EKSPRES - İNFORMASİYA

Azərbaycan Respublikası Elm və Təhsil Nazirliyi
İNFORMASİYA TEXNOLOGİYALARI İNSTİTUTU

İNFORMASİYA TƏHLÜKƏSİZLİYİ VƏ KİBERDAYANIQLIQ PROBLEMLƏRİ

məqalələrin xülasələri

EKSPRES - İNFORMASİYA

Bakı - 2026

Azərbaycan Respublikası Elm və Təhsil Nazirliyi
İNFORMASİYA TEXNOLOGİYALARI İNSTİTUTU

İNFORMASİYA TƏHLÜKƏSİZLİYİ VƏ KİBERDAYANIQLIQ PROBLEMLƏRİ

məqalələrin xülasələri

EKSPRES - İNFORMASİYA

Bakı - 2026

İnformasiya təhlükəsizliyi və kiberdayanıqlıq problemləri. Məqalələrin xülasələri. Ekspres-informasiya. Bakı: "İnformasiya Texnologiyaları" nəşriyyatı, 2026. 308 səh.

İnformasiya cəmiyyəti şəraitində informasiya təhlükəsizliyinin etibarlı təmin edilməsi informasiya sahəsində ölkəmizin milli maraqlarının qorunmasında mühüm rol oynayır. Dövlətin, cəmiyyətin və şəxslərin həyatı vacib informasiya resurslarını hədəfə alan kibertəhlükələrə qarşı effektiv təhlükəsizlik sisteminin qurulması üçün, ilk növbədə, məqsədyönlü elmi tədqiqatların aparılması zəruridir.

İnformasiya Texnologiyaları İnstitutu artıq 25 ildən çoxdur ki, informasiya təhlükəsizliyi problemləri üzrə tədqiqatlar aparır. İndiyə qədər institutda informasiya təhlükəsizliyinin müxtəlif mövzularında 500-ə yaxın elmi əsər dərc olunmuş, onlardan bir çoxu nüfuzlu beynəlxalq nəşrlərdə çap edilmişdir.

Ekspres-informasiyaya İnstitutun əməkdaşları tərəfindən informasiya təhlükəsizliyi problemləri üzrə dərc edilən elmi əsərlərin xülasələri daxil edilmişdir.

Elmi redaktor: tex. fəl. dok., dosent Ramiz Şıxəliyev

DOI:10.25045/ISCR.02

1. Алгулиев Р.М. Методы синтеза адаптивных систем обеспечения информационной безопасности корпоративных сетей // Москва, **«УРСС», 2001,** 248 с.

   Монография посвящена вопросам разработки научно-методологических основ и архитектурных принципов синтеза адаптивных систем обеспечения информационной безопасности (АСОИБ) корпоративных сетей (КС). Согласно предлагаемому подходу АСОИБ представлена как специализированная сеть, построенная по stealth-технологии и охватывающая все контролируемые точки и ресурсы информационной сферы КС. АСОИБ состоит из взаимодействующих функциональных подсистем с распределенной структурой, предназначенных для реализации отдельных задач по обеспечению информационной безопасности сети. Разработаны соответствующие математические модели и методы синтеза для каждой из этих подсистем. Предложена концептуальная модель управления глобальным состоянием безопасности КС, согласно которой функционирование АСОИБ осуществляется как многошаговые процессы принятия решений. Выработаны общесистемные критерии и требования для практической реализации предлагаемой функциональной структуры АСОИБ. Книга предназначена для научных работников, аспирантов и студентов, а также для специалистов, занимающихся теоретическими и

практическими аспектами обеспечения информационной безопасности компьютерных сетей и систем.

2. Алгулиев Р.М., Алекперов Р.К., Алиев И.М. Об одном методе обеспечения безопасной сетевой среды для распределенных вычислений / **Труды II Международной конференции «Параллельные вычисления и задачи управления»**, Москва, Россия, **4-6 октября 2004,** с. 814-821.

   В данной работе приведена модель распределенных вычислений в открытых компьютерных сетях. Для обеспечения безопасности распределенных вычислении предлагается использовать виртуальные частные сети с перестраиваемой структурой в соответствии с архитектурной решения сложных задач для каждого уровня определены условия изменения внутренний структуры среды распределенных вычислений.

3. Алгулиев Р.М., Арзуманов Х.Т., Имамвердиев Я.Н. О некоторых специальных схемах цифровой подписи на эллиптических кривых / **XII общероссийская научно-техническая конференция «Методы и технические средства обеспечения безопасности информации»,** Санкт-Петербург, Россия, **4-5 октября 2004,** с. 47.

   В работе рассматриваются некоторые криптографические протоколы на эллиптических кривых.

Предлагаются схемы групповой подписи, с дополнительными функциональными свойствами на основе эллиптических кривых.

4. Алгулиев Р.М., Имамвердиев Я.Н. Анализ современного состояния криптографии гиперэллиптических кривых / **XII общероссийская научно-техническая конференция «Методы и технические средства обеспечения безопасности информации»,** Санкт-Петербург, Россия, **4-5 октября 2004,** с. 48.

   Анализируется современное состояние криптографии гиперэллиптических кривых. Анализ охватывает алгоритмы расчета числа точек гиперэллиптической кривой, алгоритмы решения HECDLP, методы улучшения групповых операций кривых рода 2, 3 и 4, алгоритмы скалярного умножения, аппаратные и программные имплементации HECC, сравнение ECC и HECC.

5. Алгулиев Р.М., Имамвердиев Я.Н. Об одном методе умножения в GF (2m) для криптографии эллиптических кривых / **XII общероссийская научно-техническая конференция «Методы и технические средства обеспечения безопасности информации»,** Санкт-Петербург, Россия, **4-5 октября 2004,** с. 49.

Предложен метод для эффективного умножения в конечных полях характеристики два для общего случая нормальных базисов.

6. Алгулиев Р.М., Имамвердиев Я.Н. О генерации эллиптических кривых в форме Монтгомери / **XII общероссийская научно-техническая конференция «Методы и технические средства обеспечения безопасности информации»,** Санкт-Петербург, Россия, **4-5 октября 2004,** с. 50.

   Предложен метод генерации эллиптических кривых в форме Монтгомери, пригодных для использования в криптографических системах. В предложенном методе для проверки делимости порядка эллиптической кривой на 4 требуется решать алгебраические уравнения в конечных полях.

7. Алгулиев Р.М., Шыхалиев Р.Г. Основные способы экранирования корпоративных сетей / **Труды II республиканской научной конференции «Современные проблемы информатизации, кибернетики и информационных технологий»,** Баку, Азербайджан, **26-28 октября 2004,** т. 1, с. 33-35.

   Работа посвящена вопросу обеспечения информационной безопасности корпоративных сетей, подключенных к Интернет. Для решения этой задачи предлагается применять межсетевой экран. В работе рассматриваются основные схемы организации

межсетевого экрана, анализируется их функционирование и приводятся их основные преимущества и недостатки.

8. Шыхалиев Р.Г. Об одной модели управления информационными потоками во взаимоувязанных корпоративных информационных пространствах / **Тезисы докладов 10-й юбилейной международной научной конференции «Теория и техника передачи, приема и обработки информации»,** Харьков–Туапсе, Украина, **28 сентября-1 октября 2004,** ч. 1, с. 112-114.

   Работа посвящена обеспечению информационной безопасности взаимоувязанных корпоративных информационных пространств. Рассматривается одна из ключевых задач решения этой проблемы – разграничение доступом. Для решения этой задачи предлагается использовать модель контроля доступа и полномочия - это контроль полномочия на основе задач (Task-based Authorization Controls – TBAC), которая заключается в оптимизации декомпозиции процесса на задачи, а также данных, доступу к которым нуждаются множество субъектов и через это оптимизировать управление доступом.

9. Шыхалиев Р.Г. Об упорядочении информационных потоков во взаимоувязанных корпоративных информационных пространствах / **XII обще-российская научно-техническая конференция**

«Методы и технические средства обеспечения безопасности информации», Санкт-Петербург, Россия, **4-5 октября 2004,** с. 46.

В работе рассматривается упорядочение информационных потоков во взаимоувязанных корпоративных информационных пространствах (ВУКИП). Задача упорядочения информационных потоков ВУКИП состоит в том, чтобы упорядочить множества всех потоков информации, связанных с реализацией глобальной задачи ВУКИП в единую систему с учетом имеющейся попарной упорядоченности информационных потоков локальных задач.

10. Шыхалиев Р.Г. О концепции взаимоувязанности структуры корпоративных информационных пространств / **Тезисы докладов V всероссийской конференции молодых ученых по математическому моделированию и информационным технологиям.** Новосибирск, Россия, **1-3 ноября 2004,** с. 54-55.

    Работа посвящена обеспечению информационной безопасности взаимоувязанных корпоративных информационных пространств. При формировании ВУКИП для обеспечения взаимосвязанности их структуры предлагается использовать системный подход, который основывается на иерархической структуре взаимодействия субъектов и объектов в

рамках задач, решаемых в этих пространствах. Предполагается, что именно структура задач, решаемых во ВУКИП, определяет их структуры.

11. Алгулиев Р.М., Рагимов Э.Р. Методы оценки информационной безопасности корпоративных сетей в стадии их проектирования // **Информационные технологии, 2005,** № 7, с. 35-39.

    Предложена метрика оценки информационной безопасности корпоративных сетей в стадии их проектирования, основанная на статистических данных о нарушениях информационной безопасностии модели надежности программных средств. Приведен численный пример.

12. Алгулиев Р.М., Рагимов Э.Р. Нечеткая модель оценки информационной безопасности в корпоративных сетях // **Автоматика и вычислительная техника, 2005,** № 2, с. 66-74.

    Предложена нечеткая модель оценки информационной безопасности корпоративных сетей в стадии их проектирования, основанная на статистических даных о нарушениях информационной безопасности и модели надежности программных средств.

13. Имамвердиев Я.Н. Об одной схеме подписи на основе идентификационных данных с использованием билинейных отображений на эллиптических кривых // **Телекоммуникации, 2005,** № 5, с. 28-31.

Предложена новая схема подписи на основе идентификационных данных с использованием билинейных отображений на эллиптических кривых. Безопасность схемы основана на сложности вычислительной задачи Диффи-Хеллмана. Проведено сравнение предложенной схемы с другими аналогичными схемами подписи с точки зрения эффективности.

14. Имамвердиев Я.Н. Об одной схеме подписи на основе идентификационных данных с использованием билинейных отображений на эллиптических кривых // **Информационные технологии, 2005,** № 7, с. 32-35.
Предложена новая схема подписи на основе идентификационных данных с использованием билинейных отображений на эллиптических кривых. Безопасность схемы основана на сложности вычислительной задачи Диффи-Хеллмана. Проведено сравнение предложенной схемы с другими аналогичными схемами подписи с точки зрения эффективности.
15. Шыхалиев Р.Г. Моделирование межсетевых экранов фильтрацией пакетов на основе сетей Петри // **Известия НАНА. Серия физико-математических и технических наук, 2005,** т. XXV**,** № 2, с. 161-164.
В статье предложена модель межсетевых экранов (МЭ) с фильтрацией Internet Protocol (IP)-пакетов. Для моделирования использованы Раскрашенные Сети Петри (РСП). РСП хорошо подходят для моделирования систем

МЭ, которые предписывают политику контроля доступа на основании информации, находящейся в заголовках IP-пакетов. Построенная модель может использоваться для имитации МЭ с фильтрацией, для проверки корректности политики безопасности, осуществляемой ими, а также для анализа работы МЭ. Кроме того, эта модель может использоваться как основа для проектирования средств анализа МЭ с фильтрацией IP-пакетов.

16. Абдуллаева Ф.Д. Об одном способе предотвращения несанкционированного доступа к информационной системе «Население и миграция» // **Информационные технологии моделирования и управления, 2006,** № 4, с. 421-427.

    В данном исследовании проводится анализ существующих формальных моделей безопасности, представлены их достоинства и недостатки и в качестве альтернативы выбирается контроль доступа на основе задач. Данная модель подходит для осуществления разграничения доступа в распределенной системе «Население и миграция»

17. Абдуллаева Ф.Д. Гарантированная защита персональных данных от несанкционированной модификации и считывания // **Вестник Московского городского педагогического университета, 2006,** № 1, с. 220-221.

В данной статье для того, чтобы защитить персональные данные от несанкционированной модификации и несанкционированного считывания, предложенно применение криптографических методов, таких, как электронная цифровая подпись и шифрование данных.

18. Алгулиев Р.М., Рагимов Э.Р. Об одном подходе оценки риска при проектировании защищенных корпоративных сетей // **Информационные технологии моделирования и управления, 2006,** № 1, с. 94-98.

    В данной работе рассматриваются вопросы оценки риска на стадии проектирование корпоративных сетей. Продемонстрированы этапы процесса анализа рисков. На основе данного анализа, предложен подход оценки риска проектирования защищенных корпоративных сетей на основе сервисов безопасности. Исходя из данного подхода, приведены вычисления вероятности и стоимости потерь от нарушения сервисов безопасности.

19. Алгулиев Р.М., Рагимов Э.Р. Синтез архитектуры защищенной корпоративной сети // **Телекоммуникации, 2006,** № 2, с. 19-23.

    Рассмотрены вопросы синтеза защищенных корпоративных сетей по заданным критериям. Для оценки информационной безопасности корпоративных сетей используются уравнения множественной регрессии

с учетом архитектурных особенностей корпоративных сетей. Приведены примеры синтеза защищенной корпоративной сети на базе межсетевых экранов.

20. Шыхалиев Р.Г. Об одном методе экранирования мультикаст-трафика во взаимоувязанных корпоративных информационных пространствах // **Информационные технологии, 2006,** № 8, с. 36-40.

    Предлагается метод экранирования мультикаст-трафика во взаимоувязанных корпоративных информационных пространствах на основе межсетевого экрана. В основу метода положена структура SOCKS, которая является одним из решений.

21. Абдуллаева Ф.Д. Комплексный подход к обеспечению безопасности информационной системы «Население и миграция» / **Материалы международной научно-технической конференции «Наука и образование-2006»,** Мурманск, Россия, **4-12 апреля 2006,** с. 99-101.

    В данной работе предложен комплексный подход к решению проблемы безопасности информационной системы «Население и миграция», где практически любая техническая проблема этой системы не поддается одностороннему решению.

22. Шыхалиев Р.Г. Проблемы экранирования взаимоувязанных корпоративных информационных пространств / **Материалы международной**

конференции «Проблемы кибернетики и информатики», Баку, **24-26 октября 2006,** том 2, с. 43-46.

Работа посвящена вопросу обеспечения информационной безопасности взаимоувязанных корпоративных информационных пространств (ВУКИП). Для этого предлагается применять технологию экранирования. В работе проводится анализ экранирования ВУКИП и обозначены основные проблемы. Для решения проблемы экранирования ВУКИП предложены методы и модели.

23. Керимова Л.Э. Об одном методе кластеризации сетевого трафика для обнаружения некоторых типов угроз корпоративным сетям / **Материалы международной конференции «Проблемы кибернетики и информатики»,** Баку, **24-26 октября 2006**, т. 2, с. 35-38.

В материале рассматривается работа модуля кластеризация, выполненная как отдельная функциональная компонента в предложенном архитектурном подходе создания систем обнаружения вторжений. Предлагается метод обнаружения сетевых вторжений с помощью точных методов решения задачи кластеризации на основе результатов анализа данных мониторинга сети. Формулируются общие представления о качестве кластеризации в виде нового функционала, оптимум которого соответствует

наилучшей кластеризации, приводится алгоритм нахождения оптимального кластера.

24. Керимова Л.Э. Об одном подходе построения профиля кластеров для обнаружения аномалий / **Сборник докладов IV международной научно-практической конференции «Единое информационное пространство»,** Днепропетровск, **7-8 декабря 2006,** с. 46-47.

    В работе классифицируются сетевые соединения на основе различных значений особенностей в заголовке соединения для выявления аномалий. Далее, опираясь на методы добычи данных: ассоциативные правила и последовательные частотные эпизоды, построен профиль для каждого кластера.

25. Fərəcullayev R.F. WEB-saytların təhlükəsizliyinin təmin olunması üçün bəzi tədbirlər haqqında // **Bakı Universitetinin Xəbərləri.** Fizika-riyaziyyat elmləri seriyası, **2007,** № 2, s. 95-101.

    Məqalədə web-sistemlərdə informasiya təhlükəsizliyinin aktuallığına diqqət yetirilir, web-saytların təhlükəsizliyinin müxtəlif səviyyələri haqqında və web-sistemlərdə informasiya təhlükəsizliyinin təmin edilməsi üçün mövcud tədbirlər haqqında danışılır. Respublikada son zamanlar baş verən web-sayt hücumları və bu hücumlar nəticəsində sıradan çıxarılmış saytlar bu sahəyə diqqətin daha da artırılmasının, eləcə də növbəti hücumlara qarşı dayanıqlılığın daha da

möhkəmləndirilməsinin və təhlükəsizliyin gücləndirilməsinin vacibliyini göstərməkdədir. Bu səbəbdən də web təhlükəsizliyi və onun müxtəlif səviyyələrini daha yaxşı anlamaq və mümkün tədbirləri bilmək vacibdir. Məqalədə həmçinin web təhlükəsizliyi haqqında daha ətraflı informasiya toplanması və ən son yeniliklərin əldə edilməsi üçün web istinadlar tövsiyyə olunmuşdur.

26. Шыхалиев Р.Г. Об одной модели экранирования взаимоувязанных корпоративных информационных пространств с использованием сетей Петри // **Телекоммуникации, 2007,** № 1, с.41-44.

    Предложена модель экранирования взаимоувязанных корпоративных информационных пространств (ВУКИП). Для моделирования использованы сети Петри. Сети Петри хорошо подходят для моделирования систем экранирования ВУКИП, которые предписывают политику контроля доступа на основе правил фильтрации. Построенная модель может использоваться для имитации и тестирования системы экранирования ВУКИП и проверки корректности политики безопасности, осуществляемых ею. Модель может быть так же использована как основа для проектирования средств анализа систем экранирования ВУКИП.

27. Abdullayeva F.C. Milli informasiya infrastrukturunun əhali və miqrasiya seqmentində informasiya

təhlükəsizliyinin təmin edilməsi / "**Riyaziyyatın tətbiqi məsələləri və yeni informasiya texnologiyaları" respublika elmi konfransı,** Sumqayıt, **26-27 noyabr 2007**, s. 211-213.

