ПРИМЕНЕНИЕ МЕТОДОВ НЕЧЕТКОЙ ЛОГИКИ И РЕГРЕССИОННОГО АНАЛИЗА ДЛЯ ОПРЕДЕЛЕНИЯ РИСКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Козлов А.Д., Нога Н.Л.
Институт проблем управления им. В.А. Трапезникова РАН, Москва, Россия
alkozlov@ipu.ru, noga@ipu.ru

Аннотация. Приведен обзор публикаций, посвященных оценке рисков информационной безопасности в различных системах. Авторы предлагают для оценки риска информационной безопасности совместно использовать методы нечеткой логики и регрессионного анализа, которые позволяют решать задачу оценки риска в условиях неопределенности.

Ключевые слова: информационная безопасность, многофакторная оценка рисков, нечеткая логика, регрессионный анализ, продукционные правила, уравнение регрессии, условия неопределенности.

Введение

В современном мире по мере повсеместного развития цифровых технологий в условиях глобальной цифровизации экономики крайне усложнилась работа как по противодействию инцидентам, связанным с хакерскими кибератаками, так и по вычислению прогнозов по рискам информационной безопасности различных предприятий и учреждений, в том числе критической инфраструктуры. Особенно это касается последних нескольких лет, когда глобальная пандемия вынудила многих перейти на удаленный режим работы, а также в связи с беспрецедентными санкциями, введенными против России после начала специальной военной операции. В сжатые сроки, в условиях непрекращающихся атак на российские информационные ресурсы приходится решать задачи по переходу на отечественное программно-техническое обеспечение.

С этими проблемами сталкиваются компании и организации самого разного уровня от больших корпораций и вплоть до малого бизнеса. В современной напряженной международной обстановке значительно возросла активность хакеров. В ряде стран количество утечек за первую половину 2023 года в сравнении с 2022 годом выросло почти в 2,5 раза. Число персональных данных (ПДн), которые были скомпрометированы в Российской Федерации, возросло на 60% относительно 2022 года. Всего в России за год в виде утечек похищено более миллиарда записей ПДн [1].

Необходимо отметить, что кибератаки все чаще имеют политическую и экономическую направленность. Если раньше атаки на информационные ресурсы происходили в основном с целью хищения персональных данных, финансовой и коммерческой информации, то сейчас происходит усиление попыток нанести как можно больший вред различным системам, включая объекты критической информационной инфраструктуры, вплоть до их полного вывода из строя.

Защищая информационные ресурсы и инфраструктуру, мы в первую очередь защищаем бизнес, обеспечиваем работоспособность бизнес-процессов. Для построения эффективной защиты необходимо оценивать, как существующие в настоящее время риски, так и, по возможности, те риски, которые могут возникнуть в будущем. Риск – это влияние неопределенностей на достижение поставленных целей [2]. Из этого следует, что оценка риска всегда связана с неопределенностями.

Факторов риска может быть множество, и они могут быть как типовыми для определенного класса систем, так и специфическими, присущими только конкретной системе. Также влияние различных факторов может меняться со временем. Из этого следует, что оценка риска должна проводиться систематически, итеративно, основываться на актуальной информации. Также следует учитывать, что процесс оценки риска охватывает идентификацию риска, анализ риска и сравнительную его оценку [2].

Для обеспечения вышесказанного методика, используемая для оценки уровня риска, должна быть относительно простой и позволять работать с множеством неопределенностей.

В настоящей работе авторы предлагают для оценки риска информационной безопасности совместно использовать методы нечеткой логики и эконометрики, которые позволяют решать задачу оценки риска в условиях неопределенности зависимости различных параметров в сложных информационных структурах. Также это позволяет установить параметры, от которых в большей степени зависит риск информационной безопасности, и перечень параметров, которыми можно пренебречь в оцениваемой ситуации. Это позволяет планировать мероприятия по совершенствованию системы защиты информационных ресурсов, как в краткосрочной, так и в долгосрочной перспективе.

