процедура будет проведена исключительно только с согласия испытуемого и не нарушит его прав на неприкосновенность частной жизни и личного достоинства.

- Обеспечение независимого наблюдения за процессом тестирования: Для обеспечения честности и объективности процедуры важно организовать независимое сопровождение процесса тестирования. К примеру, это может быть сотрудник независимой организации или сотрудник юридической службы, который будет лично присутствовать при тестировании. Это позволит предотвратить возможное злоупотребление со стороны тех, кто организовывает и осуществляет тестирование.

- Создание механизмов контроля возможного неправомерного использования инструмента: Для предотвращения неправомерного использования полиграфа следует создать механизмы контроля за его применением. Это может быть формой в виде регулярных проверок и аудита процедур применения полиграфа, а также введение ответственности за его неправомерное использование. Подобные механизмы предотвращают злоупотребления и сохраняют добросовестность и прозрачность процедуры.

- Возможность обжалования результатов тестирования и защита прав граждан от неправомерного использования полученной информации: испытуемому следует предоставить возможность подачи апелляции на результаты тестирования и защиты своих прав, в случае ненадлежащего использования полученной информации. Это предполагает установление порядка обжалования результатов и законодательных гарантий сохранения конфиденциальности полученных данных для исключения их неправомерного использования.

- Обучение и сертификация персонала, проводящего тестирование: Необходимо убедиться, что специалисты, проводящие тестирование на полиграфе, проходили специальную подготовку, обучение и аттестацию. Такой подход является гарантией их профессионализма, знания ими этических норм и правил проведения тестирования, что, в конечном счете, способствует честности и объективности процедуры.

Тем самым, чтобы обеспечить охрану прав граждан от возможного злоупотребления полиграфом, следует установить корпоративные строгие правила и процедуры его использования, включающие получение добровольного согласия тестируемого,

проведение независимого наблюдения за процессом проверки и другие немаловажные аспекты.

Важно также в процессе профессиональной подготовки специалистов-полиграфологов учитывать то обстоятельство, что в настоящее время особое значение со стороны государства придается повышению уровня образования, правовой культуры, профессиональной компетентности сотрудников полиции при выполнении ими своих служебных обязанностей, предусмотренных федеральным законодательством в этой сфере [11].

Если проанализировать международную практику применения полиграфа в некоторых странах, то можно отметить, что существуют разнообразные подходы к использованию детектора лжи на государственной службе. В одних странах, например, в США, полиграф применяется в строгом порядке, он регламентирован и используется только в определенных случаях, например, при проверке правоохранительных органов или в расследованиях, связанных с национальной безопасностью. Это связано с тем, что в США существует законодательство, регламентирующее использование полиграфа и защиту прав сотрудников.

В Израиле, применение полиграфа может быть более масштабным, например, при наборе сотрудников правоохранительных органов. В данном случае законодательство может обеспечить более широкую сферу использования полиграфа и его применение в различных областях государственной службы.

Кудрявцев Д.С. в своей работе приводит опыт использования полиграфа практически во всех правоохранительных органах Республики Беларусь, а также в Государственном комитете судебных экспертиз, где его возможности применяются при проведении психофизиологических исследований. Данный вид экспертиз проводится при наличии неустранимых противоречий в показаниях участников уголовного процесса (свидетелей, потерпевших, обвиняемых, подозреваемых) или в случае противоречия между их показаниями и другими доказательствами по делу. Задачей эксперта является выявление у исследуемого лица признаков скрываемой на уровне психофизиологических реакций информации об интересующих орган предварительного следствия событиях[12].

Вышеперечисленные примеры заслуживают внимания специалистов в области детекции лжи и предоставляют возможность опираться на имеющиеся практические наработки в международном формате применения полиграфа, однако говоря о законодательстве Российской Федерации в настоящее время, просто брать и копировать существующие подходы мы не можем по ряду объективных причин и обстоятельств, связанных со спецификой государственного устройства, особенностями менталитета населения нашей страны и нормами права. Нам предстоит серьезная работа по разработке и внедрению национальных правовых механизмов, позволяющих использовать полученные в результате полиграфных исследований сведения для принятия различных процессуальных решений.

Следует отметить, что сложность вопроса заключается в том, что полиграф не может быть абсолютно надежным инструментом. Его показания в ходе анализа и интерпретации специалистами могут быть подвержены ошибкам и искажаться под воздействием таких факторов, как стресс, волнение или физиологические особенности человека. В связи с таким положением дел встает вопрос о праве на частную жизнь и защите личных данных сотрудников и работников.

Также к дополнительным проблемам, связанным с применением полиграфа, можно отнести возможность вмешательства в частную жизнь сотрудников и работников, а также потенциальные ошибки в трактовке результатов тестирования специалистами. Кроме того, необходимо учитывать и те обстоятельства, что применение полиграфа может способствовать созданию негативной рабочей обстановки и вызвать у сотрудников недоверие, что может отрицательно повлиять на их работоспособность и уровень мотивации. В связи с чем, алгоритм применения этих технологий должен носить сугубо профессиональный, деловой и конфиденциальный характер, с обеспечением соблюдения прав и свобод обследуемых лиц.

В заключение следует отметить, что вопросы применения полиграфа на государственной службе, с точки зрения общественности, юристов, научного сообщества и практики, имеют различные проблемные стороны, дискуссия на эту тему продолжается.

Полиграф через опыт его применения, правовое обеспечение и регламентацию несомненно должен и может стать полезным инструментом для специалистов, в целях подтверждения достоверности информации и обеспечения безопасности, и, безусловно, отмечаем, что применение этой технологии требует четкого правового регламента, учета этических аспектов и защиты конституционных и трудовых прав граждан на должном законодательном уровне.

Продолжая работу в этом направлении, необходимо сформировать обоснованные позиции профессионального сообщества полиграфологов, с учетом реалий сегодняшнего дня.

В связи с чем, несомненно, работу необходимо продолжить, вероятно, сформировать расширенную рабочую группу специалистов и экспертов, из числа наиболее авторитетных полиграфологов-практиков и ученых, с целью выработки взвешенной позиции, и, ее последующего законодательного закрепления в части организационного и правового регулирования применения полиграфа на государственной службе.

Библиография

1. Головин А. Ю., Бугаевская Н. В. Особенности расследования коррупционных преступлений // Известия ТулГУ. Экономические и юридические науки. 2012. №1-2.
2. Красинская, Е. С. Некоторые аспекты использования полиграфа при раскрытии и расследовании преступлений // Полицейская деятельность. – 2021. – № 3. – С. 13-23. – DOI 10.7256/2454-0692.2021.3.35751. – EDN DQVCHS.
3. Истомина, И. Ф. Использование полиграфа при расследовании и раскрытии преступлений // Байкальский студенческий юридический форум-2022. Современные проблемы правотворчества и правоприменения : Материалы Всероссийской студенческой научно-практической конференции, Иркутск, 24 марта 2022 года / Отв. редакторы А.М. Бычкова, Н.В Кешикова. Том 2. – Иркутск: Иркутский институт (филиал) ВГУЮ (РПА Минюста России), 2022. – С. 180-185. – EDN JNSLUY.
4. Козырев, В. Д. Видеозапись. Законное и незаконное использование: спорные вопросы и их решения // E-Scio. – 2021. – № 2(53). – С. 327-339. – EDN XNRPXM.
5. Петров, К. С. Развитие института защиты государственной тайны в России в советский и постсоветский периоды // Оперативник (сыщик). – 2016. – № 4(49). – С. 4-8. – EDN XDNFRX.
6. Неймышева, М. Д. Применение полиграфа в оперативно-розыскной деятельности // Проблемы государства и права в исследованиях студентов : Сборник материалов XVIII Межвузовской научно-практической конференции, Москва-Тюмень, 14 апреля

2023 года. – Москва-Тюмень: Автономная некоммерческая организация высшего образования "Институт деловой карьеры", 2023. – С. 212-214. – EDN QAPDLH.

7. Садеков Р.Р. Формирование правовой культуры специалиста-полиграфолога в процессе профессионального обучения // Полицейская деятельность. – 2023. – № 2. – С. 48-55. DOI: 10.7256/2454-0692.2023.2.39764 EDN: VEEWKW URL: https://nbpublish.com/library_read_article.php?id=39764
8. Миронов В. И. Трудовое право: учебник для ВУЗов. – СПб.: Питер, 2009. 864 с.
9. Приженникова, А. Н. Реализация гарантий прав работника по российскому трудовому законодательству // Colloquium-Journal. – 2019. – № 9-10(33). – С. 50-58. – EDN NAKQJG.
10. Абрамова, А. В. Проблема защиты конфиденциальности личных данных участников уголовного судопроизводства в условиях внедрения электронного правосудия // Аллея науки. – 2019. – Т. 4, № 1(28). – С. 650-653. – EDN ZAALCX.
11. Садеков Р.Р., Крохина Ю.В. Организационно-правовые аспекты организации профессиональной подготовки сотрудников МВД России в системе дополнительного профессионального образования // Вопросы безопасности. – 2023. – № 1. – С. 58-65. DOI: 10.25136/2409-7543.2023.1.39710 EDN: LOQZMF URL: https://nbpublish.com/library_read_article.php?id=3971
12. Кудрявцев Д. С. "Опыт и перспективы использования полиграфа как метода преодоления противодействия раскрытию и расследованию преступлений в Республике Беларусь" Известия Тульского государственного университета. Экономические и юридические науки, №4-2, 2017. С. 152-159.