Məqalədə Azərbaycan Respublikasının Milli informasiya infrastrukturunun əsas hissəsini təşkil edən və əhali haqqında fərdi məlumatların toplanmasını həyata keçirən əhali və miqrasiya seqmentinin (sisteminin) təhlükəsizliyinin təmin edilməsi üçün sistemin istifadəçilərinin autentifikasiyasını həyata keçirən informasiya təhlükəsizliyinin təmin edilməsi sisteminin arxitekturası işlənmişdir. Əhali və miqrasiya sisteminin təhlükəsizliyinin təmin edilməsi məqsədi ilə informasiya təhlükəsizliyi arxitekturası ölkədə yaradılacaq elektron imza mexanizmindən istifadə etməyə imkan verən açıq açarlar infrastrukturunu tətbiq etməklə yaradılmışdır. Bunun üçün "Əhali və miqrasiya" informasiya sistemini təşkil edən resursların qarşılıqlı əlaqəsinə kliyent-server sistemi kimi baxılmış. Burada kliyentlər müvafiq rollara əsasən, serverlərdə yerləşən informasiya resurslarına müraciət etmək hüquqlarına malik olurlar. İstifadəçilərin həqiqiliyinin yoxlanmasına xidmət edən autentifikasiya prosesi rəqəmli sertifikatların köməyi ilə həyata keçirilir.

28. Əliquliyev R.M., Fərəcullayev R.F. Web sistemlərdə informasiya təhlükəsizliyinin təmin olunması üçün bəzi metodlar haqqında / "**Riyaziyyat, mexanika və**

informatikanın müasir problemləri" beynəlxalq simpoziumun tezisləri, Naxçıvan, **2-3 noyabr 2007,** s. 16.

Respublika Prezidenti tərəfindən Azərbaycanda İKT-nin inkişafı və ümumilikdə ölkənin davamlı inkişafına güclü təkan verən, onun hərtərəfli tərəqqisinə xidmət göstərən mühüm əhəmiyyətli dövlət proqramları və qərarlar, qanun və normativ aktlar qəbul olunmuşdur. Cəmiyyətin müxtəlif sferalarının informasiyalaşdırılmasını nəzərdə tutan "Azərbaycan Respublikasında rabitə və informasiya texnologiyalarının inkişafı üzrə 2005-2008-ci illər üçün Dövlət Proqramı"nı – Elektron Azərbaycan proqramını rəhbər tutaraq demək olar ki, Respublikada web-sistemlərə ehtiyac getdikcə artacaq. Burdan göründüyü kimi, web-sistemlərdə informasiya təhlükəsizliyi olduqca əhəmiyyətli və aktual məsələdir.

29. İmamverdiyev Y.N. Biometrik texnologiyaların təhlükəsizliyi / "**Elm və təhsildə informasiya-kommunikasiya texnologiyalarının tətbiqi" II beynəlxalq konfransı,** Bakı, **1–3 noyabr 2007,** I kitab, s. 831-832.

Biometrik texnologiyalar ənənəvi audentifikasiya vasitələri ilə müqayisədə bir sıra üstünlüklərə malik olsalar da onların təhlükəsizliyi yetərincə tədqiq olunmamışdır. Biometrik texnologiyaların praktik tətbiqində meydana çıxan əsas problemlər, konkret texnologiyalara yönələn təhdidlər, hücumların spesifik növləri və biometrik texnologiyaların təhlükəsizliyinin qiymətləndirilməsi məsələləri araşdırılır.

30. İmamverdiyev Y.N. İnformasiya təhlükəsizliyi kursunun tədrisi / "**Riyaziyyatın tətbiqi məsələləri və yeni informasiya texnologiyaları" respublika elmi konfransı,** Sumqayıt, **26-27 noyabr 2007**, s. 250-251.
Məruzədə Bakı Dövlət Universiteti Tətbiqi riyaziyyat və kibernetika fakültəsinin bakalavr pilləsi IV kurs informatika ixtisası tələbələri üçün 2007-ci ildə aparılmış "İnformasiya təhlükəsizliyinin əsasları" kursunun təcrübəsi haqqında məlumat verilir. Kurs informasiya təhlükəsizliyi və kriptoqrafiyaya geniş giriş verməklə vacib baza konsepsiyaları və metodları əhatə edir.
31. İmamverdiyev Y.N. Milli CERT yaradılmasına mərhələli yanaşma modeli / "**Riyaziyyatın tətbiqi məsələləri və yeni informasiya texnologiyaları" respublika elmi konfransı,** Sumqayıt, **26-27 noyabr 2007,** s. 252-254.
Milli informasiya fəzasında baş verən müxtəlif informasiya təhlükəsizliyi insidentlərinə vaxtında reaksiya verilməsi və onların qarşısının alınması, təhqiq olunması üçün Milli CERT-in yaradılması mərhələləri və hər mərhələdə həll edilməli olan məsələlər müzakirə edilir və konkret təkliflər irəli sürülür.
32. İmamverdiyev Y.N., Derakshandeh S.A. Mürəkkəb sistemlərdə informasiya təhlükəsizliyi risklərinin qiymətləndirilməsi **/ "Riyaziyyatın tətbiqi məsələləri və yeni informasiya texnologiyaları" respublika elmi konfransı,** Sumqayıt, **26-27 noyabr 2007,** s. 254-256.

İnformasiya təhlükəsizliyinin təmin edilməsində informasiya təhlükəsizliyi risklərinin analizinə və onların idarə edilməsinə mühüm rol ayrılır. İnformasiya təhlükəsizliyi risklərinin qiymətləndirilməsinə mövcud yanaşmalar analiz edilir. Qeyri-səlis məntiq əsasında mürəkkəb sistemlərdə informasiya təhlükəsizliyi risklərinin qiymətləndirilməsi üçün model təklif olunur.

33. Керимова Л.Э. Об одном архитектурном подходе к синтезу интеллектуальных систем обнаружения вторжений / **"Elm və təhsildə informasiya-kommunikasiya texnologiyalarının tətbiqi" II Beynəlxalq konfransı,** Bakı, **01-03 noyabr 2007,** I kitab, s.73-75.

В работе представлен новый архитектурный подход к синтезу интеллектуальных систем обнаружения вторжений (СОВ) как с явными, так и с неявными сигнатурами, который позволит расширить функциональные возможности существующих СОВ. Представлена реализованная в этой архитектуре мультимодульная система обнаружения вторжений.

34. Кязимов Т.Г., Махмудова Ш.Д. Информационная идентификационная система распознавания людей по фотопортретам // **Телекоммуникации, 2008,** №11, с. 22-25.

Для распознавания лиц (объектов, сигналов, ситуаций и событий) используются многочисленные ресурсы

человеческого мозга, в том числе, 10-12 миллиардов нейронов. В результате чего люди распознают друг друга, с большой скоростью читают изданные и рукописные тексты, на улице в сложных условиях водят машины, обрабатывают детали в конвейерах, расшифровывают пароли аэрокосмических фотографий. Распознавание человека по лицу и выбор его признаков основывается на интуиции. В автоматизации многих задач, как различительный признак для распознавания, очень сложно использовать информативные данные.

35. Абдуллаева Ф.Д. Метод вычисления вероятности отказоустойчивости и надежности информационной системы "Население и миграция" // **Вопросы защиты информации,** № 2**, 2008,** с. 49-52.

    Предложен метод вычисления отказоустойчивости и надежности распределенной информационной системы (ИС) "Население и миграция". Отказы серверов ИС "Население и миграция", являющихся независимыми один от другого, моделируются как распределение Пуассона с интенсивностью l. Для вычисления отказоустойчивости и надежности использован способ резервируемости объектов. Резервирование в данном случае выглядит как перенаправление повторных запросов пользователей на альтернативный сервер. Проведен численный расчет вычисления вероятности отказоустойчивости ИС "Население и миграция".

36. Abdullayeva F.D. On One Model of Access Differentiation to Resources of Information System "Population and Migration" by using Petri Nets // **Journal of Automation and Information Sciences, 2008,** vol. 40, iss. 9, pp. 69-74.

    The analysis of properties and possibilities of social networks is performed. The possible relations between personal data in the environment of the distiributed information system "Population and migration" is presented. The example of calculation of the neighborhood relation between the personal data is given.

37. İmamverdiyev Y.N. İnformasiya təhlükəsizliyi mütəxəssislərini sertifikatlaşdırma sistemləri / **"İnformasiya sistemləri və metodların hərbi-dəniz kadrlarının hazırlanmasında rolu" elmi-praktik konfrans,** Bakı**, 2008,** s. 129-134.

    İnformasiya təhlükəsizliyinin təmin edilməsi sistemində bu sahə üzrə ixtisaslaşan mütəxəssislərin hazırlanması mühüm yer tutur. İnformasiya təhlükəsizliyi sahəsində mütəxəssislərin hazırlanmasında ali məktəblərlə yanaşı bir sıra beynəlxalq konsorsiumlar və şirkətlər də əhəmiyyətli rol oynayırlar. Təqdim olunan işdə beynəlxalq konsorsiumların bu sahədəki fəaliyyəti və müvafiq sertifikatlaşdırma sistemləri analiz edilir.

38. Abdullayeva F.D., Imamverdiyev Y.N., Musayev V.Y., Wayman J.J. Analysis of Security Vulnerabilities in Biometric Systems / **Proceedings of the 2nd**

International Conference "Problems of cybernetics and informatics", Baku, **10-12 September 2008**, vol.1, pp. 60-63.

Biometrics is a rapidly developing branch of information technology. Biometric technologies are automated methods and means for identification based on biological and behavioral characteristics of an individual. There are several advantages of biometric technologies compared to traditional identification methods. To take adequate measures against increasing security risks in modern world, countries are considering these advantages and are shifting to new generation identification systems based on biometric technologies.

39. Derakhshandeh S.A., Imamverdiyev Y.N. Fuzzy majority modeling of information security risks / **Proceedings of the 2nd International Conference "Problems of cybernetics and informatics",** Baku, **10-12 September 2008**, vol. 1, pp. 64-66.

    Management of information security is grounded on the analysis and evaluation of information security risks. At present, there exist a number of standards (ISO 27001, NIST, MITRE), approaches and many instrumental means based on them (COBRA, CRAMM, MethodWare, RiskWatch, Avangard, GRIF), for evaluation of risks of information security. Risks evaluation based on fuzzy logic allows substituting the approximate schedule estimation for adequate modern mathematic methodology on the problem concerned.

40. Kazimov T.H., Mahmudova Sh.J. Information identification system for identifying people by portrait photos / **Proceedings of the 2nd International Conference "Problems of cybernetics and informatics",** Baku, **10-12 September 2008,** vol. 1, pp. 204-207.

    Manifold resources of human brain including 10-12 billion neurons are used for identification of peoples' faces (objects, signals, situations and events). It enables people to identify each other, read printed and handwritten texts with high speed, to drive cars in the street in complicated situations, process parts in assembly lines, decode aero cosmic photos. Choice of features for recognizing a human by his face is based on intuition. In automation of many tasks such as choice of the discriminating feature for recognition it is very difficult to use the factual information.

41. Shikhaliyev R.H., Imamverdiyev Y.N., Musayev V.Y., Wayman J.J. Analysis of the biometric systems security evaluation methodologies / **Proceedings of the 2nd International Conference "Problems of cybernetics and informatics",** Baku, **10-12 September 2008,** vol.1, pp. 71-74.

    One of the problems of biometric systems is certification on the basis of international standards issued by various biometric technologies. The paper analyzes the evolution methodologies for certification of biometric systems.

42. Əliquliyev R.M., Mahmudov R.Ş. İnformasiya asılılığı problemləri və onlarla mübarizə yolları. **Ekspress-informasiya.** İnformasiya cəmiyyəti seriyası. "İnformasiya Texnologiyaları" nəşriyyatı**, 2009,** 64 s.

Ekspress-informasiyada informasiya cəmiyyəti şəraitində xüsusi aktuallıq kəsb edən informasiya asılılığı problemi araşdırılır. Addiktologiyanın yeni tədqiqat sahəsi olan informasiya asılılığının yaranma səbəbləri, xüsusiyyətləri və doğurduğu fəsadlar göstərilir. İnternet-asılılığın tibbi-psixoloji profilaktikası, uşaqların bu təhlükədən qorunması, habelə bu problemlərlə mübarizə sahəsində beynəlxalq təcrübə tədqiq edilir, yeni təklif və tövsiyələr irəli sürülür.

43. Алгулиев Р.М., Имамвердиев Я.Н., Мусаев В.Я. Методы обнаружения живучести в биометрических системах // **Вопросы защиты информации, 2009,** №3, с. 16-21.

Методы обнаружения живучести являются важными мерами противодействия фальсификации биометрических характеристик. Эти методы автоматически определяют, что поступающий в биометрическую систему биометрический образец принят от живого человека. Опубликовано сравнительно мало результатов исследований эффективности этих мер, поэтому пользователи биометрических систем встречаются с трудностями при выборе метода обнаружения живучести, отвечающего требованиям

безопасности. Анализируются методы обнаружения живучести для разных биометрических характеристик, указываются направления дальнейших исследований по методам обнаружения живучести.

44. Abdullayeva F.J. On One Method of Constructing Relations between Personal Data in Social Networks // **Journal of Automation and Information Sciences, 2009,** vol. 41, no. 1, pp. 69-74.

    The analysis of properties and possibilities of social networks is performed. The possible relations between personal data in the environment of the distiributed information system "Population and migration" is presented. The example of calculation of the neighborhood relation between the personal data is given.

45. Алгулиев Р.М., Имамвердиев Я.Н., Абдуллаева Ф.Д. Вектор атаки и защитные меры персональных данных / **Материалы III международной научно-практической конференции «Актуальные проблемы безопасности информационных технологий»,** Красноярск, **9-11 сентября 2009,** с. 111-115.

    Рассматривается проблема обеспечения безопасности персональных данных. Излагается понятие вектора атаки персональных данных технического, физического и социально-инженерного характера. Понятие «кража данных» описывается как реальная угроза широкого

использования персональных данных. На основе методики управления рисками предлагается подход к снижению рисков краж персональных данных.

46. Əliquliyev R.M., Mahmudov R.Ş. İnternet fenomeninə çoxaspektli baxış. **Ekspres-informasiya.** İnformasiya cəmiyyəti seriyası. "İnformasiya Texnologiyaları" nəşriyyatı, **2010**, 96 s.

    Kitabda İnternet şəbəkəsinə texnoloji və sosial-humanitar aspektlərdan müxtəlif baxışlar şərh edilir. İnternetin təsiri nəticəsində əməyin transformasiyası, virtual əmək münasibətlərinin formalaşması kimi məsələlər araşdırlır. Qlobal şəbəkənin elm və təhsil sahələrinə gətirdiyi imkanlar, yeniliklər, bunların nəticəsində formalaşan elektron elm və təhsil mühitinin əhəmiyyəti göstərilir. Mədəni sferada İnternetin imkanları hesabına əldə edilən üstünlüklər, bir sira ənənəvi problemlərin həlli imkanları analiz edilir. İstifadəçilərin İnternetdə etik normalara əməl etmələri ilə bağlı problemlər araşdırılır.

47. Əliquliyev R.M., Mahmudov R.Ş. İnternetin tənzimlənməsi problemləri. **Ekspres-informasiya.** İnformasiya cəmiyyəti seriyası. "İnformasiya Texnologiyaları" nəşriyyatı**, 2010,** 115 s.

    Tədqiqat işində İnternetin tənzimlənməsi zərurəti və problemləri araşdırılır. Müvafiq tənzimləmə sahəsində beynəlxalq təşəbbüslər, qabaqcıl ölkələrin təcrübəsi analiz edilir. Tənzimləmə zamanı tətbiq edilən üsullar, hüquqi

mexanizmlər və yurisdiksiya məsələləri öyrənilir. Həmçinin İnternetlə bağlı digər problemlər – şəxsi həyatın toxunulmazlığı və fərdi məlumatların qorunması, domen adları sisteminin idarə edilməsi, provayderlərin hüquqi məsuliyyətinin müəyyənləşdirilməsi, kibercinayətkarlıqla, spamlarla mübarizə, intellektual mülkiyyət hüquqlarının qorunması, elektron kommersiya fəaliyyətinin tənzimlənməsi məsələləri tədqiq edilir.

48. Əliquliyev R.M., Mahmudov R.Ş. İnternet mühitində intellektual mülkiyyət hüquqlarının qorunması məsələləri. **Ekspres-informasiya.** İnformasiya cəmiyyəti seriyası. "İnformasiya Texnologiyaları" nəşriyyatı**, 2010,** 60 s.

    Ekspress-informasiyada İnternet mühitində intellektual mülkiyyət hüquqlarının qorunması problemlərinə və onların tənzimlənməsi məsələlərinə baxılır. Bu istiqamətdə mövcud olan müxtəlif yanaşmalar, ziddiyyətli məqamlar, beynəlxalq hüquqi normaları, qabaqcıl ölkələrin təcrübəsi araşdırılır, çatışmazlıqlar təhlil edilir. O cümlədən müəllif hüquqları və əlaqəli hüquqların qorunması, bunun üçün tətbiq edilən texnoloji vasitələrin hüquqi problemləri, müvafiq hüquqların qorunmasında İnternet-provayderlərin məsuliyyətinin müəyyən edilməsi məsələləri analiz olunur.

49. Əliquliyev R.M., İmamverdiyev Y.N. E-dövlətin informasiya təhlükəsizliyi: aktual tədqiqat istiqamətləri // **İnformasiya Cəmiyyəti Problemləri, 2010,** № 1, s. 3-13.

E-dövlət quruculuğunda qarşıya çıxan ən vacib və ən çətin məsələlərdən biri e-dövlətin etibarlı informasiya təhlükəsizliyinin təmin edilməsidir. Tədqiqat işində e-dövlətin informasiya təhlükəsizliyinin idarə edilməsi üzrə aktual elmi-tədqiqat problemləri müəyyən olunmuş və onların müasir vəziyyəti analiz edilmişdir. E-dövlətin informasiya infrastrukturuna yeni təhdidlər, təhdid aktorlarında baş vermiş keyfiyyət dəyişiklikləri ətraflı analiz edilmiş, ənənəvi təhlükəsizlik modellərinin e-dövlət kimi mürəkkəb obyektə tətbiqində meydana çıxan əsas çətinliklər göstərilmişdir.

50. İmamverdiyev Y.N., Derakshandeh S.A. İnformasiya təhlükəsizliyi risklərinin optimal idarə edilməsi modeli və onun genetik həll alqoritmi // **İnformasiya Texnologiyaları Problemləri, 2010,** № 2, s. 36-46.
İnformasiya təhlükəsizliyi risklərinin optimal idarə edilməsi üçün riyazi model təklif edilir. Risk amillərinin parametrləri və təhlükəsizlik mexanizmlərinin effektivliyi qeyri-səlis mənsubiyyət funkiyaları ilə ifadə olunmuşdur. Təklif edilmiş model verilmiş büdcə daxilində qalıq riskin minimallaşdırılması üçün təhlükəsizlik mexanizmlərinin optimal seçilməsi məsələsini həll edir. Optimal seçim tamqiymətli proqramlaşdırma məsələsi kimi formalizə olunmuş və onun həlli üçün genetik alqoritm təklif edilmişdir.
51. Mahmudov R.Ş. İnternetin tənzimlənməsinin aktual məsələləri // **İnformasiya Cəmiyyəti Problemləri, 2010,** № 1, s. 51-63.