1. Краткий обзор публикаций

В связи с изменением направленности угроз организациям требуются все более продвинутые решения для определения рисков информационной безопасности в эксплуатируемых системах. Эти решения диктуют создание методик, которые используют процедуры оценки, анализа и управления рисками информационной безопасности, например, уже устоявшихся, но все еще актуальных: CORAS и OCTAVE, CRAMM и ГРИФ, RiskWatch и методология от Microsoft [3-4]. Идентификации угроз безопасности посвящен также ряд работ, например, работа [5]. Оценка рисков безопасности в облачных вычислениях рассматривается в работах [6-8]. Во всех этих работах, чтобы оценить риск, необходимо провести оценку угроз и уязвимостей, через которые осуществляются угрозы, а также подсчитать ущерб от реализации этих угроз. Чтобы провести анализ рисков и реализовать процедуру управления рисками, необходимо построить модели, демонстрирующие появление как благоприятных, так и неблагоприятных условий, учитывая многочисленные характеристики, свойственные этим рискам. Кроме того, такие модели помогают решать задачу уменьшения возможного ущерба в результате проведения атак на ресурсы организаций или осуществления угроз через как выявленные, так и не выявленные уязвимости. Также эти модели помогают решать задачу по планированию дополнительных мер для улучшения защищенности информационных объектов и, соответственно, уменьшения наносимого ущерба при реализации угроз через уязвимости.

Если есть возможность количественно оценить параметры, от которых зависит риск, то указанные методики дают неплохой результат при оценивании риска. Если же оценивание проводится в условиях высокой неопределенности, например, при зависимости риска от субъективных факторов [9], то могут быть достаточно высокие погрешности. Методы же, основанные на использовании нечеткой логики [10], позволяют решать задачу оценки риска в условиях неопределенности корреляции различных факторов.

Для оценки риска в условиях неопределенности взаимосвязи таких параметров как уровень угроз, наносимый ущерб и т.п., а также, частичная утрата контроля за собственными информационными ресурсами при использовании облачных структур, была предложена в работе [11]. В [12] большое внимание уделено разработке методологии оценки и анализа рисков и уязвимостей в контексте управления рисками безопасности с помощью рассмотрения модели оценки рисков на основе нечеткой логики. Метод оценки рисков, основанный на мультинечетких системах был предложен в работе [13]. При этом для оценки киберугроз было предложено оценивать риск как функцию следующих параметров: общие возможности злоумышленника, вероятность успеха атаки и последствия атаки. В работах [14-15] были предложены методики по решению задачи обнаружения критических узлов в информационных системах, используя методы нечеткой логики для оценки рисков в условиях неопределенности. В работе [16] переход к количественному представлению качественных характеристик был обеспечен использованием нечеткой модели при обработке неточных факторов рисков информационной безопасности. Предложенные здесь нечеткая модель и методы могут быть использованы для оценки как конкретных видов рисков информационной безопасности ERP-системы, так и общего риска информационной безопасности ERP-системы. При этом для осуществления методик, описанных в работах [11,16] можно воспользоваться системой Matlab [17], с реализацией которой можно ознакомиться в работе [18].

2. Материалы и применяемые методы

В данном докладе предлагается к рассмотрению методика, основанная на методах нечеткой логики и эконометрики в разделе регрессионного анализа. Использование данной методики позволяет определить множество факторов, от которых в большей степени зависит риск информационной безопасности, и перечень параметров, которыми можно пренебречь в оцениваемой ситуации.

Ясно, что увеличение числа рассматриваемых факторов и интервалов, принимаемых ими значений, может значительно усложнить формирование продукционных правил. При данной методике задача управления безопасностью информационной системы решается с максимально большим числом факторов, а также при наличии разного количества интервалов значений для каждого фактора.

По данной методике в самом общем виде уровень риска можно представить в виде некоторой функции n факторов.

$$R = R(P_1, P_2, ..., P_n), \quad (1)$$

где $P_i, i = 1,...,n,$ – факторы, от которых зависит уровень риска.

Полагается, что количественные значения всех этих факторов изменяются в промежутке от 0 до 1, а качественные принимают значения, например, незначительный, критический и т.п.

Требуется найти объясняющие лингвистические переменные, наибольшим образом влияющие на значение выходной переменной *R*, и далее построить уравнение множественной регрессии. При этом, предлагается не учитывать в дальнейшем переменные, слабо влияющие на уровень риска. Границы термов задаются экспертным путем.

Чтобы определить уровень риска, авторы предлагают воспользоваться методами нечеткой логики [11,15,19]. При этом можно реализовать многофакторную оценку уровня риска. Необходимо отметить, что влияние рассматриваемых факторов может оказаться достаточно неопределенным из-за их возможной корреляции, соответственно. их возможной избыточности. Здесь необходимо отметить, что точность оценки зависит от качества формирования как продукционных правил, так и от подробного описания термов каждой лингвистической переменной.