Результаты процедуры рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов издательства можно ознакомиться здесь.

Предметом исследования в представленной на рецензирование статье являются, как это следует из ее наименования, актуальные аспекты и проблемные вопросы применения полиграфа на государственной службе в современных условиях. Заявленные границы исследования соблюдены автором.
Методология исследования в тексте статьи не раскрывается, но очевидно, что ученым использовались всеобщий диалектический, логический, сравнительно-правовой, формально-юридический методы исследования.
Актуальность избранной автором темы исследования несомненна и обосновывается им следующим образом: "... в рамках качественного обеспечения функционирования государственной службы, достоверность, оперативность и точность получаемой информации является одним из фундаментов для принятия кадровых и управленческих решений, дальнейшего построения государственной политики в вопросах обеспечения безопасности. А значит актуальным остается вопрос обоснованного и законного применения современных технологий, в том числе и полиграфа, связанных с получением исчерпывающих сведений о лицах, претендующих на работу в государственной сфере. Кадровые риски, которые могут причинить критический ущерб интересам государственной службы достаточно объёмные, и в их число входит наличие таких факторов, как связи с преступным миром, коррупционные правонарушения, наличие в истории кандидата тщательно скрываемых им криминальных фактах биографии и т.д. Список этот достаточно широкий, в связи с чем специалистам-полиграфологам, руководителям кадрового звена, HR-директорам необходимо четко

знать свои полномочия, быть компетентными, грамотными и главное осуществлять свою работу в строгом соответствии с требованиями законодательства". Дополнительно ученому необходимо перечислить фамилии ведущих специалистов, занимавшихся исследованием поднимаемых в статье проблем, а также раскрыть степень их изученности.

Научная новизна работы проявляется в некоторых заключениях автора: "... мы считаем, должны быть соблюдены неотъемлемые обязательные этапы и процедуры применения полиграфа. Они включают в себя:

- Обязательное согласие испытуемого: это подразумевает, что перед началом тестирования на полиграфе от лица, в отношении которого будет проводиться проверка, должно быть получено письменное согласие. ... - Обеспечение независимого наблюдения за процессом тестирования: Для обеспечения честности и объективности процедуры важно организовать независимое сопровождение процесса тестирования. К примеру, это может быть сотрудник независимой организации или сотрудник юридической службы, который будет лично присутствовать при тестировании. Это позволит предотвратить возможное злоупотребление со стороны тех, кто организовывает и осуществляет тестирование. - Создание механизмов контроля возможного неправомерного использования инструмента: Для предотвращения неправомерного использования полиграфа следует создать механизмы контроля за его применением. Это может быть формой в виде регулярных проверок и аудита процедур применения полиграфа, а также введение ответственности за его неправомерное использование. Подобные механизмы предотвращают злоупотребления и сохраняют добросовестность и прозрачность процедуры. - Возможность обжалования результатов тестирования и защита прав граждан от неправомерного использования полученной информации: испытуемому следует предоставить возможность подачи апелляции на результаты тестирования и защиты своих прав в случае ненадлежащего использования полученной информации. Это предполагает установление порядка обжалования результатов и законодательных гарантий сохранения конфиденциальности полученных данных для исключения их неправомерного использования. - Обучение и сертификация персонала, проводящего тестирование: Необходимо убедиться, что специалисты, проводящие тестирование на полиграфе, проходили специальную подготовку, обучение и аттестацию. Такой подход является гарантией их профессионализма, знания ими этических норм и правил проведения тестирования, что, в конечном счете, способствует честности и объективности процедуры" и др. Таким образом, статья вносит определенный вклад в развитие отечественной правовой науки и заслуживает внимания потенциальных читателей, но ряд ее положений нуждается в уточнении и конкретизации.

Научный стиль исследования выдержан автором в полной мере.

Структура работы вполне логична. Во вводной части статьи автор обосновывает актуальность избранной им темы исследования. В основной части работы ученый исследует ряд проблем, связанных с применением полиграфа, и предлагает пути их решения. В заключительной части статьи содержатся общие выводы по результатам проведенного исследования.

Содержание статьи соответствует ее наименованию, но не лишено некоторых недостатков.

Автор говорит о проблемах правового регулирования применения полиграфа, и только потом дает определение данного понятия, тем самым нарушая логику изложения материалов статьи.

Ученый пишет: "Это значит, что должны быть установлены законы и нормативные акты, которые определяют условия и процедуры применения полиграфа". Законы тоже

относятся к нормативным актам. Налицо логическая ошибка.

Автор указывает: "1. Расследование тяжких преступлений или нарушений закона: - При расследовании тяжких преступлений, таких как убийство, террористический акт, факты коррупции и другие значительные правонарушения, применение полиграфа может оказаться оправданным". Расследуются исключительно преступления, а не правонарушения.

Ученый пишет: "Если проанализировать международную практику применения полиграфа в некоторых странах, то можно отметить, что существуют разнообразные подходы к использованию детектора лжи на государственной службе. В одних странах, например, в США, полиграф применяется в строгом порядке, он регламентирован и используется только в определенных случаях, например, при проверке правоохранительных органов или в расследованиях, связанных с национальной безопасностью. Это связано с тем, что в США существует законодательство, регламентирующее использование полиграфа и защиту прав сотрудников. В отличие от этого, в Израиле применение полиграфа может быть более масштабным, например, при наборе сотрудников правоохранительных органов. В данном случае законодательство может обеспечить более широкую сферу использования полиграфа и его применение в различных областях государственной службы". Критического анализа описываемых подходов к применению полиграфа автор не осуществляет, не выявляет их достоинств и недостатков, не дает соответствующих рекомендаций.

В работе встречается множество опечаток, орфографических и пунктуационных ошибок.

Так, автор пишет: "Отметим также, что существует и множество методических проблем связанных с подходами к проверкам испытуемых на полиграфных устройствах" - после слова "проблем" пропущена запятая.

Ученый отмечает: "Рассуждая о правовом регулировании применения полиграфа на госслужбе мы должны придерживаться позиций об ограничениях и гарантиях для работников, которые подвергаются тестированию" - после словосочетания "на госслужбе" пропущена запятая.

Автор указывает: "В.И. Миронов выделяет основные признаки, характеризующие гарантии работников. Так, к ним можно отнести: установление в законодательстве, соглашениях, коллективном договоре, иных локальных правовых актах организации, трудовом договоре;" - установление чего?

Ученый пишет: "В заключении следует отметить, что вопросы применения полиграфа на государственной службе с точки зрения общественности, юристов, научного сообщества и практики имеют различные проблемные стороны, дискуссия на эту тему продолжается" - "В заключение" (предлог).

Приведенный перечень опечаток и ошибок не является исчерпывающим! Статья нуждается в тщательном вычитывании с привлечением специалиста-филолога.

Библиография исследования представлена 11 источниками (научными статьями и учебником). С формальной точки зрения этого достаточно, но некоторые положения работы нуждаются в углублении.

Апелляция к оппонентам как таковая отсутствует. Автор ссылается на ряд теоретических работ исключительно в подтверждение своих суждений или для иллюстрирования отдельных положений работы, но в научную дискуссию не вступает.

Выводы по результатам проведенного исследования имеются ("В заключении следует отметить, что вопросы применения полиграфа на государственной службе с точки зрения общественности, юристов, научного сообщества и практики имеют различные проблемные стороны, дискуссия на эту тему продолжается. Полиграф через опыт его применения, правовое обеспечение и регламентацию должен стать полезным инструментом для специалистов в целях подтверждения достоверности информации и

обеспечения безопасности, и, безусловно, отмечаем, что применение этой технологии требует четкого правового регламента, учета этических аспектов и защиты конституционных и трудовых прав граждан на должном законодательном уровне"), но носят общий характер и не отражают всех научных достижений автора. Таким образом, они нуждаются в конкретизации. Ученому необходимо определить, какие именно изменения в части регламентации применения полиграфа необходимо внести в действующее российское законодательство.

Интерес читательской аудитории к представленной на рецензирование статье может быть проявлен прежде всего со стороны специалистов в сфере трудового права, уголовного процесса и криминалистики при условии ее существенной доработки: раскрытии методологии исследования, дополнительном обосновании актуальности его темы, уточнении и углублении отдельных положений работы, введении дополнительных элементов научной новизны и дискуссионности, формулировании четких и конкретных выводов по результатам проведенного исследования, устранении многочисленных опечаток и ошибок в тексте статьи.

Результаты процедуры повторного рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.

Со списком рецензентов издательства можно ознакомиться здесь.

РЕЦЕНЗИЯ

на статью на тему «Актуальные аспекты и проблемные вопросы применения полиграфа на государственной службе в современных условиях».