Məqalədə internetin tənzimlənməsinin aktual problemləri araşdırılır. O cümlədən İnternet-yurisdiksiyanın müəyyən edilməsi, şəxsi həyat sirrinin və fərdi məlumatların qorunması, İnternet-provayderlərin məsuliyyətinin müəyyən edilməsi, domen adları sisteminin idarə edilməsi, spamlarla mübarizə, virtual məkanda intelektual mülkiyyət hüquqlarının qorunması, kibercinayətkarlıq, elektron kommersiyanın tənzimlənməsi üçün İnternetin tənzimlənməsinin zəruriliyi əsasındadır.

52. Алгулиев Р.М., Имамвердиев Я.Н., Дераkшанде С.А. Пути повышения точности методов оценки рисков информационной безопасности // **Информационные технологии, 2010,** № 12, с. 6-11.

Приведен сравнительный анализ существующих подходов к оценке рисков информационной безопасности (ИБ). Традиционные подходы к оценке рисков ИБ базируются в основном на качественных оценках, которые являются в высокой степени субъективными и не обладают необходимой достоверностью. Для разработки адекватных моделей оценки рисков необходимо учесть природу неопределенности. Анализируются вероятностный, нечетко-множественный и экспертный подходы к моделированию различных типов неопределенностей в контексте ИБ. Структурированы основные преимущества и недостатки методов оценки

рисков ИБ на основе этих подходов и намечены важные направления исследований в этой области.

53. Алгулиев Р.М., Имамвердиев Я.Н., Мусаев В.Я. Метод усиления безопасности биометрических систем с помощью водяных знаков // **Вопросы защиты информации, 2010,** № 6, с. 24-28.

    Хранение биометрической информации в виде шаблонов в базах данных и передача по незащищенным каналам для сравнения требуют обеспечения безопасности биометрических систем более надежными средствами. Предложены два варианта метода водяных знаков, они могут занять важное место в защите биометрической информации без шифрования. В первом методе изображение отпечатков пальцев скрывается в другом изображении, во втором — один биометрический образец (отпечатки пальцев) скрывают в другом биометрическом образце (изображение лица), это позволяет обеспечить более эффективный и надежный процесс идентификации.

54. Алгулиев Р.М., Имамвердиев Я.Н., Деракшанде С.А. Оценка риска информационной безопасности с использованием сетей Байеса // **Телекоммуникации, 2010,** № 6, с. 30-34.

    Управление информационной безопасностью требует точное определение риска. В этой работе обосновано использование сетей Байеса для оценки рисков

информационной безопасности. Для вычисления условных вероятностей предложен подход на основе деревьев атак как специальных сетей Байеса. Сети Байеса позволяют эффективным образом объединить исторические количественные данные с качественными. Существует возможность использования условных вероятностей для учета взаимной зависимости уязвимостей. Предложена также модель использования сетей Байеса для оценки ущерба от событий информационной безопасности.

55. Алгулиев Р.М., Имамвердиев Я.Н., Дераkшанде С.А. Сравнительный анализ методологий управления рисками информационной безопасности // **Azərbaycan Milli Aerokosmik Agentliyinin Xəbərləri, 2010,** № 2-3, s. 77-85.

    В работе предложена система критериев для сравнительной оценки методологий управления рисками информационной безопасности. Для критериев предлагаются легко оцениваемые метрики. Приводится оценка и сравнение некоторых распространенных методологий управления рисками.

56. Имамвердиев Я.Н. Метод биометрического хэширования на основе ортогональных преобразований для защиты биометрических шаблонов // **Вопросы защиты информации, 2010,** № 4, с. 18-22.

Безопасность биометрических шаблонов является важной задачей, так как скомпрометированные биометрические шаблоны невозможно аннулировать, и незащищенные биометрические шаблоны приводят к рискам конфиденциальности персональных данных. В работе предлагается метод биометрического хеширования для защиты биометрических шаблонов отпечатков пальцев. С использованием неинвертируемых преобразований изображения отпечатков пальцев преобразуются в случайные строки битов. Предлагаемый метод позволяет выполнить сравнение биометрических шаблонов в преобразованном пространстве.

57. Рагимов Э.Р. Механизм верификации безопасности программных средств, функционирующих в системе защиты информации корпоративных сетей // **Вопросы защиты информации, 2010**, № 4, с. 37-40.

Проведен анализ существующих недостатков как во внутренних архитектурах, так и в сервисах, предоставляемых программными средствами функционирующих в системе защиты информации корпоративных сетей. Определена метрика сложности поиска недостатков в программных средствах. На основе изучения существующих и приобретенных недостатков в программных средствах как во время эксплуатации, так и на стадии проектирования предложен механизм верификации безопасности программных средств,

составляющих основную линию системы защиты информации корпоративных сетей.

58. Рагимов Э.Р. Об одном подходе к безопасности программных средств в системе защиты информации корпоративных сетей // **Телекоммуникации, 2010,** № 12, с. 20-24.

    В данной работе проведен анализ существующих методов выявления элементов уязвимости как в кодах, внутренних архитектурах, так и в сервисах, предоставляемых программными средствами функционирующих в системе защиты информации корпоративных сетей. Определена метрика сложности поиска уязвимостей в программных средствах. На основе изучения существующих и приобретенных уязвимостей в программных средствах предложен механизм поиска этих уязвимостей, составляющих основную линию системы защиты информации корпоративных сетей.

59. Рагимов Э.Р. Выявление уязвимостей и выбор программного обеспечения для системы защиты информации корпоративных сетей // **Телекоммуникации, 2010,** № 1, с. 46-48.

    Рассмотрена математическая модель выявления уязвимостей в системе защиты информации корпоративных сетей, использующей определенный набор программного обеспечения в целях организации безопасности. Предложена метрика для оценки

информационной безопасности корпоративных сетей и на основе данного подхода указаны возможности выбора программного обеспечения безопасности для корпоративных сетей.

60. Шыхалиев Р.Г. Об одной модели экранирования взаимоувязанных корпоративных информационных пространств с использованием сетей Петри // **İnformasiya Texnologiyaları Problemləri, 2010,** №1, s. 19-25.

    В статье предложена модель экранирования взаимоувязанных корпоративных информационных пространств (ВУКИП). Для моделирования использованы сети Петри. Сети Петри хорошо подходят для моделирования систем экранирования ВУКИП, которые предписывают политику контроля доступа на основании правил фильтрации. Построенная модель может использоваться для имитации и тестирования системы экранирования ВУКИП и проверки корректности политики безопасности, осуществляемой ею. Также эта модель может быть использована как основа для проектирования средств анализа систем экранирования ВУКИП.

61. Imamverdiyev Y.N., Derakhshandeh S.A. Processing of Information Security Risks with Ordered Weighted Averaging Operators // **Australian Journal of Basic and Applied Sciences, 2010,** vol. 12, no. 4, pp. 6061-6064.

One of the processing mechanisms of information security risks is eduction of risks by using correct selection of counter-measures against threats.

62. Ələkbərova İ.Y. İnformasiya müharibəsinin dövlətin informasiya mühitinə təsiri problemləri haqqında / "**Elektron hökumət: Azərbaycanda nailiyyətlər və perspektivlər" I beynəlxalq konfrans,** Bakı, **26-28 aprel 2010,** s. 146-149.

    Material innovasiya iqtisadiyyatın formalaşmasının əsas istiqamətlərdən biri olan elektron kommersiya sistemlərinin təşkilati-iqtisadi modellərinin təhlilinə həsr olunmuşdur.

63. Алгулиев Р.М., Алекперова И.Я. Сетевые атаки как средства ведения информационной войны в интернет-среде / **7-я международная научно-практическая конференция «Интернет–Образование-Наука-2010»,** Винница, **28 сентября – 3 октября 2010,** с. 38-41.

    Необходимость исследования данной темы вызвана тем, что в настоящее время межгосударственные, межнациональные конфликты все чаще протекают в информационной сфере, главном образом в глобальной сети Интернет. Разнообразие информационного оружия и информационных атак, особенности появления и применения породили сложнейшие задачи защиты от них. В статье перечислены средства информационного оружия и приведена классификация информационных

атак. Также перечислены самые распространенные информационно-сетевые атаки, такие как Cross-site Scripting, DoS атаки, SQL инъекции и т.д. Классификация информационных атак дает возможность для выбора эффективных средств по обеспечению информационной безопасности и осуществлению соответствующего противодействия противнику в интернет-среде, а также в общей сети обмена информацией.

64. Имамвердиев Я.Н. Приоритетные направления научных исследований по управлению информационной безопасностью электронного государства / **IV научно-техническая конференция «Актуальные проблемы безопасности информационных технологий»,** Красноярск, **10-12 ноября 2010,** с. 52-55.

    Надежное обеспечение информационной безопасности электронного государства (э-государства) требует разработки соответствующего научно-теоретического базиса. Проанализированы различные инициативы по идентификации приоритетных направлений научных направлений и прикладных разработок в области информационной безопасности. Выделены приоритетные проблемы научных исследований по управлению информационной безопасностью э-государства.

65. Имамвердиев Я.Н., Деракшанде С.А. Эталонная модель для управления рисками информационной безопасности / **IV научно-техническая конференция «Актуальные проблемы безопасности информационных технологий»,** Красноярск, **10-12 ноября 2010,** с. 55-58.

    Предлагается подход к формализации задачи управления рисками информационной безопасности на основе подходов систем управления бизнес-процессами и информационными технологиями.

66. Imamverdiyev Y.N., Derakshandeh S.A. Processing of information security risks with ordered weighted averaging operators / **Proceedings of the Third International Conference "Problems of Cybernetics and Informatics".** Baku, **6-8 September 2010,** vol.1, pp. 132-134.

    One of the processing mechanisms of information security risks is reducton of risks by using correct selection of counter-measures against threats.

67. Imamverdiyev Y.N. Architecture of e-government information security management system / **Proceedings of the Third International Conference "Problems of Cybernetics and Informatics",** Baku, **6-8 September 2010,** vol. 1, pp. 79-82.

    The main object of the research is the information security of e-government; therefore exact definition of e-government term is

important. The point is that "electronic state" definition is often identified with "electronic government" term. Besides, often "state" and "government administration institutions" definitions are used in the same meaning.

68. Kazimov T.H., Mahmudova Sh.J. Methods of improvement of efficiency in recognition identification systems / **Proceedings of the Third International Conference "Problems of Cybernetics and Informatics",** Baku, **6-8 September 2010**, vol. 1, pp. 322-325.

    "Recognition" automated identification system prepared on proposed algorithm can be used during control of identifications cards (passports, driving licences), information security (sending requests to computers, data bases, etc), observing criminal events, as well as banks etc.

69. Mahmudov R.Ş. İnternetin tənzimlənməsi metodlarının bəzi aspektləri haqqında // **İnformasiya Cəmiyyəti Problemləri, 2011,** № 1, s. 47-55.

    Məqalədə İnternetin tənzimlənməsi metodları araşdırılır. O cümlədən yanaşma, rəhbər prinsiplər, analogiyalar kimi təsnif edilən tənzimləmə metodlarının ayrı-ayrı formaları analiz edilir. Hər bir metodun tətbiqinin üstün və çatışmayan cəhətləri göstərilir.

70. Əliquliyev R.M., İmamverdiyev Y.N., Yusifov F.F. Cəmiyyətin informasiya təhlükəsizliyinə dair bəzi konseptual baxışlar // **İnformasiya Cəmiyyəti Problemləri, 2011**, № 2, s. 3-9.

İnformasiya təhlükəsizliyinin təmin olunması üzrə beynəlxalq təcrübədə mövcud olan mexanizmlər tədqiq olunmuş, bu sahədə milli normativ-hüquqi bazanın formalaşdırılması istiqamətində görülən işlər araşdırılmış və təkliflər verilmişdir. Cəmiyyətin təhlükəsizliyinin mühüm komponenti kimi informasiya təhlükəsizliyinin vəzifələri müəyyənləşdirilmiş, mövcud təhlükələr və onların hədəfləri araşdırılmış, cəmiyyətin informasiya təhlükəsizliyinin təmin olunmasına dair təklif və tövsiyələr verilmişdir.

71. Ələkbərova İ.Y. Kompüter şəbəkəsində informasiya hücumları və onların reallaşdırılması mexanizmləri // **İnformasiya Cəmiyyəti Problemləri, 2011,** № 1, s. 69-80.
Məqalədə kompüter şəbəkəsində informasiya hücumları problemlərinə baxılmış, hücumların həyata keçirilməsi üsulları tədqiq edilmişdir. İnformasiya hücumlarının təsnifatı aparılmış, həmçinin hücumlarda istifadə olunan proqram vasitələri təsnif edilmiş, onların kompüter şəbəkəsində fəaliyyəti araşdırılmışdır.
72. Алгулиев Р.М., Махмудова Р.Ш., Махмудов Р.Ш. Вопросы защиты детей школьного возраста от интернет-зависимости // **Дистанционное и виртуальное обучение, 2011,** № 5, с. 97-107.
В статье исследуется опасность, создаваемая интернетом для детей школьного возраста. В числе этих опасностей особо указывается проблема интернет-зависимости и ее последствия. Также исследуется

международная практика в сфере борьбы с этой проблемой. Выдвигаются предложения по защите школьников от вредного воздействия глобальной сети и интернет-зависимости.

73. Имамвердиев Я.Н., Деракшанде С.А. Нечеткая OWA-модель для управления рисками информационной безопасности // **Автоматика и вычислительная техника, 2011,** № 1, с. 30-42.

    Одним из методов обработки рисков информационной безопасности является обоснованный выбор и реализация контрмер против угроз. В работе предложена ситуативная нечеткая OWA-модель многокритериальной задачи принятия решения о выборе контрмер для уменьшения рисков информационной безопасности. Предложенная модель позволяет модифицировать ассоциированные веса критериев на основе энтропии информации относительно ситуации агрегации. Кроме того, преимуществом модели является непрерывное улучшение весов критериев и агрегация мнений экспертов в зависимости от параметра, характеризующего ситуацию агрегации.

74. Имамвердиев Я.Н., Деракшанде С.А. Сервис-ориентированная эталонная модель для управления рисками информационной безопасности // **Информационные технологии, 2011,** № 3, с. 35-41.

Предлагается подход к формализации задачи управления рисками информационной безопасности на основе процессной и сервис-ориентированной моделей систем управления бизнес-процессами и информационными технологиями.

75. Имамвердиев Я.Н., Гамзаев Р.Ф. Создание CERT-команды для научной компьютерной сети AzScienceNet // **İnformasiya Cəmiyyəti Problemləri, 2011,** № 1, с. 15-26.

    Реагирование на инциденты является важным аспектом управления информационной безопасностью. В этой работе описывается методология создания команды AZ-CERT для научной компьютерной сети AzScienceNet. Дается обзор нормативных и научно-методических документов в области управления инцидентами, обосновывается выбор организационной структуры и набора услуг для команды AZ-CERT, предлагается модель поэтапного создания CERT-команды. Приводится также описание общего процесса реагирования на инциденты в сети AzScienceNet и технической инфраструктуры AZ-CERT.

76. Рагимов Э.Р. Квалиметрические показатели безопасности программных комплексов, реализующих систему управления корпоративными сетями // **İnformasiya Texnologiyaları Problemləri, 2011,** №1, с.18-23.

Статья посвящена вопросам определения квалиметрических показателей безопасности программных комплексов, которые выполняют основную роль системы управления корпоративными сетями. С помощью определения качественных характеристик показана возможность выявления первичных элементов безопасности. На основе данного подхода был разработан механизм выявления надежности квалиметрических данных безопасности программного комплекса.

77. Рагимов Э.Р. Модель идентификации безотказной работы программных средств в корпоративных сетях // **Телекоммуникации, 2011,** № 2, с. 2-5.

    В данной работе рассмотрены механизмы существования недостатков во внутренних архитектурах программных средств, функционирующих в рамках единой политики безопасности корпоративной сети. Описаны возможные сложности поиска недостатков в программных средствах. Предложена аналитическая модель оценки безотказной работы программных средств в целях определения их безопасности.

78. Рагимов Э.Р. Роль программных комплексов в управлении безопасностью корпоративной информационной системы // **Телекоммуникации, 2011,** № 12, с. 4-7.

    В статье на примере системы управления взаимодействием с клиентами рассмотрен рабочий

механизм корпоративных информационных систем и программных комплексов, реализующих безопасность данной системы. Для достижения поставленной цели были изучены организационно-технические показатели безопасности корпоративной информационной системы. Далее на основе теорий нечетких чисел и функций принадлежности была разработана модель выявления роли программного комплекса в управлении безопасностью корпоративной информационной системы.

79. Alguliyev R.M., Imamverdiyev Y.N., Yusifov F.F. Some conceptual views on information security of the society / **The 5th International Conference on Application of Information and Communication Technologies Conference Proceedings,** Baku, **12-14 October 2011,** pp.150-153.

    Mechanisms existing in the international practice on ensuring information security were studied, the work done in the direction of formation of a national legal and regulatory base in this area was investigated and proposals were put forward. As a key component of security of the society, duties of information security were specified, existing threats and their targets were investigated, proposals and recommendations to ensure information security of the society were given.

80. Əliquliyev R.M., İmamverdiyev Y.N. **İnformasiya təhlükəsizliyi insidentləri.** Bakı, **"**İnformasiya Texnologiyaları" nəşriyyatı**, 2012**, 219 s.
Kitabda informasiya təhlükəsizliyi insidentlərini cavablandırma komandalarının təşkilinə və fəaliyyətinə müasir yanaşmalar öz əksini tapmışdır.
81. İmamverdiyev Y.N. E-dövlətin informasiya təhlükəsizliyinin idarə edilməsi üzrə tədqiqatların müasir vəziyyətinin analizi // **İnformasiya Cəmiyyəti Problemləri, 2012,** № 2, s. 19-26.
E-dövlət mühitində informasiya təhlükəsizliyinin təmin edilməsi və fərdi məlumatların qorunması e-dövlət texnologiyasının əsas problemləridir. E-dövlətin e-xidmətləri inkişaf etdikcə və genişləndikcə bu problemlər daha kəskin xarakter alır. Etibarlı informasiya təhlükəsizliyinin təmin edilməsi sistematik yanaşma, şəraitə adekvat və çevik idarəetmə modelləri tələb edir. Bu məqalədə e-dövlətin informasiya təhlükəsizliyinin idarə edilməsi sahəsində elmi tədqiqatların müasir vəziyyəti analiz edilir və aktual tədqiqat problemləri seçilir.
82. İmamverdiyev Y.N., Nəbiyev B.R. Presedentlər nəzəriyyəsi əsasında şəbəkə təhlükəsizliyinin monitorinqi üzrə qərarların qəbulu metodu // **İnformasiya Texnologiyaları Problemləri, 2012,** №2, s.53-58.