Используя метод наименьших квадратов (МНК), вычисляем коэффициенты уравнения множественной регрессии. Для сравнения коэффициентов уравнения [20] и выстраивания параметров по степени влияния на риск, необходимо построить уравнение регрессии в стандартизованном масштабе. Таким образом можно выстроить полученные коэффициенты по степени влияния на риск и, определив избыточные параметры, т.е. параметры, слабо влияющие на риск, исключить эти параметры из уравнения.

Схема решения предусматривает выполнение задачи за несколько шагов.

Шаг 1. Проведение обследования объекта информатизации

По результатам проведенного обследования объекта информатизации определяется множество из *n* факторов (параметров), от которых зависит информационная безопасность данного объекта (эксплуатируемой информационной системы). Применительно к информационным системам факторы риска можно разбить на четыре основных вида, в которые входят:

- Экономические параметры: ценность актива (информационного ресурса), уровень зависимости основного производства от информационной инфраструктуры, уровень затрат на информационную составляющую в целом и средства обеспечения кибербезопасности в частности, уровень потенциального ущерба и другие.
- Технические параметры, к которым относятся: уровень уязвимостей в аппаратно-программном комплексе эксплуатируемой системы; уровень технологической независимости от импортных разработок (отношение количества программно-аппаратных средств, разработанных и произведенных в России, к общему числу используемых средств на объекте информатизации), уровень технической защиты информации и другие.
- Организационные параметры: уровень изолированности объекта от внешних систем, уровень использования привлеченных специалистов, уровень организации защиты информационной системы (наличие и исполнение инструкций и регламентов, наличие средств контроля доступа, наличие администраторов безопасности, наличие подрядных организаций) и другие.
- Субъективные параметры: уровень квалификации сотрудников и администраторов, уровень зарплаты сотрудников, уровень «текучести» кадров и другие [9].

По результатам обследования объекта информатизации могут быть установлены и другие факторы риска. Совокупность таких факторов будет представлять результат идентификации рисков.

Шаг 2. Создание нечеткой базы знаний

Из множества полученных на первом шаге *n* параметров выбирается *m* параметров (от пяти до восьми), представляющих все четыре приведенные выше группы, от которых, по мнению экспертов, в большей степени зависит информационная безопасность объекта. Если принять в рассмотрение все *n* параметров, то таблица продукционных правил может принять неприемлемо большой размер, обрабатывать который будет достаточно сложно. Выбранные параметры (лингвистические переменные) нормируются, чтобы их значения находились в границах от 0 до 1.

Все входные лингвистические переменные P_i оцениваются каждая по своей шкале, как на качественном уровне («незначительный», «критический» и т.п.), так и в количественном виде в границах от 0 до 1. Границы термов, как указывалось выше, задаются экспертным путем. Аналогично для уровня риска *R* присваиваются качественные значения «низкий», «допустимый» и т.п. Затем формируется таблица продукционных правил, каждая строка которой представляет собой комбинацию значений входных параметров. При этом каждой строке соответствует определенное значение выходного параметра. И это выполняется для любой возможной комбинации значений выбранных

параметров. Далее качественным значениям переменных ставятся в соответствие усредненные количественные значения в границах от 0 до 1 по алгоритму, представленному в работе [19]. Таким образом получаем совокупность данных для возможности применения методов регрессионного анализа.

Шаг 3. Построение уравнения множественной регрессии

Используя опции Matlab, MS Excel или других программных продуктов, имеющих опции для работы с регрессиями, строим для простоты изложения линейную модель множественной регрессии из (1) с введенными в рассмотрение объясняющими переменными:

$$R = a_0 + \sum_{i=1}^{m} k_i P_i + \varepsilon \qquad (2)$$

где a_0 и $k_i, i = 1,...,m$, несравнимые коэффициенты, вычисляемые с помощью МНК. Далее от уравнения (2) переходим к уравнению в стандартизованном масштабе и находим стандартизованные коэффициенты.

Шаг 4. Анализ полученного результата

Выстраиваем коэффициенты в порядке возрастания для определения переменных, от которых в большей степени зависит риск информационной безопасности. Кроме того, исследуем переменные на зависимость между собой.

Чтобы оценить качество построенной модели, вычисляется один из важных показателей при построении регрессии - коэффициент множественной детерминации для оценки совместного влияния переменных. Чем он выше, тем большее влияние оказывают выбранные переменные на уровень риска *R*.