Предмет исследования.

Предложенная на рецензирование статья посвящена актуальным вопросам применения полиграфа на государственной службе в современных условиях. Автор рассматривает различные юридические и этические вопросы, связанные с использованием полиграфа, а также практические проблемы его внедрения в деятельность кадровых подразделений различных органов. В качестве предмета исследования выступили, прежде всего, мнения различных ученых, положения правовых актов, а также материалы практики использования полиграфа.

Методология исследования.

Цель исследования прямо в статье не заявлена. При этом она может быть ясно понята из названия и содержания работы. Цель может быть обозначена в качестве рассмотрения и разрешения отдельных проблемных аспектов вопроса о применении полиграфа на государственной службе в современных условиях. Исходя из поставленных цели и задач, автором выбрана методологическая основа исследования.

В частности, автором используется совокупность общенаучных методов познания: анализ, синтез, аналогия, дедукция, индукция, другие. В частности, методы анализа и синтеза позволили обобщить и разделить выводы различных научных подходов к предложенной тематике, а также сделать конкретные выводы из материалов практики применения полиграфа на государственной службе в современных условиях.

Наибольшую роль сыграли специально-юридические методы. В частности, автором активно применялся формально-юридический метод, который позволил провести анализ и осуществить толкование норм действующего законодательства. Например, следующий вывод автора: «Кадровые работники и юристы зачастую включают в трудовые соглашения требования о том, что сотрудники государственных организаций должны

следовать чёткому соблюдению правил предприятий и вменяют в должностные инструкции пункт о прохождении полиграфа в случае необходимости. В части 4 статьи 29 Конституции Российской Федерации определены права каждого [4] свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Перечень сведений составляющих государственную тайну определяется Федеральным Законом [5]. В свою очередь применение полиграфа на государственной службе не должно противоречить конституционным требованиям. А пока однозначной правовой позиции и регламентации по отношению к полиграфу не выработано. Отметим также, что существует и множество методических проблем связанных с подходами к проверкам испытуемых на полиграфных устройствах. Пока прослеживается в динамике и позиция судейского корпуса, которая пока не в полной мере поддерживает работодателя в коллизионных вопросах, сопряженных с применением полиграфа».
Таким образом, выбранная автором методология в полной мере адекватна цели исследования, позволяет изучить все аспекты темы в ее совокупности.

Актуальность.
Актуальность заявленной проблематики не вызывает сомнений. Имеется как теоретический, так и практический аспекты значимости предложенной темы. С точки зрения теории тема применения полиграфа на государственной службе в современных условиях. Безусловно, важно применять использование современных технических средств для решения конкретных государственных задач (в данном случае: обеспечение проверенными кадрами органов государственной власти). Однако в ситуации с полиграфом это приводит к самым различным юридическим и этическим вопросам. Сложно спорить с автором в том, что «На сегодняшний день в нашем государстве современные информационные, компьютерные, инновационные кадровые и психолого-педагогические технологии являются неотъемлемыми стратегическими составляющими в организации работы системы государственных органов. Актуальной задачей сотрудников, отвечающих за отбор кандидатов на работу и службу в государственный сектор, является применение комплекса специальных мер, направленных на недопущение проникновения в государственные структуры лиц, которые могут нанести ущерб интересам страны и общества. Следует отметить тот факт, что сложность и достаточно большие объемы обнаруживаемой и поступающей информации вызывают необходимость компетентным специалистам государственного сектора постоянно уделять особое внимание безопасности получения, выявления, обработки, сохранения и надежности данных. При этом необходимо также учитывать, что в каждом случае, недостоверная, искаженная, некорректная информация, ошибочно интерпретированная специалистами, отвечающими за кадровую политику и безопасность, может повлечь за собой серьезные юридические правовые последствия, ущерб от которых может нанести серьезный вред интересам службы и создать реальную угрозу национальной безопасности страны».
Тем самым, научные изыскания в предложенной области стоит только поприветствовать.

Научная новизна.
Научная новизна предложенной статьи не вызывает сомнений. Во-первых, она выражается в конкретных выводах автора. Среди них, например, такой вывод:
«Полиграф через опыт его применения, правовое обеспечение и регламентацию несомненно должен и может стать полезным инструментом для специалистов, в целях подтверждения достоверности информации и обеспечения безопасности, и, безусловно, отмечаем, что применение этой технологии требует четкого правового регламента, учета этических аспектов и защиты конституционных и трудовых прав граждан на должном

законодательном уровне. Продолжая работу в этом направлении, необходимо сформировать обоснованные позиции профессионального сообщества полиграфологов, с учетом реалий сегодняшнего дня. В связи с чем, несомненно, работу необходимо продолжить, вероятно, сформировать расширенную рабочую группу специалистов и экспертов, из числа наиболее авторитетных полиграфологов-практиков и ученых, с целью выработки взвешенной позиции, и, ее последующего законодательного закрепления в части организационного и правового регулирования применения полиграфа на государственной службе».

Указанный и иные теоретические выводы могут быть использованы в дальнейших научных исследованиях.

Во-вторых, автором выявлены конкретные проблемы в данной сфере, что может быть использовано в правотворческой деятельности, а также конкретными специалистами по кадрам в целях совершенствования процедур использования полиграфа.

Таким образом, материалы статьи могут иметь определенных интерес для научного сообщества с точки зрения развития вклада в развитие науки.

Стиль, структура, содержание.

Тематика статьи соответствует специализации журнала «Вопросы безопасности», так как она посвящена правовым проблемам, связанным с применением полиграфа на государственной службе в современных условиях.

Содержание статьи в полной мере соответствует названию, так как автор рассмотрел заявленные проблемы, в целом достиг цели исследования.

Качество представления исследования и его результатов следует признать в полной мере положительным. Из текста статьи прямо следуют предмет, задачи, методология и основные результаты исследования.

Оформление работы в целом соответствует требованиям, предъявляемым к подобного рода работам. Существенных нарушений данных требований не обнаружено.

Библиография.

Следует высоко оценить качество использованной литературы. Автором активно использована литература, представленная авторами из России (Богаевский В.А., Печенкова Е.А., Дашко М.Н., Виноградов М.В., Ульянина О.А., Деулин Д.В., Паршутин И.А., Андриянова О.Ю., Ерошенков Н.В., Юрина О.И., Лаврентьева И.В. и другие).

Таким образом, труды приведенных авторов соответствуют теме исследования, обладают признаком достаточности, способствуют раскрытию различных аспектов темы.

Апелляция к оппонентам.

Автор провел серьезный анализ текущего состояния исследуемой проблемы. Все цитаты ученых сопровождаются авторскими комментариями. То есть автор показывает разные точки зрения на проблему и пытается аргументировать более правильную по его мнению.

Выводы, интерес читательской аудитории.

Выводы в полной мере являются логичными, так как они получены с использованием общепризнанной методологии. Статья может быть интересна читательской аудитории в плане наличия в ней систематизированных позиций автора применительно к решению некоторых проблем, возникающих при применении полиграфа на государственной службе в современных условиях.

На основании изложенного, суммируя все положительные и отрицательные стороны статьи

«Рекомендую опубликовать»

Англоязычные метаданные

Some ways of countering fraud committed using digital payments according to the legislation of Russia and China

Sergeeva Anzhelika Anatol'evna

PhD in Law

Associate Professor, Department of Criminal Law and Procedure, St. Petersburg Institute (Branch) All-Russian State University of Justice

190000, Russia, Saint Petersburg, Baskov lane, 16

lokhi@yandex.ru

Gurev Mikhail Sergeevich

PhD in Law

Associate Professor, Department of Criminal Law and Procedure, St. Petersburg Institute (branch) of the All-Russian State University of Justice

190000, Russia, St. Petersburg, Baskov Lane, 16

lokhi@rambler.ru

Kirillova Yana Maksimovna

PhD in Law

Associate Professor, Department of Criminal Law and Procedure, St. Petersburg Institute (branch) of the All-Russian State University of Justice

190000, Russia, St. Petersburg, Baskov Lane, 16

lokhi@rambler.ru

Pyatkova Oksana Vladimirovna

PhD in Law

Associate Professor, Department of Criminal Law and Procedure, St. Petersburg Institute (branch) of the All-Russian State University of Justice

190000, Russia, St. Petersburg, Baskov Lane, 16

lokhi@rambler.ru

Feizullaev Firudin Makhramali Ogly

PhD in Law

Associate Professor, Department of Criminal Law and Procedure, St. Petersburg Institute (branch) of the All-Russian State University of Justice

190000, Russia, St. Petersburg, Baskov Lane, 16

lokhi@rambler.ru

Lototskii Anton Sergeevich

Senior Lecturer, Department of Criminal Law and Procedure, St. Petersburg Institute (branch) of the All-Russian State University of Justice

190000, Russia, St. Petersburg, Baskov Lane, 16

lokhi@rambler.ru

Abstract. The relevance of the study is due to the increase in crimes on funds operating in non-cash form. In the future, the development of the digital economy will be associated with an increase in such risks. In this regard, the authors have made a comparison of the Russian

and Chinese experience of their minimization. In both countries, there is a steady increase in the number of thefts committed using illegal access to digital payment systems. At the same time, criminal law norms designed to counteract fraudulent actions have certain drawbacks. The judicial interpretation of these norms is also ambiguous. In conditions of limited functioning of international payment systems, theft of non-cash funds can be committed in new ways. In the future, non-cash payments will increase in volume, so it is necessary to improve the security of their conduct. The authors used a comparative legal method, as well as analysis and synthesis, which made it possible to give the study a complete character. The article summarizes the Russian and Chinese experience in countering the theft of funds deposited in non-cash form. Since the share of non-cash payments in Russia and China is significant, not only economic entities, but also citizens are involved in their turnover. The latter, not having financial literacy, can become victims of fraudsters. The state policy regarding the regulation of non-cash payments is built in the direction of establishing control over the functioning of electronic platforms. However, this does not seem to be sufficient, since it does not reduce financial risks. The criminal legal field remains virtually the only lever to counteract this type of theft. At the same time, the structure of the criminal law prohibition does not reflect the nature and degree of public danger of fraudulent actions and does not clearly distinguish them from secret theft.