Kompüter şəbəkələrinin təhlükəsizliyi sistemlərində hadisələr haqqında sensorlardan daxil olan məlumatların emalından sonra insident kimi təsnif edilmiş hadisələrin sonrakı emalı haqqında qərarların avtomatik qəbul edilməsi mühüm praktiki əhəmiyyət daşıyır. Məqalədə şəbəkə təhlükəsizliyinin monitorinqi sistemlərində presedentlər nəzəriyyəsi əsasında qərarların qəbul edilməsi metodu təklif edilir. Təklif edilmiş yanaşmada insanın iştirakı minimaldır, presedentlərin müxtəlif yaxınlıq ölçülərinin qəbul edilmiş qərarlara təsiri də analiz edilir.

83. Рагимов Э.Р. Методология оптимальной идентификации расположения программных единиц в комплексе безопасных программ, реализующих систему защиты информации корпоративной сети // **Вопросы защиты информации, 2012,** № 1, с. 51-56.

Проанализированы априорные аспекты оптимального распределения безопасного программного обеспечения в рамках системы защиты информации корпоративной сети, функционирующей на основе единой политики безопасности. Для достижения поставленной цели были рассмотрены возможные пути и механизмы оценки уровня функциональности, а также квалиметрические показатели безопасности управления производительностью программных единиц в составе комплекса безопасных программ. Для создания полной структуры оптимального распределения безопасного программного

обеспечения в рамках системы защиты информации корпоративной сети предложена методология идентификации расположения программных единиц в комплексе безопасных программ

84. Alguliyev R.M., Imamverdiyev Y.N., Yusifov F.F. Some Conceptual Views on Information Security of the Society **// Journal of Communication and Computer, 2012,** no. 6, vol. 9, pp. 644-648.

    Mechanisms existing in the international practice on ensuring information security were studied, the work done in the direction of formation of a national legal and regulatory base in the area was investigated and proposals were put forward. As a key component of security of the society, duties of information security were specified, existing threats and their targets were investigated, proposals and recommendations to ensure information security were given.

85. Alguliyev R.M., Nazirova S.H. Two Approaches on Implementation of CBR and CRM Technologies to the Spam Filtering **// Journal of Information Security, 2012,** vol. 3, no. 1, pp. 11-17.

    Recently the number of undesirable messages coming to e-mail has strongly increased. As spam has changeable character the anti-spam systems should be trainable and dynamical. The machine learning technology is successfully applied in a filtration of e-mail from undesirable messages for a long time. In this paper it is offered to apply Case Based Reasoning

technology to a spam filtering problem. The possibility of continuous updating of spam templates base on the bases of which new coming spam messages are compared, will raise efficiency of a filtration. Changing a combination of conditions it is possible to construct flexible filtration system adapted for different users or corporations. Also in this paper it is considered the second approach as implementation of CRM technology to spam filtration which is not applied to this area yet.

86. Abdullayeva F.C. Cloud computing mühitində təhlükəsizlik problemlərinin analizi / **"Riyaziyyatın tətbiqi məsələləri və yeni informasiya texnologiyaları" II Respublika elmi konfransı,** Sumqayıt, **27-28 noyabr 2012,** s. 160-162.

    Cloud computing informasiya əsrində meydana çıxan yeni terminlərdən biridir. Terminin yeni olmasına baxmayaraq onun konsepsiyası utilitar kompyutinq, qrid kompyutinq, servisyönümlü arxitektur, virtuallaşma, web 2.0 texnologiyaları üzərində qurulub və bu texnologiyaların funksiyalarını özündə əks etdirir.

87. Alguliyev R.M., Imamverdiyev Y.N., Aliyev E.R. Conceptual architecture of national information Space Security System of Azerbaijan / **IV International Conference "Problems of cybernetics and informatics"**, Baku, **12-14 September 2012**, vol. 1, pp. 7-10.

The provision of security in the national electronic information space (national e-space) is a complicated and complex problem. It requires an application of a unified state policy, the balance of the interests, formation of hierarchical registry of information resources, specification and distribution of executors' authority working for information security, the unification of security procedures, structured approach, "divide et impera" and other vital principles. The architecture of the security system (SS) of nature e-space shall be determined for the development of complex action program, and security objects (what?), security procedures (how?), the subjects ensuring the execution of these procedures (who?) shall be identified. The study offers the constituent classification of 3 stability sides ("What, How, Who") of SS architectural components, and3D matrix form (4D matrix – by adding time and cause and result dependencies - "when?") which is the synthesis of tables indicating mutual relations between them – "objects &procedures", "objects & subjects", "subjects & procedures".

88. Ağayev B.S., Əliyeva K.T. Elektron tullantılar və məlumat daşıyıcılarının informasiya təhlükəsizliyinin bəzi aspektləri // **İnformasiya Cəmiyyəti Problemləri, 2013,** № 1, s. 67-74.

Məqalədə elektron tullantıların texnoloji emal tsikli mərhələlərində informasiya təhlükəsizliyi problemləri araşdırılır. Elektron və elektrik avadanlıqlarının informasiya

daşıyıcılarının utilizasiyası və zərərsizləşdirilməsi prosesində müxtəlif dərəcəli sirli informasiyanın təhlükəsizliyi və qorunması problemləri tədqiq edilir.

89. Əliquliyev R.M., Abdullayeva F.C. Bulud texnologiyalarında inam məsələlərinin analizi // **İnformasiya Texnologiyaları Problemləri, 2013,** №2, s.3-9.

    Təqdim olunan işdə bulud texnologiyalarının təhlükəsizlik problemləri sırasında mühüm məsələ olan inam məsələləri araşdırılır. Bunun üçün müxtəlif elm sahələri tərəfindən öyrənilmiş inam anlayışına aydınlıq gətirilir, bulud texnologiyaları üçün aktual olan reputasiya tipli inamın yaradılması texnologiyaları, buludların şəffaflığının təmin edilməsinə yanaşmalar, inamın servis səviyyəsi müqaviləsinə əsasən qurulması üsulları, "inam servis kimi" xidmətləri araşdırılır.

90. Əliquliyev R.M., Mahmudov R.Ş. İnformasiya iqtisadiyyatının təhlükəsizliyinin təmin edilməsi məsələləri // **İnformasiya Cəmiyyəti Problemləri, 2013,** № 1, s. 3-13.

    Məqalədə informasiya iqtisadiyyatının təhlükəsizliyinin təmin edilməsi məsələləri araşdırılır. İqtisadiyyatda informasiya təhlükəsizliyinin artan rolu göstərilir. İqtisadi təhlükəsizliyin mühüm istiqamətləri olan infrastruktur, istehsal, maliyyə və sosial təhlükəsizliyinin təmin edilməsi məsələləri informasiya təhlükəsizliyi kontekstində analiz edilir. İnformasiya

iqtisadiyyatının təhlükəsizliyinin təmin edilməsi ilə bağlı təkliflər irəli sürülür.

91. Əliquliyev R.M., Mahmudova R.Ş. Fərdlərin informasiya mədəniyyəti indikatorlarının işlənməsi // **İnformasiya Cəmiyyəti Problemləri, 2013,** № 2, s. 3-12.

    İnsanlarda informasiyanın əldə olunması, emalı, tətbiq olunması və s. ilə bağlı bilik və bacarıqların formalaşdırılması informasiya cəmiyyəti quruculuğunun vacib aspektlərindən biridir. İnformasiya mədəniyyəti və onun strukturu ilə bağlı müxtəlif yanaşmalar mövcuddur. Məqalədə bu yanaşmalar təhlil edilmiş, beynəlxalq təşkilatlar tərəfindən informasiya mədəniyyətinin formalaşdırılması istiqamətində aparılan işlər araşdırılmışdır. Şəxsiyyətin informasiya mədəniyyətinə informasiyanın qəbulu, yadda saxlanılması, emalı, təhlükəsizliyi və təqdim edilməsi mədəniyyətlərinin məcmusu kimi baxılmış və həmin struktura uyğun indikatorlar təklif edilmişdir.

92. Əliyev E.A. Korporativ informasiya sistemlərində informasiya təhlükəsizliyinin menecmenti üçün təhlükəsizlik tələblərinin təsnifi modeli // **İnformasiya Cəmiyyəti Problemləri, 2013**, № 2, s. 67-76.

    Tədqiqat işində korporativ informasiya sistemlərində informasiya təhlükəsizliyinin idarə edilməsi üçün informasiya təhlükəsizliyi tələblərinin sistemli müəyyənləşdirilməsi məqsədi ilə təsnifat modeli işlənilmişdir. Modelin təməl yaradan elementləri - təhlükəsizlik tələblərinin hədəfləri kimi

informasiya sisteminə aid olan obyektlər, proseslər və subyektlər ("insan faktoru") qəbul edilir və onlar üçün təsnifat modeli təklif edilir, təhlükəsizlik tələblərinin, bu tələblərlə bağlı olan mümkün risklərin, bu risklərə adekvat olan əks-vasitələrin təsnifatlarının uzlaşdırılması və birləşmiş reyestrin yaradılması üçün ümumi platforma müəyyən edilir.

93. İmamverdiyev Y.N. E-dövlətin informasiya təhlükəsizliyinin idarə edilməsinin konseptual modeli // **İnformasiya Cəmiyyəti Problemləri, 2013,** № 1, s. 20-31

E-dövlətin informasiya təhlükəsizliyinin idarə edilməsi çətin formallaşdırılan mürəkkəb məsələdir. Belə məsələlərin həllində ilkin mərhələ kimi konseptual modelin qurulması çox faydalıdır. Bu işdə e-dövlətin informasiya təhlükəsizliyinin idarə edilməsinin konseptual modeli təklif edilir. Konseptual modeldə e-dövlətin informasiya təhlükəsizliyinin əsas anlayışları, e-dövlətin informasiya təhlükəsizliyinin idarə edilməsinin məqsədləri, predmeti, obyektləri, subyektləri, əsas idarəetmə funksiyaları, ətraf və daxili mühitin e-dövlətin informasiya təhlükəsizliyinə təsir edən əsas faktorları müəyyən edilir.

94. İmamverdiyev Y.N. Yeni nəsil milli kibertəhlükəsizlik strategiyaları // **İnformasiya Cəmiyyəti Problemləri, 2013,** № 2, s. 42-51.

Müasir dövrdə kibertəhlükəsizlik cəmiyyətin bütün səviyyələrinə təsir edən strateji milli məsələyə çevrilir. Kibertəhdidlərə qarşı çevik, operativ və effektli mübarizə

müəyyən zaman müddətində əldə edilməli olan milli hədəflərin və prioritetlərin, maraqlı tərəflərin rollarının və məsuliyyətinin düzgün müəyyən edilməsini tələb edir. Kibertəhlükəsizlik üzrə milli strategiya bu yolda ilk addımdır. Bu işdə milli kibertəhlükəsizlik strategiyalarının işlənilməsi sahəsində ən yaxşı təcrübənin aşkarlanması məqsədi ilə mövcud milli kibertəhlükəsizlik strategiyaları analiz edilir.

95. İmamverdiyev Y.N., Tarverdiyev L.Ə. Veb təhlükəsizliyin qiymətləndirilməsi metodlarının analizi // **İnformasiya Texnologiyaları Problemləri, 2013,** №2, s.23-32.

    Veb texnologiyalar e-dövlət xidmətlərinin göstərilməsi, biznesin həyata keçirilməsi, sosial şəbəkə və sosial media vasitəsi kimi geniş yayılmışdır. Lakin Veb texnologiya özü ilə birlikdə bir sıra informasiya təhlükəsizliyi problemləri də gətirir və veb sistemləri bədniyyətlilərin cəlbedici hədəfinə çevirir. Bu məqalədə veb təhlükəsizliyin komponentləri, veb təhlükəsizliyin qiymətləndirilməsinə mövcud metodoloji yanaşmalar, veb-tətbiqlərdə boşluqların aşkarlanması üzrə metodlar və veb-saytların reputasiya sistemləri analiz edilir.

96. Mahmudova R.Ş. Cəmiyyətdə informasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması məsələləri haqqında // **İnformasiya Cəmiyyəti Problemləri, 2013,** № 1, s. 32-38.

    Müasir dövrdə mövcud olan informasiya təhlükələri və onların insanın mənəvi-psixoloji sağlamlığına neqativ təsirləri

araşdırılmışdır. Cəmiyyətdə informasiya təhlükəsizliyi mədəniyyətinin formalaşdırılmasına dair təkliflər verilmişdir.

97. Şıxəliyev R.H., Yunusov T.E. Kompüter sistemlərinin təhlükəsizliyinin qiymətləndirilməsi metodları // **İnformasiya Texnologiyaları Problemləri, 2013,** №1, s.74-80.

    Məqalə kompüter sistemlərinin təhlükəsizliyinin qiymətləndirilməsinə həsr edilmişdir. Məqalədə kompüter sistemlərinin təhlükəsizliyinin qiymətləndirilməsinin bəzi standart və metodları, o cümlədən Ümumi Meyarlar Standartı, sistemin zəiflik indeksi, çoxpilləli hücum modelləşdirilməsi, hücumun aşkarlanması metodları analiz edilmiş və mövcud problemlər müəyyən edilmişdir. Həmçinin kompüter sistemlərinin təhlükəsizliyin qiymətləndirilməsinə əsas yanaşmalar və qiymətləndirmə metrikaları analiz edilmişdir.

98. Yusifov F.F. Loq-faylların analizi əsasında informasiya təhlükəsizliyinin təmin edilməsi // **İnformasiya Texnologiyaları Problemləri, 2013**, № 1, s. 31-37.

    İnformasiya təhlükəsizliyinin təmin olunmasına dair beynəlxalq təcrübədə mövcud olan normativ-hüquqi bazalar və mexanizmlər tədqiq olunmuşdur. Cəmiyyətin təhlükəsizliyinin vəzifələri müəyyənləşdirilmiş, mövcud təhlükələr və onların hədəfləri araşdırılmış, loq-faylların analizi əsasında informasiya təhlükəsizliyinin təmin olunmasına dair metodlar təklif olunmuşdur.

99. Алыгулиев Р.М. Роль технологии интеллектуального анализа текстов в обеспечении национальной безопасности // **İnformasiya Texnologiyaları Problemləri, 2013,** № 1, s.38-43.

В статье дана краткая информация о целях, задачах и областях применения технологии интеллектуального анализа текстов (Text mining). В частности, проанализирована роль технологии Text Mining в области национальной безопасности и указаны перспективные направления исследований в данной области.

100. Abdullayeva F.C. Bulud texnologiyalarında indentifikasiya federasiyasının dinamik idarəetmə modeli / **İnformasiya təhlükəsizliyi problemləri üzrə I respublika elmi-praktiki konfransı**, Bakı, **17-18 may 2013**, s. 105-108.

İstifadəçilərin identifikasiya məlumatlarının federasiyasının dinamik idarə edilməsini təmin edən model təklif olunmuşdur. Tədqiqat prosesində vahid giriş texnologiyalarının və federativ mexanizminin iş prinsipi öyrənilmişdir, mövcud vəziyyəti araşdırılmışdır. Multiagent sistemləri və qərarların qəbulu yanaşmalarını tətbiq etməklə, indentifikasiya məlumatlarının federasiyasının dinamikliyi təmin olunmuşdur.

101. Abdullayeva F.C. Fərdi məlumatların Wikileaks-yönümlü sosial mühitlərə sızma risklərinin idarə olunması / **İnformasiya təhlükəsizliyi problemləri üzrə**

I respublika elmi-praktiki konfransı, Bakı, **17-18 may 2013,** s. 75-78.

Məqalə fərdi məlumatların sızma problemlərinin müasir vəziyyəti analiz olunur. Sızmaya bilavasitə təsir edən insayderlərin təşkilat daxilində hüquqi tənzimlənməsi yollarının beynəlxalq təcrübəsi araşdırılır. Fərdi məlumatların sızma məkanı olan Wikileaks saytının əsas prinsipləri tədqiq olunur. Mövcud sızma risklərinin azaldılması üçün təşkilatın informasiya təhlükəsizliyini idarə edən mükəmməl infrastrukturun qurulması istiqamətində bir sıra tövsiyələr verilir.

102. Ağayev B.S., Əliyeva K.T. Elektron tullantılar problemi və informasiya təhlükəsizliyi / **İnformasiya təhlükəsizliyi problemləri üzrə I respublika elmi-praktiki konfransı,** Bakı, **7-18 may 2013,** s. 145-148.

Məqalədə elektron tullantıların texnoloji emal tsikli mərhələsində informasiya təhlükəsizliyi problemləri araşdırılır. Elektron və elektrik avadanlıqlarının, informasiya daşıyıcılarının utilizasiyası və zərərsizləşdirilməsi prosesində müxtəlif dərəcəli sirli informasiyanın təhlükəsizliyi və qorunması problemləri tədqiq edilir.

103. Ələkbərov R.Q. AzSienceNet elm kompüter şəbəkəsinin informasiya təhlükəsizliyi siyasəti haqqında / **İnformasiya təhlükəsizliyi problemləri üzrə I respublika elmi-praktiki konfransı,** Bakı, **17-18 may 2013,** s. 126-127.

Məqalədə AzSienceNet şəbəkəsinin informasiya təhlükəsizliyi siyasətinin yaradılması qaydalarından bəhs edilir. Yaradılan informasiya təhlükəsizliyi siyasəti AzSienceNet şəbəkəsində informasiya təhlükəsizliyinin təmin edilməsi probleminə baxışlar sistemini müəyyən edir, informasiya təhlükəsizliyinin məqsəd və vəzifələrini, təşkilati, texnoloji və prosedur aspektlərini sistemləşdirilmiş şəkildə şərh edir.

104. Ələkbərov R.Q., Həşimov M.A., Mustafayev T.İ. AzScienceNet şəbəkəsində Cloud computing xidmətinin təhlükəsizlik məsələləri və həlli yolları / **İnformasiya təhlükəsizliyi problemləri üzrə I respublika elmi-praktiki konfransı,** Bakı, **17-18 may 2013,** s. 131-133.

Məqalədə hesablama buludları texnologiyaları əsasında paylanmış hesablama sistemlərinin yaradılması prinsipləri, AzScienceNet şəbəkəsində cloud və virtual resurslardan istifadə zamanı meydana çıxan təhlükəsizlik problemləri və onların həlli yolları analiz olunmuşdur.

105. Ələkbərova İ.Y. İnformasiya bolluğu informasiya müharibəsinə qarşı bir vasitə kimi / **İnformasiya təhlükəsizliyi problemləri üzrə I respublika elmi-praktiki konfransı,** Bakı, **17-18 may 2013**, s.56-59.