При низком значении коэффициента множественной детерминации (меньше 0,6) переменные с наименьшим значением коэффициентов k_i, исключаем из рассмотрения. Возвращаемся на шаг 2, где вместо исключенных параметров выбираем из множества *n* другие параметры и повторяем вышеуказанные шаги до получения значения коэффициента множественной детерминации не меньше 0,8.

Итерационный процесс можно завершить, когда убедимся, что любая новая комбинация параметров не дает значимого увеличения коэффициента множественной детерминации. В этом случае будем считать, что найдены параметры, максимально влияющие на значение уровня риска информационной безопасности рассматриваемого информационного объекта. Используем *F*-критерий Фишера и *t*-критерий Стьюдента, чтобы убедиться в статистической значимости или в отсутствии таковой, как коэффициентов регрессии, так и полученного уравнения регрессии в целом.

После определения факторов, максимально влияющих на уровень риска информационной безопасности, переходим к процедуре сравнительной оценки риска. Сравниваем, полученное при вышеуказанных факторах, значение уровня риска с допустимыми границами его значений. По возможности необходимо реализовать комплекс мер, чтобы обеспечить такие значения установленных факторов, при которых значение уровня риска лежит в допустимых пределах.

Необходимо учитывать, что затраты на обеспечение требуемых значений искомых параметров не должны превышать возможные потери от реализации потенциальных угроз.

3. Результаты

В результате проведения оценки уровня риска информационной безопасности по предлагаемой методике можно выйти на принятие следующих решений:

- дополнительных мер не требуется, обеспечен приемлемый уровень риска;
- требуются срочные меры по устранению критических уязвимостей;
- продолжить анализ риска с учетом дополнительных параметров, как внешнего, так и внутреннего характера;
- скорректировать цели в сторону уменьшения уровня риска и затрат.

В случае принятия любого из вышеперечисленных решений, надо учитывать необходимость постоянного мониторинга уровня риска, так как любое изменение внешних или внутренних условий функционирования информационной инфраструктуры может оказывать влияние на его значение.

Необходимо отметить, что в результате применения данной методики реализуется возможность формирования базы знаний с помощью продукционных правил. При этом вместо значений в качественном виде (значения, как указывалось выше: «низкий», «средний», «высокий» и т.п.) формируются данные в количественном виде как в работе [19,21] с помощью усреднения значений термов лингвистических переменных. Кроме того, для облегчения процедуры создания нечеткой базы знаний было предложено использовать метод усредненных коэффициентов влияния, представленный в [22] для получения значений уровня риска из (1), что в разы ускорило формирование базы знаний.

Используя данные из сформированной на основе продукционных правил базы знаний и, формируя уравнение множественной регрессии, строится модель регрессии так, чтобы уменьшить число объясняющих переменных, которые значительно влияют на значение переменной «уровень риска». При этом необходимо проанализировать взаимную корреляцию объясняющих переменных. По результатам анализа исключить из рассмотрения переменные, влияющие на риск на уровне погрешности.

Сформированная база знаний позволяет значительно упростить мониторинг уровня риска, так как для этого требуется вносить в нее изменения только по тем параметрам, значения которых изменились за рассматриваемый период.

Предлагаемая методика была апробирована при решении задачи определения критических узлов в информационных системах, имеющих сложную сетевую структуру [19], а также задачи оценки страховых рисков при страховании информационных систем, ресурсов и обеспечивающих их инфраструктур [21]. В обоих случаях методика показала хороший результат по оценке уровня риска в условиях неопределенности.

Настоящая методика достаточно универсальна и ее применение возможно не только для решения уже рассмотренных задач оценки рисков информационной безопасности, но и для решения возникающих задач в других сферах деятельности в условиях неопределенности. Например, в работе [23] авторы применили многокритериальные методы оптимизации, используемые в методике, с помощью которых были определены параметры, наибольшим образом влияющие на демографическую ситуацию в различных регионах.

4. Заключение

Совместное использование методов нечеткой логики, регрессионного анализа и многокритериальной оптимизации для оценки уровня риска информационной безопасности позволяет вычислять прогнозные значения уровня риска в условиях неопределенности и неочевидности взаимосвязи уровня риска от различных параметров, включая субъективные, такие как: уровень зарплаты, уровень заинтересованности сотрудника в конечном результате и другие.

Возможность определения факторов, наибольшим образом влияющих на значение уровня риска, позволяет сосредоточить внимание компаний на противодействии угрозам на наиболее опасных направлениях и минимизировать затраты на мероприятия по защите своих информационных ресурсов.