Keywords: penalty, damage, lie, robbery, fraud, non-cash payments, payment, prevention, cybercrime, digital economy

References (transliterated)

1. Trofimenkova E.V., Yun Sunbei, Yan Minsy. Razvitie rossiisko-kitaiskoi elektronnoi torgovli // Oikumena. Regionovedcheskie issledovaniya. 2021. № 4. S. 49-55.
2. Fenchao Tsui. Razvitie i izmenenie elektronnoi kommertsii v Kitae // Nauchnyi zhurnal. 2018. № 1. S. 80-82.
3. Kochoi S.M. Novye normy o moshennichestve v UK: osobennosti i razlichiya // Kriminologicheskii zhurnal Baikal'skogo gosudarstvennogo universiteta ekonomiki i prava. 2013. № 4. S. 105-108.
4. Pitul'ko K.V., Sergeeva A.A. Problemy presecheniya moshennicheskikh deistvii, sovershaemykh s ispol'zovaniem resursov seti «Internet» // Ugolovnyi zakon v epokhu iskusstvennogo intellekta i tsifrovizatsii : sbornik trudov po materialam Vserossiiskoi nauchno-prakticheskoi konferentsii s mezhdunarodnym uchastiem v ramkakh I Saratovskogo mezhdunarodnogo yuridicheskogo foruma, posvyashchennogo 90-letnemu yubileyu Saratovskoi gosudarstvennoi yuridicheskoi akademii, Saratov, 09 iyunya 2021 goda. Saratov, 2021. S. 224-227.
5. Boiko S.Ya. Ugolovnaya otvetstvennost' za moshennichestvo: teoretiko-prikladnoe issledovanie. M., 2019. S. 8.

Forms and methods of preventing crimes in the field of drug trafficking

Kutsev Vladimir Valentinovich

Member of Assembly, Assembly of the Rylsky District of the Kursk Region

307370, Russia, Kursk region, Rylsk, K. Liebknecht str., 21

Avto1772@mail.ru

Abstract. The subject of this study is the forms and methods of preventing crimes in the field of drug trafficking. The purpose of the study is to analyze the forms and methods of preventing drug crimes, their differentiation, identify current problems and develop ways to solve them.
Attention is drawn to the fact that the main actors in the prevention of drug crime are the state and society. The role of the state is to coordinate and determine the vectors of combating drug crime, draw up plans and programs for preventive activities, and determine the competence of other subjects of prevention. Society also plays an important role in reducing drug crime, so it is important to involve citizens in the prevention of crimes in the field of drug trafficking. It is determined that the feedback mechanism contributes to the qualitative interaction of civil society institutions with law enforcement agencies and government agencies. The research methodology includes a number of general scientific methods of scientific cognition. The following methods were used in the course of the research: the method of analysis and synthesis, methods of deduction and induction, the method of analyzing scientific literature, the method of systematization, formal legal, dialectical and other methods. The research is structured according to the principles of logic and structuring. The scientific novelty of this study is to highlight the urgent problems of drug crime prevention as one of the methods of preventing crimes in the field of drug trafficking. Special attention is paid to improving the practice of social rehabilitation of drug addicts. This topic has been the subject of scientific research, but the main focus of many researchers is on drug treatment. At the same time, social rehabilitation and employment of drug addicts are of no less importance, as they seriously reduce the likelihood of such persons committing crimes in the field of drug trafficking. The considered method of preventing drug crimes, expressed in individual preventive work with drug addicts, will also contribute to reducing the demand for drugs, which will reduce the number of crimes in the field of illicit trafficking.
The conducted research allowed us to conclude that such a method of preventing crimes in the field of drug trafficking as individual preventive work with drug addicts, their adaptation and social rehabilitation is of high importance. Some problems in this area are considered, and possible solutions are proposed.

Keywords: drug addicts, security threat, prevention, rehabilitation, crime, warning methods, subjects of the warning, prevention of drug crimes, drug crime, law enforcement agencies

References (transliterated)

1. Aganov G. M., Kovaleva E. Preduprezhdenie prestuplenii i inykh pravonarushenii sredstvami prokurorskogo nadzora pri ispolnenii nakazaniya v vide lisheniya svobody // Ugolovnoe pravo. 2005. № 4. S. 11.
2. Voronin Yu. A., Maiorov A. V. Teoreticheskie osnovy formirovaniya sistemy protivodeistviya prestupnosti v Rossii // Kriminologicheskii zhurnal Baikal'skogo gosudarstvennogo un-ta ekonomiki i prava. 2013. № 1. S. 7-16.
3. Gogoleva A. Ya. Ponyatie profilaktiki i bor'by s prestupnost'yu // Molodoi uchenyi. 2014. № 6.1 (65.1). S. 3-7.
4. Golik S. I., Mikhailov B. P. Organizatsiya i taktika obshchei profilaktiki prestuplenii organami vnutrennikh del. M., 1980. S. 10.
5. Gotchina L. V. Molodezhnyi narkotizm v sovremennoi Rossii: kriminologicheskii analiz i profilaktika: avtoref. dis. ... dokt. yurid. nauk. SPb, 2011. – 46 c.
6. Ivanov V. A., Khlebnikova N. S. Rol' grazhdanskogo obshchestva v bor'be s nezakonnym oborotom narkotikov // Mariiskii yuridicheskii vestnik. 2017. № 1(20). S. 17.

7. Plankina N. E. Sotsial'naya reabilitatsiya lits, stradayushchikh narkoticheskoi zavisimost'yu // Vestnik Amurskogo gosudarstvennogo universiteta. Seriya: Gumanitarnye nauki. 2018. № 82. S. 111-113.
8. Sidorenko A. V., Egorshin V. M. Mery preduprezhdeniya nezakonnogo oborota narkotikov // Vestnik Sankt-Peterburgskogo universiteta MVD Rossii.2012. № 2 (54). S. 157.
9. Shalagin A. E. Prestupleniya protiv zdorov'ya naseleniya: avtoreferat dis. ... doktora yuridicheskikh nauk. Kazan', 2004. 25 s.
10. Shchedrin N. V. Osnovy obshchei teorii preduprezhdeniya prestupnosti. Krasnoyarsk, 1999. S. 562.

Differentiation of criminal liability as an element of criminal law policy in the field of fair competition protection

Danilovskaia Anna Vladimirovna

PhD in Law

Associate professor, Department of Civil Law and Civil Procedural Law, Pacific State University

680000, Russia, Khabarovsk Territory, Khabarovsk, 134 Pacific Street, office 417

d_a_v@list.ru

Abstract. The subject of the study is the issues of differentiation of criminal liability for crimes infringing on fair competition (hereinafter also anti–competitive crimes), as an element of criminal law policy in the field of protection of fair competition. In particular, the problems of identifying such a group of crimes, criteria for differentiating responsibility are studied using the example of analyzing both named and non-specified elements of crimes of certain qualifying signs of crimes, other means of differentiating responsibility for their commission, problems of building sanctions for crimes of the group in question.The purpose of the work is to assess the current state, identify problems of differentiation of criminal liability for crimes that infringe on fair competition, in the light of official recognition of the need to counter them as a threat to economic security, and identify ways to solve them. The research methodology is based on general scientific and private scientific methods of cognition – historical and legal, methods of system analysis, logical, comparative, formal dogmatic methods, the method of legal forecasting and classification, questionnaires. The novelty lies in: 1) in the study of the provisions of the Criminal Code of the Russian Federation in their relation to the Federal Law "On Protection of Competition" in order to establish criteria for the allocation of a group of anti-competitive crimes and substantiate the differentiation of responsibility for their commission; 2) in proposals on the allocation as independent elements of crimes of certain types of violations of antimonopoly legislation for which criminal liability has not been established, as well as on the inclusion in a number of articles of the Criminal Code of the Russian Federation of a sign of committing a crime for the purpose of unfair competition, as differentiating responsibility for crimes involving illegal trafficking of intellectual property in the field of entrepreneurship; 3) in the analysis of problems of means of differentiating responsibility for encroachments on fair competition and in proposals for their improvement, 4) in the proposal to keep official records of a group of anti-competitive crimes in the field of the formation of static reporting on crimes committed in the structure of crimes of economic and corruption orientation.
The conclusions are that the elimination of the problems of differentiation of criminal liability for anti-competitive crimes, as well as the official accounting of such crimes, is the key to the

effectiveness of the entire criminal law policy in the field of fair competition protection.