Məqalədə informasiya müharibəsi texnologiyalarının yaranması və inkişafının səbəbləri göstərilmiş, bununla əlaqədar meydana çıxan problemlər tədqiq edilmişdir. İnformasiya təsiri problemləri analiz edilmiş və hədəflər göstərilmişdir. Həmçinin, İnternet mühitində informasiya

boşluğunun informasiya təhlükəsizliyinin təmin edilməsində rolu araşdırılmışdır.

106. Əliquliyev R.M., Kazımov S.Ş. E-dövlətin informasiya təhlükəsizliyi indikatorları / **İnformasiya təhlükəsizliyi problemləri üzrə I respublika elmi-praktiki konfransı,** Bakı, **17-18 may 2013**, s. 89-91.

E-dövlətin informasiya resurslarının qorunması, etibarlı informasiya mübadiləsi və informasiya təhlükəsizliyi məsələləri informasiya cəmiyyətinin formalaşmasının vacib komponentlərindəndir. E-dövlətin formalaşması və inkişaf mərhələləri zamanı onun ölçülməsi, monitoriqinin aparılması e-dövlət quruculuğunun ən əsas məsələlərindən biridir. İnformasiya təhlükəsizliyinin ölçülməsinin də bu prosesdə özünəməxsus çəkisi vardır. Məqalə e-dövlətin informasiya təhlükəsizliyi məsələlərinin nəzəri-metodoloji tərəflərinə baxılmışdır, e-dövlətin formalaşması proseslərin ölçülməsi zamanı informasiya təhlükəsizliyini xarakterizə edən beş baza indikatoru, həmçinin bu baza indikatorlarının əhatə edə biləcəyi sahə indikatorları təklif olunmuşdur.

107. Əliquliyev R.M., Mahmudov R.Ş. İqtisadi təhlükəsizliklə informasiya təhlükəsizliyinin qarşılıqlı əlaqəsi / **İnformasiya təhlükəsizliyi problemləri üzrə I respublika elmi-praktiki konfransı**, Bakı, **17-18 may 2013,** s. 7-10.

Məqalədə iqtisadi təhlükəsizliklə informasiya təhlükəsizliyinin qarşılıqlı əlaqəsi araşdırılır. İnformasiya və biliklərin əsas

iqtisadi resurslara çevrildiyi informasiya iqtisadiyyatında informasiya təhlükəsizliyinin mühüm istiqamətləri olan istehsal, maliyyə və infrastruktur təhlükəsizliyinin təmin edilməsi, eləcə də, intellektual mülkiyyətin, fərqli məlumatların qorunması və iqtisadi cinayətkarlıq məsələləri informasiya təhlükəsizliyi prizmasından analız edilir. İnformasiya iqtisadiyyatının təhlükəsizliyinin təmin edilməsi ilə bağlı təkliflər irəli sürülür.

108. Əliquliyev R.M., Yusifov F.F. İnternet azadlığı məsələsinə iqtisadi baxış / **İnformasiya təhlükəsizliyi problemləri üzrə I respublika elmi-praktiki konfransı,** Bakı, **17-18 may 2013,** s. 26-27.

İnternet azadlığının təmin olunmasına dair mövcud təcrübə araşdırılmış, ona təsir edən amillər və problemlər göstərilmişdir. İnternet azadlığının ölkənin iqtisadi göstəricilərindən asılılığı məsələsi tədqiq edilmiş və bəzi konseptul baxışlar şərh olunmuşdur.

109. Əliyev E.A. E-dövlət mühitində informasiya təhlükəsizliyinin idarə edilməsi problemləri / **İnformasiya təhlükəsizliyi problemləri üzrə I respublika elmi-praktiki konfransı,** Bakı, **17-18 may 2013,** s. 18-21.

İnformasiya təhlükəsizliyinin idarə edilməsi çoxeşolonlu, geniş coğrafiyaya, təsnifatlı məqsəd, prosedur və vəzifələrə, fərqli səlahiyyətli iştirakçılara malik aktual problemdir. Azərbaycan respublikasında bu sahə üçün 1971-ci ildən başlayaraq

müəyyən dayaqlar yaradılmağa başlanılmış, həmin işlər müstəqillik illərində genişlənmişdir. Bu proses 2003-cü ildə Milli Strategiyanın qəbul edilməsindən sonra davamlı inkişaf etdirilir. Həmin milli məkan, həm də korporativ informasiya mühitləri üçün informasiya təhlükəsizliyinin idarə edilməsinə hüquqa əsaslanma, vahid siyasət, proses yanaşması və standartların tətbiqi tələb olunur. Bu tədqiqat işində İSO/İEC-27001 standartına uyğun olaraq informasiya təhlükəsizliyinin idarə edilməsi üzrə vəzifələr və idarəetmənin iştirakçıları identifikasiya olunur, bu vəzifələrin uyğun iştirakçılar arasında bölünməsi, koordinasiyası və digər problemlər qaldırılır. Bəzi problemlər daha qaynar kimi seçilir və onlar üçün həllər təklif edilir.

110. Yusifov F.F. Loq-faylların analizi əsasında informasiya təhlükəsizliyinin təmin edilməsi / **İnformasiya təhlükəsizliyi problemləri üzrə I respublika elmi-praktiki konfransı,** Bakı, **17-18 may 2013,** s. 101-104.
İnformasiya təhlükəsizliyinin təmin olunmasına dair beynəlxalq təcrübədə mövcud olan normativ-hüquqi bazalar və mexanizmlər tədqiq olunmuşdur. Cəmiyyətin təhlükəsizliyinin vəzifələri müəyyənləşdirilmiş, mövcud təhlükələr və onların hədəfləri araşdırılmış, loq-faylların analizi əsasında informasiya təhlükəsizliyinin təmin olunmasına dair metodlar təklif olunmuşdur.

111. Əliyeva G.Ə. Media-analitika və informasiya təhlükəsizliyi / **İnformasiya təhlükəsizliyi problemləri**

üzrə I respublika elmi-praktiki konfransı, Bakı, **17-18 may 2013,** s. 42-43.

Məqalədə medianın cəmiyyətə təsiri, media sahəsində informasiya təhlükəsizliyi problemləri araşdırılmışdır. Medianın uşaq və gənclərə müsbət və mənfi təsirləri göstərilmişdir.

112. İmamverdiyev Y.N. Milli kibertəhlükəsizlik strategiyalarının analizi / **İnformasiya təhlükəsizliyi problemləri üzrə I respublika elmi-praktiki konfransı,** Bakı, **17-18 may 2013,** s. 14-17.

Müasir dövrdə kibertəhlükəsizlik cəmiyyətin bütün səviyyələrinə təsir edən strateji milli məsələyə çevrilir. kibertəhdidlərə qarşı çevik, operativ və effektiv mübarizə müəyyən zaman müddətində əldə edilməli olan hədəflərin və prioritetlərin, maraqlı tərəflərin rollarının və məsuliyyətinin düzgün müəyyən edilməsini tələb edir. Kibertəhlükəsizlik üzrə milli strategiya bu yolda ilk addımdır. Bu işdə milli kibertəhlükəsizlik strategiyalarının işlənilməsi sahəsində ən yaxşı təcrübənin aşkarlanması məqsədi ilə mövcud milli kibertəhlükəsizlik strategiyaları analiz edilir.

113. Əliyev Ə.Q. İnformasiya sistemlərinin təhlükəsizliyinə vurulan ziyanların kompleks qiymətləndirilməsi məsələləri / **İnformasiya təhlükəsizliyi problemləri üzrə I respublika elmi-praktiki konfransı,** Bakı, **17-18 may 2013,** s. 71-74.

İşdə informasiya sistemlərinin təhlükəsizliyinə vurulan ziyanların kompleks qiymətləndirilməsi zamanı meydana çıxan problemlər təhlil olunmuşdur. İnformasiya təhlükəsizliyinə vurulan nisbi ziyanların təsir səviyyəsinin qeyri-səlis qiymətləndirilməsi metodikasının işlənilməsi aspektləri verilmişdir.

114. İmamverdiyev Y.N. İnformasiya təhlükəsizliyinin terminoloji problemləri / **İnformasiya təhlükəsizliyi problemləri üzrə I respublika elmi-praktiki konfransı,** Bakı**, 17-18 may 2013,** s. 38-41.

Terminologiya qloballaşma və sürətli elmi-texnoloji inkişaf şəraitində xüsusi əhəmiyyət daşıyır. İnformasiya təhlükəsizliyi sahəsində terminologiya dinamik dəyişir, anlayışlar aparatının fasiləsiz formalaşması prosesi baş verir. Lakin qloballaşma nəticəsində dünya dillərində terminologiyanın unifikasiyası prosesi də baş verir, milli terminologiya sistemləri "ölüm ya qalım" problemi qarşısında qalır. Bu problem xüsusilə inkişaf etməkdə olan ölkələrdə daha kəskin hiss olunur. Bu işdə informasiya təhlükəsizliyi sahəsində terminşünaslığın aktual problemləri analiz edilir, onların aradan qaldırılması istiqamətində bir sıra tövsiyələr verilir.

115. İmamverdiyev Y.N., Fətəliyev T.X. E-elm mühitində informasiya təhlükəsizliyi problemləri **/ İnformasiya təhlükəsizliyi problemləri üzrə I respublika elmi-praktiki konfransı**, Bakı, **17-18 may 2013**, s. 113-115.

E-elm infrastrukturu paylanmış, heterogen, hər birinin avtonom informasiya təhlükəsizliyi siyasəti olan müxtəlif inzibati domenlərdən ibarətdir. Bu domenlər arasında istifadəçilərin identifikasiyası modelləri analiz edilir, onların üstün və çatışmayan cəhətləri müəyyən edilir.

116. İmamverdiyev Y.N., Həmzəyev R.F. E-dövlətdə CERT-komandaları şəbəkəsinin yaradılması / **İnformasiya təhlükəsizliyi problemləri üzrə I respublika elmi-praktiki konfransı,** Bakı, **17-18 may 2013**, s. 92-95.
E-dövlətdə informasiya təhlükəsizliyi insidentlərinin tezliyi artır və nəticələrinin miqyası genişlənir. CERT-komandaları informasiya təhlükəsizliyi insidentlərin effektiv emalı üçün özünü təsdiqləmiş təşkilatı formalardan biridir. Bu işdə e-dövlət mühitində CERT-komandalarının evolyusiyası, onların fəaliyyətinin əlaqələndirilməsi, vahid iyerarxik infrastrukturda birləşdirilməsi problemləri analiz edilir, kibertəhlükəsizlik təlimlərinin təşkili təcrübəsinə baxılır.

117. İmamverdiyev Y.N., Kang T.W. Əşyaların İnterneti üçün yüngülçəkili kriptoqrafiya / **İnformasiya təhlükəsizliyi problemləri üzrə I respublika elmi-praktiki konfransı,** Bakı, **17-18 may 2013,** s. 137-140.
Əşyaların İnterneti yalnız insanları birləşdirən hazırki İnternetin növbəti inkişaf mərhələsidir və insanları əhatə edən bütün faydalı əşyaların qlobal şəbəkəyə qoşulmasını nəzərdə tutur. Əşyaların İnternetində təhlükəsizlik və gizlilik problemləri olduqca aktualdır və bu problemlərin həllində

yüngülçəkili kriptoqrafiyanın əhəmiyyətli rol oynayacağı gözlənilir. Bu işdə kriptoqrafiyanın yeni istiqaməti olan yüngülçəkili kriptoqrafiyaya yürüdülən tələblər və bu sahədə tədqiqatların müasir vəziyyəti analiz edilir, perspektiv tədqiqat istiqamətləri müəyyən edilir.

118. İmamverdiyev Y.N., Tarverdiyev L.Ə. Veb-saytların təhlükəsizlik boşluqlarının analizi / **İnformasiya təhlükəsizliyi problemləri üzrə I respublika elmi-praktiki konfransı,** Bakı, **17-18 may 2013,** s. 122-125.

Veb-texnologiyalar e-dövlətdə, sosial mediada, mobil platformada, bank tranzaksiyalarında və s. geniş istifadə olunur. Bu səbəbdən də onlar bədniyyətlərin hücum hədəflərinə çevrilir və veb-sistemlərdə informasiya təhlükəsizliyinin təmin olunması olduqca aktualdır. Bu işdə veb-saytların mövcud təhlükəsizlik boşluqlarının avtomatik analizi üzrə eksperimentlər aparılır və həmin analizin nəticələri təqdim olunur.

119. Kazımov T.H., Mahmudova Ş.C. Fotoportretlər əsasında insan sifətinin identifikasiyası sistemi / **İnformasiya təhlükəsizliyi problemləri üzrə I respublika elmi-praktiki konfransı,** Bakı, **17-18 may 2013,** s. 149-150.

Bu məqalədə biometrik texnologiyalar, fotoportretlər üzrə insan sifətinin tanınma sistemləri haqqında məlumat verilmişdir. Məqalədə həmçinin "Tanınma" biometrik identifikasiya sistemi

haqqında məlumat verilmiş və onun digər sistemlərlə müqayisəsi aparılmışdır.

120. Qasımova R.T. Milli domen və kontentlərin xarici serverlərdə yerləşdirilmə səbəbləri və nəticələri / **İnformasiya təhlükəsizliyi problemləri üzrə I respublika elmi-praktiki konfransı,** Bakı, **17-18 may 2013**, s. 52-55.

Məqalədə milli domen adlarının xarici vətəndaşlar tərəfindən alınmasının və milli kontentlərin Azərbaycandan kənarda olan serverlərdə yerləşdirilməsinin aktual problemləri müəyyən olunmuş, onların müasir vəziyyəti analiz edilmişdir. Bu problemlərin həlli üçün müasir informasiya texnologiyalarının yaratdığı imkanlar xarakterizə olunmuş, hostinq xidmətlərin seçilməsi üçün tövsiyələr verilmişdir.

121. Mahmudov R.Ş. İnformasiya təhlükəsizliyinin normativ-hüquqi bazası / **İnformasiya təhlükəsizliyi problemləri üzrə I respublika elmi-praktiki konfransı,** Bakı, **17-18 may 2013**, s. 67-70.

Məqalədə informasiya təhlükəsizliyinin beynəlxalq və milli səviyyələrdə mövcud normativ-hüquqi bazası araşdırılır. O cümlədən informasiya təhlükəsizliyinin hüquqi-ideoloji bazası, informasiyanın əlyetərliyinin, konfidensiallığının, intellektual mülkiyyət hüquqlarının qorunmasının, informasiya texnologiyalarının, informasiya təhlükəsizliyi sahəsində qanun pozuntuları və məsuliyyət məsələlərinin hüquqi əsasları analiz edilir. Azərbaycan informasiya təhlükəsizliyi sahəsində

qanunvericilik bazasının təkmilləşdirilməsinə dair təkliflər irəli sürülür.

122. Mahmudova R.Ş. İnformasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması problemləri / **İnformasiya təhlükəsizliyi problemləri üzrə I respublika elmi-praktiki konfransı,** Bakı, **17-18 may 2013**, s. 22-25.

Müasir dövrdə mövcud olan informasiya təhlükələri və onların insanın mənəvi-psixoloji sağlamlığına neqativ təsirləri araşdırılmışdır. Cəmiyyətdə informasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması üçün təklif və tövsiyələr verilmişdir.

123. Mahmudova R.Ş., Tarverdiyev L.Ə. Uşaq və yeniyetmələrin İnternetin zərərli təsirindən qorunması problemləri / **İnformasiya təhlükəsizliyi problemləri üzrə I respublika elmi-praktiki konfransı,** Bakı, **17-18 may 2013**, s. 46-49.

Məqalə uşaq və yeniyetmələrin İnternetdə təhlükəsizliyinin təmin edilməsi problemlərinə həsr edilib. İnternetin təhlükələri ilə mübarizə sahəsində dünya ölkələrinin təcrübəsi təhlil edilmiş, beynəlxalq təşkilatlar, o cümlədən Avropa Birliyi tərəfindən bu məsələlərin həlli istiqamətində həyata keçirilən tədbirlər araşdırılmışdır. Ölkəmizdə uşaqların İnternetdə təhlükəsiz fəaliyyətinin təmin edilməsinəyönəlik təkliflər verilmişdir.

124. Məmmədov E.Ç. Elektron kitabxanalarda fərdi məlumatların qorunması məsələləri / **İnformasiya təhlükəsizliyi problemləri üzrə I respublika elmi-praktiki konfransı,** Bakı, **17-18 may 2013,** s. 79-82.

Məqalədə informasiya təhlükəsizliyinin tarixinə nəzər salınmış, onun strukturunun və qlobal elektron kitabxanalarda bu məsələnin formalaşması prinsipləri araşdırılmışdır. Həmçinin Azərbaycan elektron kitabxanalarında və ümumilikdə kitabxana-informasiya mühitində informasiya təhlükəsizliyi, fərdi məlumatların qorunması məsələləri, mövcud problemlər analiz edilmiş və müəyyən təkliflər verilmişdir.

125. Nəbiyev B.R. İnformasiya təhlükəsizliyi baxımından kritik vəzifələr üçün tələblər sisteminin formalaşdırılması / **İnformasiya təhlükəsizliyi problemləri üzrə I respublika elmi-praktiki konfransı,** Bakı, **17-18 may 2013,** s. 32-33.

Kompüter şəbəkələrində və sistemlərində baş verən proseslərə təsir göstərən sistem administratorlarının fəaliyyətinin məqsədəuyğun aparılması üçün onların qarşısında tələblər qoyulmalıdır. Bu tələblərin yerinə yetirilməsinə nəzarət edilməsi üçün informasiya təhlükəsizliyi xidmətinin yaradılması mühüm əhəmiyyət daşıyır. Bu prosesin şəffaf olması və kompüter şəbəkələrinin və sistemlərinin iş prossesinə təsir göstərməsi üçün hər iki xidmətə xüsusi tələblər müəyyən olunmalıdır.

126. Nəbiyev B.R. AzScienceNet şəbəkəsində informasiya təhlükəsizliyinin monitorinqi sistemi haqqında / **İnformasiya təhlükəsizliyi problemləri üzrə I respublika elmi-praktiki konfransı,** Bakı, **17-18 may 2013,** s. 128-130.

AzScienceNet elm kompüter şəbəkəsində monitorinq və təhlükəsizlik sistemi vasitəsilə hadisələr haqqında sensorlardan daxil olan məlumatların toplanması, analizi və təsnif edilməsi mühüm praktiki əhəmiyyət daşıyır. Məqalədə şəbəkə təhlükəsizliyinin monitorinqi sahəsində aparat və proqram təminatlıları araşdırılmışdır. Təklif edilmiş yanaşmada AzScienceNet şəbəkəsinə uyğunlaşdırılmış informasiya təhlükəsizliyinin monitorinqi sistemi işlənib hazırlanmışdır.

127. Şıxəliyev R.H., Yunusov T.E. Kompüter sistemlərinin təhlükəsizliyinin qiymətləndirilməsi metodları / **İnformasiya təhlükəsizliyi problemləri üzrə I respublika elmi-praktiki konfransı,** Bakı, **17-18 may 2013,** s.155-158.