Предложенную методику можно применять к любой сложной сетевой структуре в государственных и частных компаниях, имеющих разветвленную сеть региональных подразделений (филиалов). Причем методика позволяет не только определять риск и критические узлы, но и оценивать эффективность работы филиалов в компаниях с распределенной структурой [19, 24].

Также эту методику можно применять в сфере киберстрахования или страхования рисков в области информационных технологий [21]. Ее применение расширяет возможности использования инструментов страхования информационных рисков в различных компаниях и дает возможность относительно просто определять уровень страхового риска в условиях неопределенности и в значительной мере облегчать андеррайтинг.

Представляет интерес применение аналогичной методики, основанной на совместном использовании методов эконометрики и многокритериальной оптимизации [23], с целью проведения сравнительного анализа демографической ситуации в различных субъектах России с определением показателей, наибольшим образом влияющих на демографию региона, что позволяет региональным властям строить прогнозы и формировать политику в области демографии.

Универсальность методики позволяет применять ее во многих сферах управления от небольших компаний и предприятий до государственного сектора. Т.е. там, где требуется оценивать различные риски в условиях неопределенности.

В настоящее время в экономике и бизнесе все шире используются искусственные нейронные сети [25]. Нейросети применяются, в том числе, для повышения уровня обнаружения атак на компьютерные

сети, а также для определения уровня риска информационной безопасности таких компьютерных сетей [26-29].

При создании и эксплуатации таких сетей разработчики и пользователи также сталкиваются с рисками информационной безопасности. И эти риски в основном лежат в области неопределенности. Авторы полагают, что предложенная методика позволяет также осуществлять оценку уровня риска информационной безопасности при использовании нейросетей и систем искусственного интеллекта.