Keywords: anti-competitive crimes, means of differentiating responsibilities, unfair competition, cartel, differentiation of criminal liability, criminal law policy, criminal liability, bid rigging, leniency program, anti-competition agreements

References (transliterated)

1. Tagantsev N.S. Ulozhenie o nakazaniyakh ugolovnykh i ispravitel'nykh 1885 goda / Sost. N.S. Tagantsev. – 5-e izd., dop. – Sankt-Peterburg: tip. M. Stasyulevicha, 1886.
2. Korobeev A.I. Ugolovno-pravovaya politika Rossii: ot genezisa do krizisa : monografiya. – Moskva : Yurlitinform, 2019.
3. Danilovskaya A.V., Tenishev A.P.Ob ugolovnoi otvetstvennosti za sgovory na torgakh // Aktual'nye problemy rossiiskogo prava. 2019. № 1 (98). S. 119–131.
4. Danilovskaya A.V. Primenenie st. 1281 UK RF «Kleveta» v sfere zashchity dobrosovestnoi konkurentsii // Ugolovnoe pravo: strategiya razvitiya v XXI veke : materialy XVIII Mezhdunar. nauch.-prakt. konf., Moskva, 21–22 yanv. 2021 g. / Mosk. gos. yurid. un-t im. O.E. Kutafina. – Moskva : RG-Press, 2021. – S. 550–555.
5. Tenishev A.P., Velikanov A.P. Rol' assotsiatsii v antikonkurentnykh soglasheniyakh : analiz praktik antikonkurentnogo povedeniya i osobennostei ikh presecheniya // Konkurentnoe pravo. 2016. № 2. S. 33–37.
6. Ustinova T.D. Ugolovno-pravovaya okhrana svobody konkurentsii v aspekte izmenenii i dopolnenii ugolovnogo zakona // Aktual'nye problemy rossiiskogo prava. 2016. № 7 (68). S. 110–117.
7. Yani P.S. Problemy ugolovno-pravovoi okhrany ekonomiki ot nedobrosovestnoi konkurentsii // Rossiiskaya yustitsiya. 2010. № 11. S. 22–26.
8. Danilovskaya A.V. Ugolovno-pravovaya okhrany konkurentsii v ES, FRG, Velikobritanii i Frantsii // Yuridicheskie issledovaniya. 2020. № 6. S. 21–35.
9. Kobanenko M., Denchenkova O. Otvetstvennost' uchastnikov gruppy lits za zloupotreblenie dominiruyushchim polozheniem // Konkurentsiya i pravo. 2011. № 5. S. 27–31.
10. Martynova O.V.Gruppa lits kak samostoyatel'nyi sub''ekt zloupotrebleniya dominiruyushchim polozheniem // Sovremennaya konkurentsiya. 2013. № 5 (41). S. 18–23.
11. Aleshin K.N., Maksimov S.V.Dobrovol'noe soobshchenie o zaklyuchenii kartelya: nazrevshie reformy // Rossiiskoe konkurentnoe pravo i ekonomik. 2018. № 4 (16). S. 24–33.

Topical issues of countering modern autonomous unmanned aerial vehicles and FPV drones

Nikolaev Nikolay Vladimirovich

PhD in Economics

Staff Member, The Academy of the Federal Guard Service of the Russian Federation

302015, Russia, Orel region, Orel, Priborostroitelnaya str., 35

nnv85Nikolas@list.ru

Il'in Vladimir Viktorovich

PhD in Technical Science

Staff Member, The Academy of the Federal Guard Service of the Russian Federation

302015, Russia, Orel region, Orel, Priborostroitelnaya str., 35

w.ilin82@yandex.ru

Nekrasov Maksim Igorevich

PhD in Technical Science

Staff member, The Academy of the Federal Guard Service of the Russian Federation

302015, Russia, Orel region, Orel, Priborostroitelnaya str., 35

nekr-maks@yandex.ru

Abstract. The high level of development of unmanned aviation has predetermined the possibility of its use to solve a wide range of tasks. At the same time, it should be noted that achievements in this area are not always used for peaceful purposes. The results of the analysis of the practice of using unmanned aerial vehicles (UAVs) in modern military conflicts and information about terrorist acts with their use allow us to conclude that the most difficult targets resistant to various methods of influence are modern autonomous UAVs and FPV drones with explosive devices. Therefore, the search for effective ways to counteract them seems to be an urgent area of research. The aim of the work is to develop the means for effective counteraction to modern autonomous UAVs and FPV drones by electromagnetic, laser and mechanical ways. The methods of system analysis are used in the work. The article notes the increasing level of threats associated with the mass use of autonomous UAVs and FPV drones, presents the results of the "revision" and critical analysis of the main methods of countering modern UAVs, reflecting their characteristics, advantages and disadvantages. Based on the results obtained, a comparative analysis of methods of countering autonomous UAVs and FPV drones was carried out. It is concluded that the most effective of them are the methods of electromagnetic, laser and mechanical action. The required parameters for the effective application of these types of impacts on modern autonomous UAVs and FPV drones are presented.
The results of the research can be used as initial data for the creation of new and improvement of existing means of countering UAVs as part of physical protection systems (SFZ). The scientific novelty of the work consists in the development of a scientific and methodological apparatus for substantiating the SFZ of objects in terms of taking into account the functioning features and vulnerabilities of modern autonomous UAVs and FPV drones, as well as determining ways to improve systems to counter them based on the use of electromagnetic, laser and mechanical means.

Keywords: UAV, autonomous UAV, FPV drones, UAV counteraction methods, electromagnetic impact, laser impact, mechanical impact, unmanned aerial vehicle, physical protection systems, Security threats

References (transliterated)

1. Egurnov V. O., Sokolov A. M., Nekrasov M. I. Model' universal'noi upravlyayushchei platformy sistemy protivodeistviya robototekhnicheskim kompleksam // Naukoemkie tekhnologii v kosmicheskikh issledovaniyakh Zemli. 2020. T. 12. № 2. S. 79–87.
2. Egurnov V. O., Nikolaev N. V., Nekrasov M. I. K voprosu obosnovaniya oblika sistemy protivodeistviya robototekhnicheskim kompleksam na zashchishchaemykh ob''ektakh // Vooruzhenie i ekonomika. 2021. № 4(58). S. 121–134.

3. Il'in V. V., Nikolaev N. V., Nekrasov M. I., Sokolov A. M. Podkhod k otsenke effektivnosti sistem protivodeistviya robototekhnicheskim kompleksam na vazhnykh ob''ektakh // Voprosy bezopasnosti. 2023. № 4. S. 15–26.
4. Egurnov V. O., Il'in V. V., Nekrasov M. I., Sosunov V. G. Analiz sposobov protivodeistviya bespilotnym letatel'nym apparatam dlya obespecheniya bezopasnosti zashchishchaemykh ob''ektov // Voprosy oboronnoi tekhniki. Nauchno-tekhnicheskii zhurnal. Seriya 16. Tekhnicheskie sredstva protivodeistviya terrorizmu. 2018. № 115–116. S. 51–58.
5. Bespilotnye letatel'nye apparaty voennogo naznacheniya: monografiya, ch. 1 / V.A. Aladinskii, S.V. Bogdanovskii, V.M. Klimenko, V.A. Romashov. – Cherepovets: RIO VVIURE, 2019. – 613 s.
6. Rostopchin V. V. Udarnye bespilotnye letatel'nye apparaty i protivovozdushnaya oborona – problemy i perspektivy protivostoyaniya // Bespilotnaya aviatsiya [Elektronnyi resurs]. 2019. – URL: https://www.researchgate.net/publication/331772628_udarnye_bespilotnye_letatelnye_apparaty_i_protivovozdusnaa_oborona_-problemy_i_perspektivy_protivostoania (data obrashcheniya 19.09.2023).
7. Makarenko S. I. Protivodeistvie bespilotnym letatel'nym apparatam. – SPb.: Naukoemkie tekhnologii, 2020. – 204 s.
8. Tazetdinov M. N., Khakhalev A. I., Dukhnov S. V. Sredstva i sposoby protivodeistviya bespilotnym letatel'nym apparatam // Nauka YuUrGU: materialy 73-i nauchnoi konferentsii (Chelyabinsk, 20–22 aprelya 2021 g.). – Chelyabinsk: Izdatel'skii tsentr YuUrGU, 2021. – S. 624–632.
9. Semenets V. O., Trukhin M. P. Sposoby protivodeistviya bespilotnym letatel'nym apparatam // Naukoemkie tekhnologii v kosmicheskikh issledovaniyakh Zemli. – 2018. T. 10. № 3. S. 4–12.
10. Skiba V. A., Kuz'min A. A. Analiz metodov i sredstv protivodeistviya bespilotnym letatel'nym apparatam v interesakh Raketnykh voisk strategicheskogo naznacheniya // Voennaya mysl'. 2021. № 11. S. 104–114.
11. Teodorovich N. N., Stroganova S. M., Abramov P. S. Sposoby obnaruzheniya i bor'by s malogabaritnymi bespilotnymi letatel'nymi apparatami // Internet zhurnal «Naukovedenie». 2017. T. 9. № 1. S. 1–7.
12. Galkin D. V., Stepanov A. V. Bor'ba s bespilotnymi letatel'nymi apparatami: metody i sredstva inostrannykh armii // Voennaya mysl'. 2021. № 6. S. 142–151.
13. Sposoby protivodeistviya bespilotnym letatel'nym apparatam. Chast' 1 // Sait Sky X [Elektronnyi resurs]. 05.09.2023. – URL: https://sky-x.pro/blog/sposoby-protivodeystviya-bespilotnym-letatelnym-apparatam (data obrashcheniya: 15.09.2023).
14. Informatsionno-tekhnicheskoe vozdeistvie na BPLA. Chast' 2 // Sait Sky X [Elektronnyi resurs]. 05.09.2023. – URL: https://sky-x.pro/blog/informatsionno-tehnicheskoe-vozdeystvie-na-bpla (data obrashcheniya: 15.09.2023).
15. Mekhanicheskoe, lazernoe i mikrovolnovoe protivodeistvie BPLA kommercheskogo tipa. Chast' 4 // Sait Sky X [Elektronnyi resurs]. 05.09.2023. – URL: https://sky-x.pro/blog/mehanicheskoe--lazernoe-i-mikrovolnovoe-protivodeys-tvie-bpla-kommercheskogo-tipa (data obrashcheniya: 15.09.2023).
16. Sakharov K. Yu., Sukhov A. V., Ugolev V. L., Gurevich Yu. M. Study of UWB Electromagnetic Pulse Impact on Commercial Unmanned Aerial Vehicle // Proceedings of the 2018 International Symposium on Electromagnetic Compatibility (EMC Europe 2018), Amsterdam, The Netherlands, August 27–30, 2018.