Məqalə kompüter sistemlərinin təhlükəsizliyinin qiymətləndirilməsinə həsr edilmişdir. Məqalədə kompüter sistemlərinin təhlükəsizliyinin qiymətləndirilməsinin bəzi standart və metodları, o cümlədən Ümumi Meyarlar Standartı, sistemin zəiflik indeksi, çoxpilləli hücum modelləşdirilməsi, hücumun aşkarlanması metodları analiz edilmiş və mövcud problemlər müəyyən edilmişdir. Həmçinin kompüter

sistemlərinin təhlükəsizliliyin qiymətləndirilməsinə əsas yanaşmalar və qiymətləndirmə metrikaları analiz edilmişdir.

128. Rüstəmov D.Ə. E-dövlət mühitində dövlət sirrinin mühafizəsinin təmin edilməsi problemləri / **İnformasiya təhlükəsizliyi problemləri üzrə I respublika elmi-praktiki konfransı,** Bakı, **17-18 may 2013,** s. 96-97.

Məqalənin məqsədi müxtəlif səviyyələrdə aparılan e-dövlət xidmətlərində İnformasiya Təhlükəsizliyinin İdarə olunması probleminə diqqət yönəltmək və bu problemə beynəlxalq tələblər prizmasından baxışı təmin etməkdir. Azərbaycan Respublikasında e-dövlət quruculuğu sahəsində xeyli işlər görülmüş və ölkəmiz beynəlxalq statistika indeksini hər il yüksəkliyə doğru dəyişir. Lakin informasiya təhlükəsizliyi məsələsi dövlət qurumlarını daim narahat edən məsələ olaraq qalacaqdır. Bu baxımdan da, e-dövlət mühitində informasiya təhlükəsizliyinin idarə edilməsi probleminin elmi ictimaiyyətin müzakirə obyektinə çevrilməsi bu məqalənin əsas məqsədi hesab olunur.

129. Şərifov M.H. Veb-saytlara yürüdülən tələblər və informasiya təhlükəsizliyi / **İnformasiya təhlükəsizliyi problemləri üzrə I respublika elmi-praktiki konfransı,** Bakı, **17-18 may 2013,** s. 119-121.

Veb-in keyfiyyət standartları W3C standartları haqqında ətraflı məlumat verilmişdir. Veb-də informasiya təhlükəsizliyinin təmin olunması üçün təhlükəsizlik standartları təsvir olunmuş və bir sıra tövsiyələr irəli sürülmüşdür.

130. Рустамов Д.А., Рзаев М.Я. Вопросы безопасности государственных информационных ресурсов в кризисных ситуациях / **Труды конференции "Кибербезопасность-2013" (Information Technology and Security),** Киев, **13-17 октября 2013**, №1(3), с.95-98.

Рассмотрены вопросы безопасности государственных информационных ресурсов при различных типах кризисных ситуаций. Известно, что с точки зрения безопасности электронного правительства кризисные ситуации являются основным фактором риска. Рассмотрены международные стандарты в этой области, изучен опыт развитых стран и результаты, полученные ведущими научными центрами. Целью статьи является привлечение внимания органов государственной власти к данному вопросу.

131. Мустафаева Г.Н. Безопасность детей и подростков в сети Интернет / **İnformasiya təhlükəsizliyi problemləri üzrə I respublika elmi-praktiki konfransı,** Bakı, **17-18 may 2013,** с. 50-51.

В данной статье изложены социальные проблемы интернет-зависимости у детей и подростков. Анализируются методы и системы биометрической аутентификации, выявляя особенности по психологии, педагогике, физиологии, эргономике. В дальнейшем проводится классификация по возрастным группам.

132. Кязимов Т.Г., Махмудова Ш.Д. Разработка алгоритма компьютерного распознавания лиц на основе фотопортретов / **I Международная научно-техническая конференция «Информационная безопасность в свете Стратегии Казахстан-2050».** Астана, **12 сентября 2013,** с. 391-400.

Рассматривается алгоритм поиска человека в базе изображений по его фотопортрету. На основе выбранных идентификационных точек лица вычисляются расстояния между ними.

133. Алыгулиев Р.М. Text Mining для приложений национальной безопасности / **İnformasiya təhlükəsizliyi problemləri üzrə I respublika elmi-praktiki konfransı,** Bakı, **17-18 may 2013,** s. 98-100.

В статье дана краткая информация о целях, задачах и областях применения технологии Text Mining. Анализирована роль этой технологии в системах национальной безопасности и указаны перспективные направления исследования в данный области.

134. Alguliyev R.M., Abdullayeva F.C. Identity management based security architecture of cloud computing on Multi-Agent Systems / **Proceedings of 6th International Conference on Information Security and Cryptology**. Turkey, Ankara, **20-21 September 2013,** pp.230-233.

In traditional identity management systems user authentication is usually carried out on the basis of management list, previously defined in a system. But with the increasing number of users in such environment as a cloud the management of this list becomes more difficult. For this purpose, in this paper the model supplying the dynamic management of the users' identity federation was introduced. With the implementation of multi-agent systems and the decision making solutions the identity federation dynamization was ensured.

135. Alguliev R.M., Abdullayeva F.C. Identity management based security architecture of cloud computing on multi-agent systems / **IEEE 3rd International conference on innovative computing technology**, London, **29-31 August 2013,** pp. 123-126.

In traditional identity management systems user authentication is usually carried out on the basis of management list, previously defined in a system. But with the increasing number of users in such environment as a cloud the management of this list becomes more difficult. For this purpose, in this paper the model supplying the dynamic management of the users' identity federation was introduced. With the implementation of multi-agent systems and the decision making solutions the identity federation dynamization was ensured.

136. Imamverdiyev Y.N. An information security incident prioritization method / **7th International Conference on Application of İnformation and Communication Technologies**, Baku, **23-25 October 2013,** pp. 183-187.

Operative response to incidents is an important aspect of information security management. In the modern information systems, each day can be hundreds of information security incidents. Since resources of the incident response teams are limited, simultaneous processing of several incidents requires determination the incident priorities and distribution of resources among them in accordance with priorities. The paper highlights the main factors affecting the priority of information security incidents and proposes a method for prioritizing incidents based on fuzzy analytic hierarchy process.

137. Imamverdiyev Y.N. An application of extreme value theory to e-government information security risk assessment / **7th International conference on Application of İnformation and Communication Technologies**, Baku, **23-25 October 2013,** pp. 349-352.

Existing methods of information security risk management is designed for organizations, generalization of these methods for e-government is problematic (or impossible). In this paper, we propose an approach based on extreme value theory for e-government information security risk assessment.

138. Imamverdiyev Y.N. A hypergame model for information security / **6th International conference on**

information security and cryptology, Turkey, Ankara, **20-21 September 2013,** pp. 65-70.

Game theory is one of the most powerful mathematical tools to model information security decision making. However, in game theory it is assumed that all the players have complete knowledge about each player's strategies, preferences, and decision rules used. In many real world situations, decision makers do not always have all the information about each player's true intentions, strategies or preferences. Since the early developments of game theory attempts have been made to incorporate misperceptions in game models of either incomplete or imperfect information. However, most of these attempts are based on quantities which are too subjective in general. In this paper, we consider a special family of games if incomplete information called hypergames. Hypergame theory extends classical game theory with the ability to deal with the differences in players misperceptions. In the context of hypergames, few works have addressed the study of information security decision making. This paper presents a hypergame approach as an analysis tool in the context of information security. The proposed two level hypergame models defender's and attacker's perception of the information security situation as a series of games.

139. Imamverdiyev Y.N., Shikhaliyev R.H., Kang T.W. Mobile security threats on smart phone / **İnformasiya**

təhlükəsizliyi problemləri üzrə I respublika elmi-praktiki konfransı, Bakı, **17-18 may 2013,** pp. 116-118.

With the widespread use of smart devices and ubiquitous sensors, new mobile security threats are produced. In this paper, we identified mobile security issues in ICT converging environment and security threats due to smart phones and research subjects for mobile security.

140. Abdullayeva F.C. Buludların dinamik federallaşması üçün müştərək risk qiymətləndirilməsi üsulunun işlənməsi // **İnformasiya Texnologiyaları Problemləri, 2014,** № 2, s. 46-58.

Məqalədə buludların dinamik federallaşmasına imkan verən yanaşma təklif edilir. Yanaşma risk qiymətləndirilməsi texnologiyasına əsaslanır və buludların federallaşmasını identifikasiyaların federallaşmasını nəzərə almadan həyata keçirir. Bu problemin həlli üçün ilk öncə buludların informasiya təhlükəsizliyi səviyyəsinə ciddi təsir edə bilən faktorların seçimi aparılır və bu faktorların əsasında iyerarxik risk qiymətləndirilməsi arxitekturu təklif edilir. Sonra analitik iyerarxiyalar prosesi (analytic hierarchy process) metodologiyası tətbiq olunaraq bulud provayderinin risk prioritetləri vektoru formalaşdırılır və bu vektorun əsasında qeyri-səlis məntiqi çıxarış tipli risk qiymətləndirilməsi aparılır.

141. Ələkbərov R.Q., Həşimov M.A., Mustafayev T.İ. Cloud computing xidmətinin təhlükəsizlik məsələləri və onların

həlli yolları // **İnformasiya Texnologiyaları Problemləri, 2014,** № 2, s. 33-39.

Məqalədə cloud computing texnologiyaları əsasında paylanmış hesablama sistemlərinin yaradılması prinsipləri müəyyən edilmiş, AzScienceNet şəbəkəsində bulud və virtual resurslardan istifadə zamanı meydana çıxan təhlükəsizlik problemləri və onların həlli yolları analiz olunmuşdur.

142. Əliquliyev R.M., Yusifov F.F. Elektron dövlətin formalaşmasının bəzi aktual elmi-nəzəri problemləri və həll perspektivləri // **İnformasiya Cəmiyyəti Problemləri, 2014,** № 2, s. 3-13.

Beynəlxalq təcrübə nəzərə alınmaqla, elektron dövlətin formalaşdırılmasının konseptual və arxitektur əsasları tədqiq olunmuş və bəzi təkliflər verilmişdir. Elektron dövlətin formalaşması proseslərinin ölçülməsi və monitorinqi, veb-resursların intellektual analizi, informasiya təhlükəsizliyinin təmin olunması, elektron demokratiya və elektron vətəndaş problemləri araşdırılmış, konseptual yanaşmalar təklif olunmuşdur. Elektron dövlət nəzəriyyəsinin əsas prinsipləri nəzərə alınmaqla mühüm tədqiqat istiqamətləri müəyyən edilmişdir.

143. İmamverdiyev Y.N. İnformasiya təhlükəsizliyinin terminoloji problemləri // **İnformasiya Cəmiyyəti Problemləri, 2014,** № 1, s. 43-49.

Terminologiya qloballaşma və sürətli elmi-texnoloji inkişaf şəraitində xüsusi əhəmiyyət daşıyır. İnformasiya təhlükəsizliyi

sahəsində terminologiya dinamik dəyişir, anlayışlar aparatının fasiləsiz formalaşması prosesi baş verir. Lakin qloballaşma nəticəsində dünya dillərində terminologiyanın unifikasiyası prosesi də baş verir, milli terminologiya sistemləri "ölüm, ya qalım" problemi qarşısında qalır. Bu problem xüsusilə inkişaf etməkdə olan ölkələrdə daha kəskin hiss olunur. Bu işdə informasiya təhlükəsizliyi sahəsində terminşünaslığın aktual problemləri analiz edilir, onların aradan qaldırılması istiqamətində bir sıra tövsiyələr verilir.

144. İmamverdiyev Y.N. E-dövlətin informasiya təhlükəsizliyi üzrə koordinasiya problemləri // **İnformasiya Cəmiyyəti Problemləri, 2014,** № 2, s. 24-30.
Müasir şəraitdə e-dövlətin informasiya təhlükəsizliyini yalnız bütün maraqlı tərəflərin – dövlətin, biznes sektorunun, vətəndaş cəmiyyəti institutlarının və vətəndaşların səylərini koordinasiya etməklə təmin etmək mümkündür. Bu məqalədə e-dövlətin informasiya təhlükəsizliyi sahəsində koordinasiya üçün konseptual model təklif edilir, aktual koordinasiya problemləri analiz edilir və onların aradan qaldırılması istiqamətində bir sıra tövsiyələr verilir.

145. Yunusov T.E. Kompüter sistemlərinin təhlükəsizliyinin qiymətləndirilməsi xüsusiyyətləri // **İnformasiya Texnologiyaları Problemləri, 2014,** № 1, s. 104-108.
Məqalədə kompüter sistemlərinin təhlükəsizliyinə olan təhdidlər, texniki vasitələrin zəiflikləri, qərəzli yaradılan proqram səhvləri, hücumlar üçün istifadə olunan üsullar,

insan faktoru kimi zəifliklər analiz edilmişdir. Həmçinin, təhlükəsizliyin qiymətləndirilməsi üçün taksonomiyalar və onların xüsusiyyətləri analiz edilmişdir.

146. Имамвердиев Я.Н. Модель GM (1, 1)-Маркова для прогнозирования уязвимостей программного обеспечения // **İnformasiya Texnologiyaları Problemləri, 2014,** № 1, s. 26-37.

Прогнозирование количества уязвимостей программного обеспечения важно для оценки рисков информационной безопасности и планирования ресурсов для быстрого устранения уязвимостей. В работе предложена модель GM (1, 1)-Маркова для прогнозирования количества уязвимостей программного обеспечения. Предложенная модель тестирована для операционной системы Microsoft XP с использованием общедоступной базы данных по уязвимостям NVD (National Vulnerability Database).

147. Имамвердиев Я.Н. Модель ситуационного управления информационной безопасностью электронного правительства // **Информационные технологии, 2014**, № 8, с. 24-33.

Для надежного обеспечения информационной безопасности электронного правительства необходимо непрерывно и автоматически идентифицировать сложные динамические ситуации и реагировать на них в реальном времени. Разработана концептуальная модель ситуационного управления информационной

безопасностью электронного правительства и предлагается ее реализация на основе теории прецедентов. Предложены подходы для представления знаний о ситуации информационной безопасности и выбора прецедентов, а также оптимизации весов признаков прецедентов на основе метода роя частиц. Предложенный подход можно обобщить для тактического и стратегического уровней управления.

148. Шыхалиев Р.Г. Об одном методе классификации трафика компьютерных сетей // **İnformasiya Texnologiyaları Problemləri, 2014,** № 2, с. 59-67.

Точная классификация трафика компьютерных сетей необходима для их эффективного управления, мониторинга и обеспечения безопасности. В статье для классификации трафика компьютерных сетей предлагается использовать алгоритмы машинного обучения с учителем и поиска ассоциативных правил. Предложенный метод классификации трафика позволит повысить производительность и точность классификации даже при небольших обучающих выборках.

149. Alguliyev R.M., Abdullayeva F.J. Illegal Access Detection in the Cloud Computing Environment // **Journal of Information Security, 2014**, vol. 5, no. 2, pp. 65-71.

In this paper detection method for the illegal access to the cloud infrastructure is proposed. Detection process is based on the collaborative filtering algorithm constructed on the cloud model. Here, first of all, the normal behavior of the user is formed in the shape of a cloud model, then these models are compared with each other by using the cosine similarity method and by applying the collaborative filtering method the deviations from the normal behavior are evaluated. If the deviation value is above than the threshold, the user who gained access to the system is evaluated as illegal, otherwise he is evaluated as a real user.

150. İmamverdiyev Y.N. Elektron dövlətin informasiya təhlükəsizliyi üçün diffuziya indeksi modeli / **"Elektron dövlət quruculuğu problemləri" I respublika elmi-praktiki konfransı,** Bakı**, 4 dekabr 2014,** s. 75-78.

E-dövlətin informasiya təhlükəsizliyinin təmin edilməsi üçün böyük resurslar sərf edilir və nəticədə əldə edilmiş təhlükəsizlik səviyyəsinin ölçülməsi e-dövlətin informasiya təhlükəsizliyində maraqlı olan bütün tərəfləri düşündürən aktual məsələdir. Bu məqalədə e-dövlətin informasiya təhlükəsizliyinin ölçülməsi problemi analiz edilir və informasiya təhlükəsizliyinin qiymətləndirilməsi üçün müxtəlif informasiya təhlükəsizliyi metrikaları əsasında kompozit diffuziya indeksi təklif edilir.

151. Mahmudova R.Ş., Allahverdiyeva S.S. Elektron mühitdə gənc nəslin təhlükəsizliyinin təmin edilməsi problemləri / **"Elektron dövlət quruculuğu problemləri"**

I respublika elmi-praktiki konfransı, Bakı, **4 dekabr 2014**, s. 185-188.

Məqalədə elektron mühitdə uşaqların və yeniyetmələrin İnternet təhlükəsizliyinin təmin edilməsi problemləri dünyanın müxtəlif ölkələrində bu məsələyə aid yanaşmalar araşdırılır. Elektron mühitdə uşaqların təhlükəsizliyinin təmin olunması üçün təkliflər verilir.

152. Rüstəmov D.Ə. Dövlət sirrinin təhlükəsizliyi sahəsində ictimai problemlərin analizi və həlli yolları / **"Elektron dövlət quruculuğu problemləri" I respublika elmi-praktiki konfransı**, Bakı, **4 dekabr 2014,** s. 33-35.

Məqalədə dövlət sirrinin təhlükəsizliyi ilə bağlı ictimai problemlər analiz olunur. Bəzi texnogen xarakterli həllər və milli təhlükəsizlik sisteminə ictimai dəstəyin verilməsinə dair bəzi təkliflər irəli sürülür.

153. Yunusov T.E. Elektron dövlətdə veb xidmətlərin təhlükəsizliyinin qiymətləndirilməsi **/ "Elektron dövlət quruculuğu problemləri" I respublika elmi-praktiki konfransı,** Bakı, **4 dekabr 2014**, s. 36-39.

Məqalədə e-dövlətin veb xidmətlərinin təhlükəsizliyinin qiymətləndirilməsi, e-xidmətlərə mövcud təhdidlərin analizi, e-xidmət təhlükəsizliyi üçün vahid model və e-xidmət təhlükəsizliyi üçün ümumi təhdidlər qiymətləndirilmişdir.

154. Alıquliyev R.M., Ələkbərova İ.Y. Viki-mühitdə gizli sosial şəbəkələrin aşkarlanması metodu / **"Elektron**

dövlət quruculuğu problemləri" I respublika elmi-praktiki konfransı, Bakı, **4 dekabr 2014**, s. 145-147.
Məqalədə viki-mühitdə fəaliyyət göstərən sosial şəbəkələrin analizi ilə bağlı bəzi yanaşmalar şərh olunur. İnformasiya qarşıdurmasında iştirak edən gizli sosial şəbəkələrin aşkarlanması üçün metod təklif edilir.