Литература

1. Россия: утечки информации ограниченного доступа, 2022-2023 годы: Аналитический отчет. [Электронный ресурс], https: //www.infowatch.ru/sites/default/files/analytics/files/utechki-informatsii-ogranichennogo-dostupa-v-rossii-za-2022-2023.pdf (дата обращения 12.03.2024)
2. ГОСТ Р ИСО 31000-2019. Национальный стандарт Российской Федерации. Управление рисками. Принципы и рекомендации. [Электронный ресурс]. – [Онлайн], доступно https://pqm-online.com/assets/files/lib/std/gost-r-iso-31000-2019.pdf
3. *Разумников С.В.* Анализ возможности применения методов OCTAVE, Risk Watch, CRAMM для оценки рисков ИТ для облачных сервисов // Современные проблемы науки и образования, 2014. - № 1. - С. 247-248.
4. *Баранова С.Ю.* Методики анализа и оценки рисков информационной безопасности // Вестник Московского университета им. С.Ю. Витте. Серия 3. Образовательные ресурсы и технологии, 2015. – № 1(9). – С. 73-79.
5. *Asgari, H., Haines, S., Rysavy, O.* Identification of threats and security risk assessments for recursive internet architecture// IEEE Systems Journal. – 2018. - 12(3), 8105791, pp. 2437-2448
6. *Козлов А.Д., Нога Н.Л.* Риски информационной безопасности корпоративных информационных систем при использовании облачных технологий // Управление риском, М.: ООО «АНКИЛ», 2019. - №3. – С. 31-46.
7. *Царегородцев А.В., Зеленина А.Н., Савельев В.А.* Двухэтапная процедура количественной оценки риска информационной безопасности облачных вычислений// Моделирование, оптимизация и информационные технологии. – 2017. - №4(19). http://moit.vivt.ru
8. *Shirisha Reddy, K., Bala Raju, M., Naik, R.* Security measures in distributed approach of cloud computing// Advances in Intelligent Systems and Computing. – 2019. - 768, pp. 19-30
9. *Kozlov, A.D. & Noga, N.L.* About Some Risks Associated with Subjective Factors and the Methodology for their Assessment. Review of Business and Economics Studies. M.: Финансовый университет. №3, 2021. С.94-102
10. ГОСТ Р 58771-2019 (2020). Национальный стандарт Российской Федерации. Управление рисками. Технологии оценки рисков. [Электронный ресурс]. – [Онлайн], доступно https://meganorm.ru/Data2/1/4293724/4293724640.pdf?ysclid=ltsgsihboa807836364
11. *Kozlov A., Noga N*. Some Method of Complex Structures Information Security Risk Assessment in Conditions of Uncertainty / Proceedings of the 13th International Conference "Management of Large-Scale System Development" (MLSD). M.: IEEE, 2020. https://ieeexplore.ieee.org/document/9247662.
12. *Choudhary R., Raghuvanshi A.* Risk Assessment of a System Security on Fuzzy Logic// International Journal of Scientific & Engineering Research. - 2012. Vol. 3 (12), ISSN 2229-5518.
13. *Hany Sallem* Cyber security risk assessment using multi fuzzy inference system// International Journal of Engineering and Innovative Technology (IJEIT). – 2015. Vol.4 (8), pp. 13-19
14. *Ventresca M., Aleman D*. Efficiently identifying critical nodes in large complex networks // Computational Social Networks. 2015. Vol. 2, no. 6. pp. 3–16.
15. *Kozlov A.D., Noga N.L.* Applying the Methods of Regression Analysis and Fuzzy Logic for Assessing the Information Security Risk of Complex Systems // Proceedings of the 14th International Conference "Management of Large-Scale System Development" (MLSD). Moscow, IEEE, 2021. URL
16. *Корнев Л.В*. Нечеткая модель для оценки рисков информационной безопасности и поддержания уровня защищенности ERP-систем. Молодой ученый. № 27(369), 2021, С.48-54. https://moluch.ru/archive/369/83061 / (дата обращения: 26.01.2024).
17. Matlab R2022b free [Электронный ресурс]. – Режим доступа: https:// https://matlab.software.com/ - (Дата обращения: 09.10.2023)
18. *Булдакова Т.И., Миков Д.А.* Внедрение методологии оценки рисков информационной безопасности в среде Matlab. Вопросы кибербезопасности. 4 (12), 2015, С.53–61.
19. *Козлов А.Д., Нога Н.Л.* Методика определения наиболее критичных узлов сетевых информационных инфраструктур с целью обеспечения информационной безопасности // Информационные технологии. - М.: Новые технологии. №6, Т. 29, 2023, С. 296-306
20. *Елисеева И.И.* и др. Эконометрика // М.: Финансы и статистика, 2003. – С.344.
21. *Козлов А.Д., Нога Н.Л.* Методика определения параметров, наибольшим образом влияющих на страховые риски в области информационных технологий // Страховое дело, М.: ООО «АНКИЛ». №12, 2023, С. 17-26.
22. *Козлов А.Д., Нога Н.Л.* Метод усредненных коэффициентов влияния для формирования нечеткой базы знаний при оценке рисков информационной безопасности // Материалы 30-й Международной конференции «Проблемы управления безопасностью сложных систем» (ПУБСС'2022, Москва). М.: ИПУ РАН, 2022. С. 174–180.

23. *Kozlov, A.D. & Noga, N.L.* The Comparative Assessment Methodology of the Demographic Situation in the Regions. Proc. of the 16th int. conf. Management of Large-Scale System Development (MLSD), Moscow, IEEE, 2023, URL: https://ieeexplore.ieee.org/document/10303875
24. *Kozlov A.D., Noga N.L.* The Selection of the Comparative Evaluation Method of the Effectiveness of the Insurance Company Branches // Proceedings of the 15th International Conference "Management of Large-Scale System Development" (MLSD). Moscow, IEEE, 2022. URL: https://ieeexplore.ieee.org/document/9934192.
25. *Городнова Н.В.* Применение искусственного интеллекта в бизнес-сфере: современное состояние и перспективы // Вопросы инновационной экономики. – 2021. – Том 11. – № 4. – С. 1472-1492.
26. *Дьяченко Р.А., Частикова В.А., Лях А.Р*. Реализация атак уклонением на нейронные сети и методы их предотвращения // Электронный сетевой политематический журнал «Научные труды КубГТУ». - 2022, № 5. С. 68–77.
27. *Xu X., Chen J., Xiao J., Gao L., Shen F., and Shen H.T*. What machines see is not what they get: fooling scene text recognition models with adversarial text images. 2020, CVPR.
28. SmartEngines. Насколько неуязвим искусственный интеллект? [Электронный ресурс] – Режим доступа: https://habr.com/ru/companies/smartengines/articles/528686/ - (Дата обращения: 06.12.2023).
29. *Ермаков С.А., Болгов А.А.* Оценка риска с использованием нейро-нечеткой системы // Информация и безопасность, г. Воронеж: Концерн «Созвездие», 2022. Т. 25. вып. 4. С. 583-592