The Role of Cognitive-Information Technologies in Cybersecurity: Threat Detection and Adaptive Defense Systems

Camara Amadou Sara

Graduate student, Department of Applied Mathematics and Computer Science, Peoples' Friendship University of Russia

117198, Russia, Moscow region, Moscow, Miklukho-Maklaya str., 21, sq. 803A

leosarah109@gmail.com

Abstract. The research delves into the influence of machine learning and artificial intelligence advancements on cybersecurity within software-oriented systems. The author thoroughly examines the modeling of cognitive-information technologies and their ramifications on data analysis, training processes, and decision-making within these systems. Special emphasis is placed on identifying cybersecurity threats faced by artificial intelligence systems, such as susceptibility to cyberattacks. The study proposes adaptive defense components, including behavioral biometrics analysis, automated incident response, user and entity behavior analytics (UEBA), and vulnerability management, to address these threats. These components are underscored in the development of cybersecurity strategies in the contemporary digital environment, crucial for protecting sensitive data and infrastructure.

Methodologically, the research involves analyzing existing cybersecurity threats and their impact on artificial intelligence systems, employing data analytics and modeling techniques tailored to information technologies. It also evaluates contemporary methods of adaptive cybersecurity.

Key findings of the study not only identify cybersecurity threats to artificial intelligence systems but also propose adaptive defense components for effective mitigation. The research innovatively examines the influence of cognitive information technologies on cybersecurity strategies, offering novel approaches to safeguard data and infrastructure in the modern digital landscape. Additionally, the study highlights examples such as Natural Language Processing (NLP), image and video recognition, predictive analytics, and virtual assistants, which are integral to understanding the breadth of applications of artificial intelligence in cybersecurity. The author significantly contributes through a systematic analysis of diverse threats, culminating in comprehensive recommendations for cybersecurity. Furthermore, the study identifies future prospects for cybersecurity amidst evolving cyber threats, paving the way for further research and development in the field and enhancing understanding and ensuring security in the digital realm.

Keywords: Computer Security, Vulnerabilities, Machine Learning, Artificial Intelligence, Adaptive Defense Systems, Threat Detection, Cybersecurity, Cognitive-Information Technologies, Threat Analysis, Behavioral Biometrics

References (transliterated)

1. Rizvi, V. (2023). Usilenie kiberbezopasnosti: sila iskusstvennogo intellekta v obnaruzhenii i predotvrashchenii ugroz. Mezhdunarodnyi zhurnal peredovykh issledovanii v inzhenerii i nauke (IJAERS), 10(5), mai 2023. https://dx.doi.org/10.22161/ijaers.105.8
2. Tszyan, I., i Atif I. (2021). Selektivnaya ansamblevaya model' dlya kognitivnogo analiza kiberbezopasnosti. Zhurnal komp'yuternykh i setevykh prilozhenii, 193, noyabr' 2021, 103210. https://doi.org/10.1016/j.jnca.2021.103210

3. Chen, S., Si, Kh., i Tao, S. (2022). Videnie, status i issledovatel'skie temy obrabotki estestvennogo yazyka. Zhurnal obrabotki estestvennogo yazyka, 1, 2022, 100001. https://doi.org/10.1016/j.nlp.2022.100001
4. Ding, I., i Lyu, I. (2022). Novyi metod raspoznavaniya deistvii s nebol'shim chislom obuchayushchikh primerov: vremennye relyatsionnye kross-transformery na osnove piramidy razlichii izobrazhenii. IEEE Access, 10, 94536 – 94544. 10.1109/ACCESS.2022.3204404
5. Ke, Kh., Luo, F., i Shi, M. (2023). Proektirovanie modeli raspoznavaniya emotsii rechi. Trudy po inzhenerii, 38(1), 86. https://doi.org/10.3390/engproc2023038086
6. Egvim, S. N., Alaka, Kh., Toriola-Koker, L. O., Balogun, Kh., i Sunmola, F. (2021). Primenenie iskusstvennogo intellekta dlya prognozirovaniya zaderzhek v stroitel'nykh proektakh. Mashinnoe obuchenie s prilozheniyami, 6, 15 dekabrya 2021, 100166. https://doi.org/10.1016/j.mlwa.2021.100166
7. Islek, I., i Oguduchu, S. G. (2022). Ierarkhicheskaya sistema rekomendatsii dlya elektronnoi kommertsii s ispol'zovaniem onlain-otzyvov pol'zovatelei. Issledovaniya i prilozheniya v oblasti elektronnoi kommertsii, 52, mart–aprel' 2022, 101131. https://doi.org/10.1016/j.elerap.2022.101131
8. Khabuza, T., Navaz, A. N., Khashim, F., Al'nadzhar, F., Zaki, N., Serkhani, M. A., i Statsenko, I. (2021). Primenenie iskusstvennogo intellekta v robototekhnike, analize diagnosticheskikh izobrazhenii i meditsine tochnosti: tekushchie ogranicheniya, budushchie tendentsii, rekomendatsii po sistemam komp'yuternoi pomoshchi v meditsine. Informatika v meditsine (Informatics in Medicine Unlocked), 24, 2021, 100596. https://doi.org/10.1016/j.imu.2021.100596
9. Gkinko, L., i El'banna, A. (2023). Appropriatsiya razgovornogo iskusstvennogo intellekta na rabochem meste: taksonomiya pol'zovatelei chat-botov s iskusstvennym intellektom. Mezhdunarodnyi zhurnal upravleniya informatsiei, 69, aprel' 2023, 102568. https://doi.org/10.1016/j.ijinfomgt.2022.102568
10. Bon, Dzh. (2017). Kognitivnyi khak: novoe pole bitvy v kiberbezopasnosti ... Chelovecheskii razum. Izdatel'stvo Auerbach. S. 156-160.
11. Chio, C., & Freeman, D. (2018). Mashinnoe obuchenie i bezopasnost': Zashchita sistem s ispol'zovaniem dannykh i algoritmov (1-e izdanie). O'Reilly Media. S. 25-45.
12. Akhmad, R., Alsmadi, I., Al'khamdani, V., & Taval'bekh, L. (2023). Obnaruzhenie atak nulevogo dnya: sistematicheskii obzor literatury. Obzor iskusstvennogo intellekta. https://doi.org/10.1007/s10462-023-10437-z
13. Kandkhro, I. A., Alanazi, S. M., Ali, F., Kekhar, A., Fatima, K., Uddin, M., & Karuppaia, S. (2023). Obnaruzhenie v real'nom vremeni zlonamerennykh vtorzhenii i atak v kiberbezopasnykh infrastrukturakh, osnashchennykh internetom veshchei. IEEE Access, 11, str. 9136-9148. 10.1109/ACCESS.2023.3238664
14. Einsli, S., Tompson, D., Meinard, S., & Akhmad, A. (2023). Kiber-razvedka: obzor i issledovatel'skaya programma dlya praktiki prinyatiya reshenii v oblasti bezopasnosti. Komp'yutery i bezopasnost', 132, 103352. https://doi.org/10.1016/j.cose.2023.103352
15. D'yuis, M., & Viana, T. (2022). Phish Responder: gibridnyi metod mashinnogo obucheniya dlya obnaruzheniya fishinga i spam-pisem. Prikladnye sistemnye innovatsii, 5(4), 73. https://doi.org/10.3390/asi5040073
16. Khuan'es-Martino, F., Alaiz-Rodriges, R., Gonsales-Kastro, V., Fidalgo, E., & Alegre, E. (2023). Obzor obnaruzheniya spama v elektronnoi pochte: analiz strategii spamerov i problemy sdviga nabora dannykh. Obzor iskusstvennogo intellekta, 56, 1145–1173. https://doi.org/10.1007/s10462-022-10195-4