155. Alguliev R.M., Abdullayeva F.J. Development of risk factor management method for federation of clouds / **The IEEE International Conference on Connected Vehicles and Expo,** Vienna, Austria, **3-7 November 2014**, pp.24-29.
This paper suggests an approach for providing the dynamic federations of clouds. The approach is based on risk assessment technology and implements cloud federations without consideration of identity federations. Here, for solving this problem, first of all, important factors which are capable of seriously influencing the information security level of clouds are selected and then hierarchical risk assessment architecture is proposed vectors are formed by applying the AHP methodology and fuzzy logic excerpt type risk evaluation is carried out based on this vector.

156. Alguliev R.M., Imamverdiyev Y.N. Big Data: Big Promises for Information Security / **8th International Conference on Application of Information and Communication Technologies**, Astana, **15-17 October 2014,** pp. 216-219.

Big Data is related to technologies for collecting, processing, analyzing and extracting useful knowledge from very large volumes of structured and unstructured data generated by different sources at high speed. Big Data creates critical information security and privacy problems, at the same time Big Data analytics promises significant opportunities for prevention and detection of advanced cyber-attacks using correlated internal and external security data. We must address several challenges to realize true potential of Big Data for information security. The paper analyzes Big Data applications for information security problems, and defines research directions on Big Data analytics for security intelligence.

157. Alguliyev R.M., Rustamov D.A., Rzayev M. Computational approach for detection of illegal activities over the Internet / **Proceedings of the IEEE International Conference on Intelligence and Security Informatics**, The Hague, Netherlands, **24-26 September 2014**, pp. 326.
No illegal activity is carried out at once. Usually, parties of illegal activity collect and analyze all possible information about the target and carry out the planning and then proceed to the realization stage. In this paper, heuristic algorithm is suggested for detection of illegal activities and permanent monitoring on current situation in the country over the internet.

158. Fataliyev Z.T., Imamverdiyev Y.N., Hanseok K.O. Security Operation Center Architecture for E-government based on Big Data Analysis / **"Elektron dövlət quruculuğu problemləri" I respublika elmi-praktiki konfransı,** Baku, **4 December 2014,** s. 140-144.

This paper proposes a new architecture for Security Operations Center for handling Big Data and usage of Big Data Analytics for network security of organization. Design flow of proposed architecture has been explained for each step. Proposed architecture is designed using open-source platforms which is designed to handle Big Data.

159. İmamverdiyev Y.N. **İnformasiya təhlükəsizliyi terminlərinin izahlı lüğəti.** Bakı, "İnformasiya Texnologiyaları" nəşriyyatı**, 2015,** 160 s.

Təqdim olunan izahlı lüğətdə informasiya təhlükəsizliyi üzrə elmi və kütləvi ədəbiyyatda rast gəlinən 600-dən çox ingilis dilli termin toplanmış və onların azərbaycan dilində tərcümə variantı verilmişdir. Terminlər informasiya təhlükəsizliyi üzrə elmi və praktiki fəaliyyətin əsas istiqamətlərini əhatə edir. İnformasiya təhlükəsizliyi üzrə ixtisaslaşan mütəxəssislər, tələbələr və elmi tədqiqat aparan şəxslər üçün nəzərdə tutulmuşdur.

160. Əliquliyev R.M., Mahmudov R.Ş. İnformasiya cəmiyyətində intellektual mülkiyyət hüquqlarının qorunması problemləri // **İnformasiya Cəmiyyəti Problemləri,** Bakı**, 2015,** № 2, s. 4-14.

Məqalədə innovativ inkişaf mərhələsində intellektual mülkiyyət hüquqlarının qorunmasının aktual məsələləri araşdırılır. Müəllif hüquqlarının qorunması, o cümlədən plagiatlıq, piratçılıq, vərəsəlik, habelə elmin kommersiyalaşdırılması, patentləşdirmə, intellektual mülkiyyətin sığortalanması məsələləri ilə bağlı mövcud problemlər analiz edilir. İnternet mühitində bu məsələ ilə bağlı yaranan əlavə çətinliklər şərh olunur. Müvafiq problemlərin həllinin Azərbaycanın dövlət siyasətinin prioritet istiqamətlərindən biri olduğu göstərilir. Azərbaycanda innovativ inkişafın, intellektual mülkiyyət hüquqlarının etibarlı təminatı üçün təkliflər irəli sürülür.

161. Cəbrayılova Z.Q. İnsan resurslarının idarə olunması sistemlərində işçinin fərdi məlumatlarının qorunması // **İnformasiya Cəmiyyəti Problemləri, 2015,** № 2, s. 26-34.

Məqalədə insan resurslarının idarə olunması (İRİO) sistemlərinin mahiyyəti, əhəmiyyəti qeyd olunur və bu sistemlərdə işçilər haqqında saxlanılan məlumatın xarakteri verilir. Qeyd olunur ki, bu sistemlər İRİO məsələlərinin həllində nə qədər əhəmiyyətlidirsə, işçilərin fərdi məlumatlarının yayılmasında bir o qədər təhlükələr yaradır, "əmək fəaliyyəti ilə şəxsi həyat arasında uçurumu dərinləşdirir". Belə sistemlərdə işçinin fərdi məlumatlarının qorunması və təhlükəsizliyinin tənzimlənməsi məsələləri qabaqcıl ölkələrin normativ-hüquqi sənədlərinə istinad etməklə analiz olunur. Beynəlxalq təcrübəyə istinadən Azərbaycanda da hər bir təşkilatın hüquqi-normativ aktı kimi işçilərin fərdi

məlumatlarının qorunması haqqında əsasnamənin işlənilməsinin zəruriliyi əsaslandırılır.

162. Ələkbərova İ.Y. Kibermünaqişələrin yaratdığı problemlər və onların həlli yolları // **İnformasiya Cəmiyyəti Problemləri, 2015,** № 2, s. 35-40.

Məqalədə kiberməkanda baş verən münaqişələr və informasiya qarşıdurmaları ilə bağlı problemlər analiz edilir. Kiberhücumların məqsəd və hədəfləri göstərilir, kiberməkanda informasiya qarşıdurmasının üsul və vasitələri təsnifatlandırılır. Kibermünaqişələrdə informasiya təhlükəsizliyi vasitələrindən effektiv istifadə üçün əsas şərtlər göstərilir.

163. Hacırəhimova M.Ş. Elektron sənəd dövriyyəsi sistemlərinin təhlükəsizliyinin bəzi aspektləri // **İnformasiya Cəmiyyəti Problemləri, 2015,** № 2, s. 50-58.

İnformasiya-kommunikasiya texnologiyalarının ən geniş tətbiq sahələrindən biri kargüzarlıqdır. Belə ki, keçən əsrin 90-cı illərindən başlayaraq, informasiya texnologiyalarının tətbiqi ilə kargüzarlıq fəaliyyətinin elektron formada aparılmasına imkan verən elektron sənədlərin idarə edilməsi üzrə kompüter sistemləri tətbiq olunmağa başlanmışdır. Məqalə hazırda idarəetmə məsələlərinin həllində zəruri bir amilə çevrilmiş bu sistemlərin təhlükəsizlik məsələlərinə həsr olunur. Elektron sənəd dövriyyəsi sistemlərinin təhlükəsizliyini şərtləndirən əsas amillər şərh edilir, təhlükələrin təsnifatına baxılır, əsas təhlükəsizlik aspektləri araşdırılır. Həmçinin bu sistemlərdə

təhlükəsizliyin təmin edilməsi üçün istifadə edilən texnologiyalar analiz olunur.

164. İmamverdiyev Y.N. Kiberqoşunlar: funksiyaları, silahları, kadr potensialı // **İnformasiya Cəmiyyəti Problemləri, 2015,** № 2, s. 15-25.

Ölkələr arasındakı münaqişələr kiberfəzaya da keçir və virtual məkanda həm sülh, həm də müharibə dövründə əməliyyatlar aparmaq üçün xüsusi qoşun növləri – kiberqoşunlar yaradılmağa başlayır. Bir sıra ölkələrdə milli informasiya təhlükəsizliyini təmin etmək üçün kiberqoşunlar mövcuddur və ya yaxın illərdə yaradılması planlaşdırılır. Bu işdə kiberqoşunların formalaşdırılması problemləri tədqiq edilir. Kiberqoşunların yaradılmasının əsas aspektləri, kiberqoşunların məqsədləri və funksiyaları, kiberkomandanlığın struktur-təşkilati modelləri araşdırılır, kiberqoşunların silah arsenalı və kadr potensialı, inkişaf etmiş ölkələrin bu sahədə təcrübəsi analiz edilir. Kiberqoşunların və kibertəhlükəsizliklə əlaqəli digər dövlət təşkilatlarının fəaliyyətinin koordinasiyası və beynəlxalq əməkdaşlıq məsələləri də müzakirə edilir.

165. İmamverdiyev Y.N. E-dövlətin informasiya təhlükəsizliyinə etimadın qiymətləndirilməsi modeli // **İnformasiya Texnologiyaları Problemləri, 2015,** №1, s.25-32.

Vətəndaşların e-dövlətin informasiya təhlükəsizliyinə etimadının təmin edilməsi e-dövlətin həqiqi potensialından tam

istifadə edilməsi üçün xüsusi əhəmiyyət daşıyır. Bu məqalədə e-dövlətin informasiya təhlükəsizliyinə etimadın qurulması mexanizmləri analiz edilir və etimadın qiymətləndirilməsi üçün model təklif edilir. Model müxtəlif mənbələrdən alınmış etimad məlumatları əsasında hesablanmış reputasiya qiymətlərinin mənbələrin çəki əmsalları nəzərə alınmaqla inteqrasiyasına əsaslanır.

166. İmamverdiyev Y.N. E-dövlət mühitində informasiya təhlükəsizliyi mədəniyyəti problemləri // **İnformasiya Texnologiyaları Problemləri, 2015,** № 1, s. 80-88.
İnformasiya təhlükəsizliyi problemlərinin həlli texniki üsul və vasitələrlə yanaşı, həm də insanların mədəniyyətindən və peşə vərdişlərindən də asılıdır. Məqalədə informasiya təhlükəsizliyi anlayışının məzmununa müxtəlif yanaşmalar analiz edilir, informasiya təhlükəsizliyi mədəniyyəti ilə korporativ mədəniyyətin qarşılıqlı əlaqəsi aydınlaşdırılır və e-dövlət mühitində təşkilatın informasiya təhlükəsizliyi mədəniyyəti üçün konseptual model təklif edilir, konseptual modelin komponentlərinin formalaşdırılması istiqamətində bir sıra aktual problemlər müəyyən edilir.

167. Qasımova R.T. İnternetdə qlobal domen infrastrukturunun təhlükəsizliyi // **İnformasiya Texnologiyaları Problemləri, 2015,** № 2, s. 61-67.
Müasir şəraitdə domen adları sistemində (Domain Name System, DNS) sorğuların ələ keçirilməsi, saxtalaşdırılmanın və digər təhlükələrin aradan qaldırılmasında DNS

təhlükəsizliyinin təkmilləşdirilməsi (DNS Security Extensions, DNSSEC) texnologiyasından istifadə edilir. Məqalədə bu texnologiyanın təhlükəsizlik aspektləri tədqiq olunur, domen infrastrukturuna tətbiqinin zəruriliyi əsaslandırılır və DNS-serverə olunan hücumların analizi aparılır. Eyni zamanda DNSSEC texnologiyasının həyata keçirilməsi problemləri, üstünlükləri və təhlükəsizliklə bağlı imkanları müəyyən olunur. Bu texnologiyanın tətbiqi ilə bağlı statistika və proqnozlar analiz edilir və onun reallaşdırılması istiqamətində bir sıra tövsiyələr verilir.

168. Şıxəliyev R.H. Müasir kompüter şəbəkələrinin təhlükəsizlik trendləri haqqında // **İnformasiya Cəmiyyəti Problemləri, 2015,** № 2, s. 82-86.
Məqalə kompüter şəbəkələrinin (KŞ) təhlükəsizliyi sahəsində mövcud trendlərin analizinə həsr olunmuşdur. Bunun üçün əvvəlcə KŞ-də (İnternetdə) baş verən infrastruktur, tətbiqi və istifadə trendləri və onların KŞ-nin təhlükəsizliyinə təsiri analiz edilmişdir. Əsaslandırılmışdır ki, KŞ-in təhlükəsizlik trendlərinin müəyyən edilməsi yeni təhdidlərin aşkar edilməsinə və onlara qarşı effektiv mübarizə aparmağa imkan verir.
169. Имамвердиев Я.Н. Нечеткая когнитивная модель стратегического управления информационной безопасностью электронного правительства // **Информационные технологии, 2015,** № 6, с.440-447.

Рассматриваются сущность и особенности применения нечеткого когнитивного моделирования в стратегическом управлении информационной безопасностью на уровне государства. Определены факторы стратегического управления информационной безопасностью, и на основе экспертного оценивания построена нечеткая когнитивная карта для управления информационной безопасностью электронного правительства. На основе разработанной когнитивной модели проанализированы результаты разных стратегий управления информационной безопасностью электронного правительства.

170. Мамедова М.Г. Информационная безопасность персональных медицинских данных в электронной среде // **İnformasiya Texnologiyaları Problemləri, 2015,** № 2, с. 16-30.

Исследованы вопросы защиты персональных данных в системе электронной медицины. Приведены подходы к обеспечению информационной безопасности данных о состоянии здоровья пациентов в мировой практике, выделены специфические особенности персональных медицинских данных и показаны потенциальные угрозы конфидециальности и безопасности медицинской и врачебной тайн в медицинских информационных системах. Рассмотрена правовая основа защиты персональных данных в Азербайджане и обоснована

целесообразность разработки в республике нормативно-методических документов, регулирующих информационную безопасность персональной медицинской информации.

171. Рустамов Д.А., Рзаев М.Я. Вопросы безопасности государственных информационных ресурсов в кризисных ситуациях // **Вопросы защиты информации, 2015,** № 1, с. 71-74.

Рассмотрены вопросы безопасности государственных информационных ресурсов при различных типах кризисных ситуаций. Известно, что с точки зрения безопасности электронного правительства кризисные ситуации являются основным фактором риска. Рассмотрены международные стандарты в этой области, изучен опыт развитых стран и результаты, полученные ведущими научными центрами. Цель - привлечение внимания органов государственной власти к важности данного вопроса.

172. Ağayev B.S., Mehdiyev Ş.A., Əliyev T.S. Elektron tullantılarda məlumat daşıyıcılarının təhlükəsizliyinin təmin olunmasının bəzi məsələləri haqqında / **Beynəlxalq Telekommunikasiya İttifaqının 150 illiyinə həsr olunmuş İnformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransı,** Bakı, **14 may 2015,** s. 236-239.

Məqalədə bir sıra məlumat daşıyıcılarının informasiya təhlükəsizliyi və mühafizə problemləri araşdırılır. Elektron tullantıların daşıyıcılarında və kağızda saxlanılan məxfi və dövlət sirri daşıyan məlumatların qorunması, ehtiyat nüsxələrinin yaradılması, utilizasiyası, bərpa metodları və qurğuları analiz edilir. Məlumat daşıyıcılarının təhlükəsizliyinin idarə edilməsi sisteminin yaradılması məqsədəuyğunluğu məsələsi nəzərdən keçirilir.

173. Ağayeva S.R. İnformasiya təhlükəsizliyinin təmin olunması üçün internet-media resurslarının monitorinqi / **Beynəlxalq Telekommunikasiya İttifaqının 150 illiyinə həsr olunmuş İnformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransı,** Bakı, **14 may 2015,** s. 88-90.

Məqalədə media sahəsində informasiya təhlükəsizliyi problemləri, medianın cəmiyyətə təsiri, həmçinin informasiya təhdidlərinin qarşısının alınmasında internet-medianın monitorinqinin rolu istiqamətində araşdırmalar aparılmışdır. İnternet-medianın ölkənin media infrastrukturunda önəmli bir sahəyə çevrildiyi, əhalinin xeyli hissəsini internet-media vasitəsilə informasiya əldə etdiyi bir dövrdə milli internet məkanının informasiya təhlükəsizliyinin təmin edilməsi zərurəti yaranmışdır. Bu baxımdan internet-mediada informasiya təhlükəsizliyi ilə əlaqədar problemlərin araşdırılması vacib məsələlərdəndir.

174. Cəbrayılova Z.Q. İnsan resurslarının idarə olunması sistemlərində fərdi məlumatların təhlükəsizliyi problemləri / **Beynəlxalq Telekommunikasiya İttifaqının 150 illiyinə həsr olunmuş İnformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransı,** Bakı, **14 may 2015**, s. 70-73.

Məqalədə insan resurslarının idarə olunması sistemlərində işçilərin fərdi məlumatlarının xarakteri verilir, onların qorunması və informasiya təhlükəsizliyi problemlərinə baxılır. Qeyd olunur ki, bu sistemlər təşkilatda kadrların idarə olunması ilə bağlı məsələlərin həllində nə qədər əhəmiyyətlidirsə, işçilər haqqında fərdi məlumatların yayılmasında bir o qədər təhlükələr yaradır. İşçilərin fərdi məlumatlarının qorunması ilə bağlı qabaqcıl ölkələrin təcrübəsini öyrənmək məqsədilə onların qanunvericilikləri analiz olunur. Qabaqcıl təcrübəyə istinad etməklə Azərbaycan Respublikasının əmək məcəlləsində "işçilərin fərdi məlumatlarının qorunması" ilə bağlı maddələrin olması təklif olunur və hər bir təşkilatda müvafiq əsasnamənin işlənilməsinin zəruriliyi göstərilir.

175. Ələkbərov R.Q., Həşimov M.A., Mustafayev T.İ., Yaqubov M.M. AzScienceNet elm kompüter şəbəkəsinin İnternet xidmətlərinin təhlükəsizlik məsələləri / **Beynəlxalq Telekommunikasiya İttifaqının 150 illiyinə həsr olunmuş İnformasiya təhlükəsizliyinin**

multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransı, Bakı, **14 may 2015,** s. 119-122.

Məqalədə AzScienceNet elm kompüter şəbəkəsinin İnternet xidmətlərinin (hostinq, elektron poçt, eduroam, cloud computing) təhlili aparılmışdır. Qeyd olunan xidmətlərin istifadəsi zamanı meydana çıxan təhlükəsizlik məsələləri və onların həlli öz əksini tapmışdır.

176. Əliquliyev R.M., İmamverdiyev Y.N. İnformasiya təhlükəsizliyinin humanitar aspektləri / **Beynəlxalq Telekommunikasiya İttifaqının 150 illiyinə həsr olunmuş İnformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransı,** Bakı, **14 may 2015,** s. 9-12.