17. Mugkhaid, A., Al'Zu'bi, S., Khnaif, A., Taamne, S., Al'nadzhar, A., & Abu Elsoud, E. (2022). Intellektual'naya sistema obnaruzheniya fishinga v kiberbezopasnosti s ispol'zovaniem tekhnik glubokogo obucheniya. Klasternye vychisleniya, 25, 3819–3828. https://doi.org/10.1007/s10586-022-03604-4
18. Neupane, K., Khaddad, R., & Chen, L. (2018). Brandmauer sleduyushchego pokoleniya dlya setevoi bezopasnosti: obzor. Doklad predstavlen na SoutheastCon 2018, Sankt-Peterburg, Florida, SShA, str. 1-6. IEEE. 10.1109/SECON.2018.8478973.
19. Kim, Dzh., & Sim, A. (2019). Novyi podkhod k mul'tivariativnomu analizu setevogo trafika. Zhurnal po komp'yuternym naukam i tekhnologiyam, 34, 388–402. https://doi.org/10.1007/s11390-019-1915-y
20. Abbasi, M., Shakhraki, A., & Takherkordi, A. (2021). Glubokoe obuchenie dlya monitoringa i analiza setevogo trafika (NTMA): obzor. Komp'yuternye kommunikatsii, 170, 19-41. https://doi.org/10.1016/j.comcom.2021.01.021
21. Alotaibi, A., & Rassam, M. A. (2023). Ataki na obuchenie sopernichestvom mashinnogo obucheniya na sistemy obnaruzheniya vtorzhenii: obzor strategii i zashchity. Budushchii internet, 15, 62. https://doi.org/10.3390/fi15020062
22. Baig, A. F., Eskeland, S., & Yang, B. (2023). Sokhranenie konfidentsial'nosti nepreryvnoi autentifikatsii s ispol'zovaniem povedencheskoi biometrii. Mezhdunarodnyi zhurnal informatsionnoi bezopasnosti, 1-10. https://doi.org/10.1007/s10207-023-00721-y
23. Traore, I., Voungang, I., Obaidat, M. S., Nakkabi, I., & Lai, I. (2014). Onlain autentifikatsiya na osnove riskov s ispol'zovaniem povedencheskoi biometrii. Mul'timediinye instrumenty i prilozheniya, 71, 575–605. https://doi.org/10.1007/s11042-013-1518-5
24. Shalini P., & Shankaraiya. (2022). Sotsial'nyi povedencheskii biometricheskii mul'timodal'nyi soyuz dlya predotvrashcheniya sozdaniya poddel'nykh akkauntov v Facebook. Mul'timediinye instrumenty i prilozheniya, 81, 39715–39751. https://doi.org/10.1007/s11042-022-13104-7
25. Ban, T., Takakhashi, T., Ndichu, S., & Inoue, D. (2023). Preodolenie ustalosti ot trevogi: II-pomoshchnik v ramkakh sistemy monitoringa informatsionnoi bezopasnosti dlya effektivnogo reagirovaniya na intsidenty. Prikladnye nauki, 13, 6610. https://doi.org/10.3390/app13116610
26. Rengaradzhan, R., & Shekar Babu. (2021). Obnaruzhenie anomalii s ispol'zovaniem analitiki povedeniya sub''ektov i vizualizatsii dannykh. VIII Mezhdunarodnaya konferentsiya IEEE po vychislitel'noi tekhnike dlya ustoichivogo global'nogo razvitiya (INDIACom), N'yu-Deli, Indiya, str. 842-847. https://ieeexplore.ieee.org/document/9441226
27. Malik, A. A., & Tosh, D. K. (2023). Dinamicheskaya klassifikatsiya uyazvimostei dlya uluchshennogo kibersituatsionnogo osvedomlennosti. Konferentsiya IEEE po sistemam (SysCon), Vankuver, Britanskaya Kolumbiya, Kanada, 2023, str. 1-8. 10.1109/SysCon53073.2023.10131235.
28. Andrade, R., Torres, Zh., & Tello-Okendo, L. (2018). Zadachi kognitivnoi bezopasnosti s ispol'zovaniem instrumentov Big Data. Mezhdunarodnaya konferentsiya po vychislitel'nym naukam i vychislitel'nomu intellektu (CSCI), Las-Vegas, Nevada, SShA, str. 100-105. 10.1109/CSCI46756.2018.00026.
29. Lorents, B., & Kikkas, K. (2020). Pedagogicheskie vyzovy i eticheskie soobrazheniya pri razvitii kriticheskogo myshleniya v kiberbezopasnosti. 20-ya mezhdunarodnaya konferentsiya po peredovym tekhnologiyam obucheniya (ICALT) IEEE, Tartu, Estoniya,

2020, str. 262-263. 10.1109/ICALT49669.2020.00085.

30. Bem, Dzh., Dias, D., L'yuis, K., Li, K., & Uollens, D. (2022). Tendentsii kiberbezopasnosti: vzglyad v budushchee. McKinsey & Company. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizo

Analysis of software products and the study of automation of processes in the field of monitoring purchases and goods.

Perelygin Ivan

Student, Department of Industrial Programming, MIREA - Russian Technological University

78 Prospekt Vernadskogo str., Moscow, 119454, Russia, Moscow region

iv_perelygin@mail.ru

Abstract. The subject of this report is a comparative analysis of software products and a study of business processes in the field of optimization of purchases and monitoring of goods. Within the framework of this study, the following tasks were set: the study of existing software solutions for optimizing procurement processes, the analysis of their functionality and effectiveness, as well as the study of business processes of companies in the field of monitoring goods. As a result of this research, an analysis of various software products was carried out, their advantages and disadvantages were identified, as well as current business processes were analyzed and opportunities and potential for optimization were identified. The obtained results and conclusions can be used to develop recommendations for improving procurement processes and monitoring of goods in organizations. In this study, a comparative analysis of software solutions for automating procurement processes is carried out. The research methodology included an analysis of the functionality, effectiveness and cost of the programs, as well as the study of user feedback and industry experts. The results made it possible to identify the main advantages and disadvantages of each software considered. The study of the main characteristics and functionality of procurement management systems represents a significant contribution to the field of information technology and business process management. An analysis of the comparative characteristics of ERM systems, their integration capabilities and compliance with business needs allows us to identify key factors for successful automation of procurement processes. This study not only expands scientific understanding in the field of procurement automation, but also provides practical recommendations for choosing the optimal procurement management system.
The conclusions of the work emphasize the importance of customizing the software to the unique needs of the organization in order to achieve optimal efficiency and effectiveness in procurement management. The comparison table of the disadvantages of ERM systems presented in the final part by key parameters allows you to highlight the main advantages and disadvantages of each software product, which is an important step in choosing the most appropriate solution for a particular business.
Thus, this study not only contributes to the development of scientific knowledge in the field of procurement management, but also provides valuable practical recommendations for the business community, helping to increase the efficiency and effectiveness of procurement processes in a modern business environment.

Keywords: flexibility, adaptation, modularity, ERM-system, optimization, integration, business-process, monitoring, procurements, automatization

References (transliterated)

1. Comindware procurement management (tadviser.com). URL: https://tadviser.com/index.php/Product:Comindware_Procurement_Management#:~:text=Comindware%20Procurement%20Management%20was%20developed,to%20the%20specified%20business%20logic (data obrashcheniya: 20.10.2023).
2. Procurement management software market outlook 2022 to 2031 – Supply chain council of European Union | scceu.org. URL: https://scceu.org/procurement-management-software-market-outlook-2022-to-2031/ (data obrashcheniya: 21.10.2023).
3. Procurement contract approval process – BPI – The destination for everything processes related (businessprocessincubator.com). URL: https://www.businessprocessincubator.com/content/procurement-contract-approval-process/ (data obrashcheniya: 21.10.2023).
4. Avtomatizatsiya biznes-protsessa soglasovaniya dogovorov – Comindware. URL: https://www.comindware.ru/usecases/document-approval-business-process/ (data obrashcheniya: 22.10.2023).
5. Agora.ru – B2C i B2B E-commerce platforma dlya tsifrovizatsii biznesa. URL: https://www.agora.ru/?ysclid=lovz0vvkq9695817461 (data obrashcheniya: 22.10.2023).
6. Construction ERP Software | AGORA | Simpro business solutions. URL: https://simpro.co.in/construction-erp-software-agora/ (data obrashcheniya: 23.10.2023).
7. AGORA: Razrabotka onlain-reshenii dlya avtomatizatsii zakupochnoi deyatel'nosti (ocs.ru). URL: https://www.ocs.ru/agora-razrabotka-onlajn-reshenij-dlya-avtomatizaczii-zakupochnoj-deyatelnosti/?ysclid=lovzgbwbo9129914734 (data obrashcheniya: 23.10.2023).
8. Naumen SRM/GPMS | avtomatizatsiya zakupochnoi deyatel'nosti. URL: https://naumensrm.ru/srm-sistema/?ysclid=lovzzfaa303290434 (data obrashcheniya: 23.10.2023).
9. Naumen SRM/GPMS | avtomatizatsiya zakupochnoi deyatel'nosti. URL: https://softfinder.ru/service/naumen-srmgpms?ysclid=lsqp6djt7d226861212 (data obrashcheniya: 23.10.2023).
10. Naumen SRM/GPMS – sistema avtomatizatsii zakupochnoi deyatel'nosti (softfinder.ru). URL: https://tadviser.com/index.php/Product:Naumen_GPMS_%E2%80%93_Purchase_management?ysclid=low06isokp673800220 (data obrashcheniya: 23.10.2023).
11. Norbit: effektivnye zakupki (norbit.ru). URL: https://products.norbit.ru/effektivnye-zakupki/?ysclid=low1n3id4f104510856 (data obrashcheniya: 23.10.2023).
12. Norbit business trade (NBT) (tadviser.com). URL: https://tadviser.com/index.php/Product:Norbit_Business_Trade_(NBT)?ysclid=low1nagqio924137887 (data obrashcheniya: 23.10.2023).
13. Norbit SRM: effektivnaya tsifrovizatsiya zakupok (norbit-srm.com). URL: https://norbit-srm.com/news-and-events/norbit-srm-effektivnaya-tsifrovizatsiya-zakupok/?ysclid=low1nfc75t624810865 (data obrashcheniya: 23.10.2023).
14. Sistema upravleniya zakupkami ITender SRM: planirovanie, kontrol' - ai tender fogsoft (fogsoft.ru). URL: https://fogsoft.ru/solutions/itender-srm/?ysclid=low0rjouqt552056949 (data obrashcheniya: 23.10.2023).
15. Razrabotka kompanii Fogsoft – ITender SRM (itender-online.ru). URL: https://itender-

online.ru/solutions/itender-srm/?ysclid=low0nkld1j406386270 (data obrashcheniya: 23.10.2023).

16. ITender development – polnotsennaya SRM dlya zastroishchikov (bizneslab.com). URL: https://bizneslab.com/itender-development/?ysclid=low0nwc8r523448463 (data obrashcheniya: 23.10.2023).

Current aspects and problematic issues of the use of a polygraph in public service in modern conditions

Sadekov Rustem Rafekovich

PhD in Pedagogy

Deputy Head of the Department of Psychological-Pedagogical and Medical Support of the Department of Internal Affairs Activities at the Russian Institute of Officials Training and Education

142007, Russia, Moscow Region, Domodedovo, Fir street, 3

vipk10kafedra@yandex.ru

Abstract. In the work, the author examines problematic issues related to the study of the peculiarities of the organization and legal regulation of the use of a polygraph in public service. The article deals with various aspects of the use of a polygraph in the public sphere, including legal aspects, psychological and pedagogical features, physiological and ethical issues, as well as the protection of citizens' rights. In addition, it examines the experience of using a polygraph in various conditions when the procedure for obtaining, identifying, processing, storing and reliability of data is carried out, and as a result, it becomes necessary for competent public sector specialists to constantly pay special attention to the safety of storing and using confidential information received. In order to analyze the effectiveness of the use of a polygraph, the paper describes the tasks facing specialists, considers algorithms and techniques used to assess the reliability of the information received. The following methods were used in the preparation of the article : an analysis of literature, a system approach, comparative analysis and synthesis, induction and deduction, logical thinking techniques, classification. The main conclusions of the research conducted by the author are organizational aspects aimed at respecting the rights and freedoms of citizens who, for one reason or another, will have to undergo the testing procedure on a polygraph device. A prerequisite is the fact that the legal regulation of the use of a polygraph in the civil service requires clear formulation, transparency and objectivity of procedures, timely clarification of the upcoming nuances of the polygraph examination, related possible restrictions, but at the same time compliance with guarantees for employees who are being tested. This topic, in its content and meaning, is relevant, and therefore, today, the development of legal and methodological mechanisms for the use of a polygraph in the public sphere, based on scientific developments by leading scientists and practitioners in this field of knowledge, is in demand.

Keywords: provision, citizen, right, psychology, quality, legislation, feature, specialist, system, polygraph

References (transliterated)

1. Golovin A. Yu., Bugaevskaya N. V. Osobennosti rassledovaniya korruptsionnykh prestuplenii // Izvestiya TulGU. Ekonomicheskie i yuridicheskie nauki. 2012. №1-2.
2. Krasinskaya, E. S. Nekotorye aspekty ispol'zovaniya poligrafa pri raskrytii i

rassledovanii prestuplenii // Politseiskaya deyatel'nost'. – 2021. – № 3. – S. 13-23. – DOI 10.7256/2454-0692.2021.3.35751. – EDN DQVCHS.

3. Istomina, I. F. Ispol'zovanie poligrafa pri rassledovanii i raskrytii prestuplenii // Baikal'skii studencheskii yuridicheskii forum-2022. Sovremennye problemy pravotvorchestva i pravoprimeneniya : Materialy Vserossiiskoi studencheskoi nauchno-prakticheskoi konferentsii, Irkutsk, 24 marta 2022 goda / Otv. redaktory A.M. Bychkova, N.V Keshikova. Tom 2. – Irkutsk: Irkutskii institut (filial) VGUYu (RPA Minyusta Rossii), 2022. – S. 180-185. – EDN JNSLUY.
4. Kozyrev, V. D. Videozapis'. Zakonnoe i nezakonnoe ispol'zovanie: spornye voprosy i ikh resheniya // E-Scio. – 2021. – № 2(53). – S. 327-339. – EDN XNRPXM.
5. Petrov, K. S. Razvitie instituta zashchity gosudarstvennoi tainy v Rossii v sovetskii i postsovetskii periody // Operativnik (syshchik). – 2016. – № 4(49). – S. 4-8. – EDN XDNFRX.
6. Neimysheva, M. D. Primenenie poligrafa v operativno-rozysknoi deyatel'nosti // Problemy gosudarstva i prava v issledovaniyakh studentov : Sbornik materialov XVIII Mezhvuzovskoi nauchno-prakticheskoi konferentsii, Moskva-Tyumen', 14 aprelya 2023 goda. – Moskva-Tyumen': Avtonomnaya nekommercheskaya organizatsiya vysshego obrazovaniya "Institut delovoi kar'ery", 2023. – S. 212-214. – EDN QAPDLH.
7. Sadekov R.R. Formirovanie pravovoi kul'tury spetsialista-poligrafologa v protsesse professional'nogo obucheniya // Politseiskaya deyatel'nost'. – 2023. – № 2. – S. 48-55. DOI: 10.7256/2454-0692.2023.2.39764 EDN: VEEWKW URL: https://nbpublish.com/library_read_article.php?id=39764
8. Mironov V. I. Trudovoe pravo: uchebnik dlya VUZov. – SPb.: Piter, 2009. 864 s.
9. Prizhennikova, A. N. Realizatsiya garantii prav rabotnika po rossiiskomu trudovomu zakonodatel'stvu // Colloquium-Journal. – 2019. – № 9-10(33). – S. 50-58. – EDN NAKQJG.
10. Abramova, A. V. Problema zashchity konfidentsial'nosti lichnykh dannykh uchastnikov ugolovnogo sudoproizvodstva v usloviyakh vnedreniya elektronnogo pravosudiya // Alleya nauki. – 2019. – T. 4, № 1(28). – S. 650-653. – EDN ZAALCX.
11. Sadekov R.R., Krokhina Yu.V. Organizatsionno-pravovye aspekty organizatsii professional'noi podgotovki sotrudnikov MVD Rossii v sisteme dopolnitel'nogo professional'nogo obrazovaniya // Voprosy bezopasnosti. – 2023. – № 1. – S. 58-65. DOI: 10.25136/2409-7543.2023.1.39710 EDN: LOQZMF URL: https://nbpublish.com/library_read_article.php?id=3971
12. Kudryavtsev D. S. "Opyt i perspektivy ispol'zovaniya poligrafa kak metoda preodoleniya protivodeistviya raskrytiyu i rassledovaniyu prestuplenii v Respublike Belarus'" Izvestiya Tul'skogo gosudarstvennogo universiteta. Ekonomicheskie i yuridicheskie nauki, №4-2, 2017. S. 152-159.