İnformasiya təhlükəsizliyinin təmin edilməsində insan faktorunun əhəmiyyətli rola malik olması hazırda hamı tərəfindən etiraf olunan bir həqiqətdir. İnsan faktoru vasitəsilə informasiya təhlükəsizliyinin humanitar və ictimai elmlərlə bir çox predmet hiperəlaqələri yaranır. İnformasiya cəmiyyəti şəraitində informasiya təhlükəsizliyinin təmin edilməsi yeni texnoloji həllər tələb etməklə yanaşı, humanitar və ictimai elmlər qarşısında da bir sıra mürəkkəb problemlər qoyur. Bu işdə informasiya təhlükəsizliyinin humanitar və ictimai elmlər baxımından aktual problemləri analiz edilir və bir sıra multidissiplinar tədqiqat istiqamətləri müəyyən edilir.

177. Əliyev E.A. Korporativ mühitdə biznes, informasiya texnologiyaları və təhlükəsizliyi üzrə fəaliyyət növlərinin

koordinasiyası problemləri / **Beynəlxalq Telekommunikasiya İttifaqının 150 illiyinə həsr olunmuş İnformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransı,** Bakı, **14 may 2015**, s. 209-212.

Bu məqalədə korporativ mühitdə biznes, informasiya texnologiyaları və təhlükəsizliyi üzrə fəaliyyət növlərinin koordinasiyası problemi qoyulur. Bunun üçün həmin fəaliyyət növlərinin əsas prosesləri ISO-21500, ISO-9001, ISO/IEC-12207 və ISO/IEC-27001 beynəlxalq standartlar əsasında identifikasiya edilir, fəaliyyət prosesləri əhəmiyyət prioritetlərinə, icra fazalarına və digər parametrlərinə görə təsnifatlaşdırılır, proseslər arasında asılılıq əlaqələri araşdırılır, belə təsnifatlaşdırma modelinin fəaliyyət növləri arasında koordinasiya üçün əhəmiyyəti göstərilir, koordinasiya mexanizmini formalaşdırmaq üçün metod təklif edilir.

178. Hacırəhimova M.Ş. Big Data texnologiyalarının təhlükələri **/ Beynəlxalq Telekommunikasiya İttifaqının 150 illiyinə həsr olunmuş İnformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransı,** Bakı, **14 may 2015,** s. 248-251.

Məqalədə informasiyanın emalında yeni eranı əks etdirən "Big data" texnologiyalarının qısa xülasəsi verilir. Bu texnologiyanın bəzi təhlükəsizlik aspektləri tədqiq olunur.

179. Əliyev Ə.Q., Musayeva E.H., Əkbərova L.Ə., Abbasova V.Ə. İqtisadiyyatın informasiyalaşdırılmasının bəzi təhlükəsizlik aspektləri / **Beynəlxalq Telekommunikasiya İttifaqının 150 illiyinə həsr olunmuş İnformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransı,** Bakı, **14 may 2015,** s. 148-149.

Məqalədə müasir dövrdə iqtisadiyyatın informasiyalaşdırılması proseslərinin qarşılıqlı təsiri öyrənilmiş və onların təhlükəsizlik aspektləri təhlil olunmuşdur. İnformasiyalaşdırma prosesinə cəmiyyətin və iqtisadiyyatın dayanıqlı inkişafının təmini kimi baxılmışdır. Yeni iqtisadiyyatın İKT əsasında inkişafı üzrə bəzi sahələr göstərilmişdir. Elmə, biliyə və informasiyaya təhlükə və risk mənbəyi kimi baxılmışdır. İqtisadiyyatın informasiyalaşdırılması prosesində yarana biləcək sosial təhlükəlilik halları araşdırılmış və həmin istiqamətdə müəyyən təhlükəsizlik texnologiyalarının işlənilməsi təklif olunmuşdur.

180. Əliyev Ə.Q., Şahverdiyeva R.O. İnnovativ struktur və proseslərin idarə olunmasında informasiya təhlükəsizliyi məsələləri / **Beynəlxalq Telekommunikasiya İttifaqının 150 illiyinə həsr olunmuş İnformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransı,** Bakı, **14 may 2015**, s. 66-69.

Məqalədə innovativ strukturların və proseslərin mahiyyəti izah olunur. Onlara sosial-iqtisadi sistemin elementi kimi baxılır.

Həmin struktur və proseslərin idarə olunmasında informasiya təhlükəsizliyinin mühüm rolu, məqsəd və funksiyaları göstərilir. İnnovativ strukturların informasiya təhlükəsizliyi siyasəti izah olunur. İnformasiya təhlükəsizliyinin fəaliyyət sxemi verilir. İnnovativ strukturların informasiya təhlükəsizliyinin üsul və xüsusiyyətləri təhlil olunur. İnnovativ strukturların informasiya təhlükəsizliyinin təkmilləşdirilməsi üzrə bəzi tövsiyələr verilir.

181. Əliyeva A.S., Əkbərova L.Ə. Elektron kommersiyanın təhlükəsizliyinin təmin edilməsi problemləri / **Beynəlxalq Telekommunikasiya İttifaqının 150 illiyinə həsr olunmuş İnformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransı,** Bakı, **14 may 2015**, s. 183-185.

Məqalədə etibarlı elektron sənəd dövriyyəsi sistemləri üçün nəzərdə tutulmuş elektron imza formatları haqqında ümumi məlumat verilir. Asan imza, gücləndirilmiş elektron imza və təkmil elektron imza nəzərdən keçirilir və CAdES, PAdES və XAdES kimi elektron imza formatları analiz edilir.

182. Fətəliyev T.X. Elektron elmin informasiya təhlükəsizliyi haqqında / **Beynəlxalq Telekommunikasiya İttifaqının 150 illiyinə həsr olunmuş İnformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransı,** Bakı, **14 may 2015**, s. 145-147.

Məqalədə Azərbaycan Respublikasında formalaşdırılan e-elmin informasiya təhlükəsizliyi məsələlərinə baxılmışdır. E-elmin effektiv kiber müdafiəsi üçün prioritet istiqamətlər və bu sahədə görülmüş işlər təqdim olunmuşdur.

183. Hacırəhimova M.Ş. E-sənəd dövriyyəsi sistemlərinin təhlükəsizliyinin təmin edilməsinin bəzi aspektləri / **Beynəlxalq Telekommunikasiya İttifaqının 150 illiyinə həsr olunmuş İnformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransı,** Bakı, **14 may 2015,** s. 159-162.

Məqalə hazırda istər özəl, istərsə də dövlət sektorunda idarəetmə məsələlərinin həllində tətbiqi zəruri bir amilə çevrilmiş elektron sənəd dövriyyəsi sistemlərinin təhlükəsizlik məsələlərinə həsr olunur. Bu sistemlərin təhlükəsizliyini şərtləndirən əsas faktorlar şərh olunur, təhlükələrin təsnifatına baxılır, sistemin əsas təhlükəsizlik aspektləri araşdırılır.

184. İmamverdiyev Y.N. Sosial media və təhlükəsizlik problemləri / **Beynəlxalq Telekommunikasiya İttifaqının 150 illiyinə həsr olunmuş İnformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransı**, Bakı, **14 may 2015**, s.189-192.

Sosial media təkcə rahat ünsiyyət və fayl paylaşımı platforması deyil, həm də ictimai-siyasi təsir və idarəetmə aləti, qarşıdurma və informasiya müharibəsi meydanıdır. Sosial media onu istifadə edənlərin məqsədlərindən asılı olaraq milli

təhlükəsizliyə bir sıra təhdidlər də yarada bilər. Bu işdə sosial medianın milli təhlükəsizliyə təhdid törədə biləcək bir sıra risk ssenariləri təsvir edilir, sosial mediada saxta aktorların – botların yaradılması və idarə edilməsi texnologiyaları və bu sahədə bəzi ölkələrin təcrübəsi analiz edilir. Sosial medianın monitorinqi və analizi üçün mövcud onlayn servislər barəsində məlumat verilir.

185. İmamverdiyev Y.N. İnformasiya-psixoloji təhlükəsizliyin təmin edilməsi problemləri / **Beynəlxalq Telekommunikasiya İttifaqının 150 illiyinə həsr olunmuş İnformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransı,** Bakı, **14 may 2015**, s. 78-81.

Qlobal informasiya cəmiyyəti yaratdığı böyük imkanlarla yanaşı bir sıra neqativ nəticələr də doğurur: dövlətlərarası ziddiyyətlər və münaqişələr qlobal informasiya fəzasına keçir, informasiya müharibəsi imkanları artır, mədəni və ideoloji ekspansiya genişlənir, informasiya müstəmləkəçiliyi meydana çıxır. Dövlətlər qarşısında öz informasiya fəzasının suverenliyini təmin etmək, zərərli informasiyanın fərdi, qrup və kütləvi şüura neqativ təsirlərini effektiv neytrallaşdırmaq problemi durur. Bu işdə informasiya-psixoloji təhlükəsizlik anlayışı dəqiqləşdirilir, informasiya-psixoloji təsir mexanizmləri və informasiya-psixoloji təhlükəsizlik təhdidləri analiz edilir, e-dövlət mühitində informasiya-psixoloji təhlükəsizliyin təmin edilməsinin əsas problemləri göstərilir.

186. Kazımov T.H., Bayramova T.A. Proqram sistemlərinin təhlükəsizliyi və etibarlılığının təmin edilməsində özünüidarə mexanizmləri / **Beynəlxalq Telekommunikasiya İttifaqının 150 illiyinə həsr olunmuş İnformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransı,** Bakı, **14 may 2015**, s. 242-245.

Məqalədə proqram sistemlərinə olan haker hücumlarının sayının artması ilə əlaqədar olaraq yaranan təhlükələr təhlil edilir. Bu təhlükələrin qarşısını almaq məqsədilə onların avtomatik aşkar edilmə vasitələrinin, proqram təminatının özünüidarə mexanizmlərinin işlənilməsi və yaradılan proqram məhsullarının sertifikatlaşdırılması məsələləri araşdırılır.

187. Kazımov T.H., Mahmudova Ş.C. İnformasiya təhlükəsizliyinin təmin olunmasında biometrik texnologiyaların rolu / **Beynəlxalq Telekommunikasiya İttifaqının 150 illiyinə həsr olunmuş İnformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransı**, Bakı**, 14 may 2015**, s.218-221.

Məqalədə informasiya təhlükəsizliyinin təmin olunmasında biometrik texnologiyaların rolundan bəhs olunur. Dünyada terror təhlükəsinin artması ilə əlaqədar olaraq təhlükəsizliyi təmin edən sistemlərin təkmilləşdirilməsi məqsədilə biometrik identifikasiya sistemlərinin yaradılması zərurəti meydana çıxmışdır. Milli zəmində hüquq-mühafizə sistemi, dövlət

təhlükəsizliyi sistemi və ölkənin müdafiə təminatı orqanlarının qarşısında duran məsələlərin həlli üçün biometrik texnologiyalardan istifadə etməyin üstünlükləri göstərilmişdir.

188. Kərimova Ş.A. Smartfonlarda informasiya təhlükəsizliyi riskləri / **Beynəlxalq Telekommunikasiya İttifaqının 150 illiyinə həsr olunmuş İnformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransı,** Bakı, **14 may 2015,** s. 255-258.

Smartfonlar geniş imkana malikdirlər: sensor massivi, çoxkanallı radio, şəbəkə interfeysi, qiqabaytlı yaddaş və güclü prosessor. Belə xüsusiyyətlərinə görə smartfonlar artıq gündəlik həyatımızın bir hissəsinə çevrilib. Smartfonlar həm də informasiya mənbəyidir. Şəxsi həyatımız, işimiz, bir sözlə özümüzlə bağlı olan bu informasiyanın təhlükəsizliyini də nəzərə almaq üçün bir sıra tədbirlər görmək lazımdır. Bu işin məqsədi smartfonlarda informasiya təhlükəsizliyini və smartfon istifadəçilərinin gizlilik risklərini göstərmək və təhlükəsizliyi qorumaq üçün istifadəçilərə praktiki məsləhətlər verməkdir. İşdə smartfon istifadəçilərinin informasiya təhlükəsizliyi üçün 10 risk qiymətləndirilir.

189. Qasımova R.T. İnternet domen infrastrukturunun təhlükəsizliyi – DNSSEC texnologiyası / **Beynəlxalq Telekommunikasiya İttifaqının 150 illiyinə həsr olunmuş İnformasiya təhlükəsizliyinin**

multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransı, Bakı, **14 may 2015,** s. 224-227.

Müasir şəraitdə domen adları sistemində (DNS) sorğuların ələ keçirilməsində, saxtalaşdırılmanın aradan qaldırılması və təhlükəsizliyin təmin edilməsində DNS təhlükəsizliyinin təkmilləşdirilməsi (DNSSEC) texnologiyasından istifadə edilir. Bu məqalədə DNS-serverə olan hücumların analizi aparılır, DNSSEC-in tətbiqinin zəruriliyi əsaslandırılır. DNSSEC texnologiyasının həyata keçirilməsi problemləri, üstünlükləri, eyni zamanda təhlükəsizliklə bağlı imkanları tədqiq edilir. Bu texnologiyanın reallaşdırılması istiqamətində bir sıra tövsiyələr verilir.

190. Mehdiyev Ş.A., İmamverdiyev Y.N. E-dövlətin informasiya təhlükəsizliyi və texnoloji çağırışlar / **Beynəlxalq Telekommunikasiya İttifaqının 150 illiyinə həsr olunmuş İnformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransı,** Bakı, **14 may 2015,** s. 130-133.

E-dövlətin informasiya təhlükəsizliyinə yönəlmiş təhdidlər informasiya sahəsində milli maraqlara qarşı yönəlib. E-dövlətin informasiya təhlükəsizliyinin etibarlı təmin edilməsi üçün siyasi, hüquqi, təhsil, idarəetmə ilə yanaşı, adekvat texnoloji bazanın formalaşdırılması və təkmilləşdirilməsi xüsusi əhəmiyyət daşıyır. Bu işdə milli informasiya təhlükəsizliyi sisteminin formalaşdırılması və təkmilləşdirilməsində qarşıya çıxan əsas texnoloji çağırışlar analiz edilir, inkişaf etmiş

ölkələrin bu sahədə təcrübəsi araşdırılır və bir sıra elmi-praktiki tövsiyələr verilir.

191. Məmmədova M.H. İnformasiya cəmiyyətində e-universitetin informasiya təhlükəsizliyi / **Beynəlxalq Telekommunikasiya İttifaqının 150 illiyinə həsr olunmuş İnformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransı,** Bakı, **14 may 2015,** s. 128-129.

Məqalədə informasiya cəmiyyətində informasiya və kommunikasiya texnologiyalarının tətbiqi ilə əldə olunan nəticələrlə yanaşı, mövcud təhlükələr araşdırılmış, e–dövlətin strateji obyekti kimi e-universitetlərin bu sahədə hansı təhlükələrin hədəfi ola biləcəyi və bu təhlükələrdən mümkün qorunma yolları göstərilmişdir.

192. Mahmudov R.Ş. Əşyaların İnternetinin bəzi təhlükəsizlik problemləri / **Beynəlxalq Telekommunikasiya İttifaqının 150 illiyinə həsr olunmuş İnformasiya cəmiyyətinin multidissiplinar problemləri üzrə II Respublika elmi-praktiki konfransı**, Bakı, **14 may 2015,** s. 99-101.

Tədqiqat işində Əşyaların İnterneti ilə bağlı mövcud təhlükələr araşdırılır. O cümlədən, informasiya təhlükəsizliyi, fərdi məlumatların qorunması məsələlərinə baxılır. Bu sahədəki problemlər şərh olunur və həlli yolları göstərilir.

193. Musayev V.Y., İmamverdiyev Y.N. İnformasiya təhlükəsizliyi sahəsində beynəlxalq çağırışlar,

təşəbbüslər və öhdəliklər / **Beynəlxalq Telekommunikasiya İttifaqının 150 illiyinə həsr olunmuş İnformasiya təhlükəsizliyinin multidis-siplinar problemləri üzrə II respublika elmi-praktiki konfransı,** Bakı, **14 may 2015,** s.102-105.

Məqalədə informasiya təhlükəsizliyi sahəsində beynəlxalq əməkdaşlıqla bağlı qlobal təşkilatların və regional qurumların təşəbbüsləri və konkret fəaliyyət istiqamətləri araşdırılmışdır. Bu sahədə siyasi, hüquqi, elmi-texniki müstəvidə, həmçinin xüsusi istiqamətlər üzrə beynəlxalq təşkilatların əsas fəaliyyət istiqamətləri və qarşılıqlı əlaqələri xülasə olunmuşdur.

194. Naxçıvanski C.Y. Elektron hökumət portalı modeli və onun təhlükəsizliyi məsələləri / **Beynəlxalq Telekommunikasiya İttifaqının 150 illiyinə həsr olunmuş İnformasiya təhlükəsizliyinin multidis-siplinar problemləri üzrə II respublika elmi-praktiki konfransı,** Bakı, **14 may 2015**, s. 163-166.

Məqalədə elektron hökumət portalının konseptual modeli üzərindən onun komponentləri, struktur mexanizmləri və təhlükəsizlik məsələləri təsvir edilmişdir. Təhlükəsiz informasiya mübadiləsi, informasiyanın tamlığı ilə bağlı sistemdə nəzərdə tutulan yanaşmalar, alqoritmlər və protokollar barədə məlumat verilmişdir.

195. Nəbiyev B.R. Şəbəkə trafikinin klasterizasiya metodu haqqında / **Beynəlxalq Telekommunikasiya İttifaqının 150 illiyinə həsr olunmuş İnformasiya**

təhlükəsizliyinin multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransı, Bakı, **14 may 2015,** s. 213-215.

Kompüter şəbəkələrinin təhlükəsizliyinin təmin olunması və prosesin optimallaşdırılması üçün bir çox vasitələr mövcuddur. Məlumdur ki, təhlükələrin yaranmasının əsas səbəblərindən biri şəbəkə trafikində anomal və qeyri profil trafikin generasiya olunmasıdır. Bunları nəzərə alaraq, məqalədə şəbəkə trafikində davranış profilinin müəyyən olunması üçün şəbəkə trafikinin klasterizasiya metodu təklif olunur. Davranış profilinin müəyyən olunması üçün K-ortalar klasterizasiya metodu tətbiq olunur.

196. Şıxəliyev R.H. Müasir kompüter şəbəkələrinin təhlükəsizlik trendləri haqqında / **Beynəlxalq Telekommunikasiya İttifaqının 150 illiyinə həsr olunmuş İnformasiya təhlükəsizliyinin multidis-siplinar problemləri üzrə II respublika elmi-praktiki konfransı,** Bakı, **14 may 2015**, s. 156-158.

Məqalə kompüter şəbəkələrinin təhlükəsizliyi sahəsində mövcud trendlərinin analizinə həsr olunmuşdur. Bunun üçün əvvəlcə kompüter şəbəkələrində (İnternetdə) baş verən infrastruktur, tətbiqi və istifadə trendləri analiz edilmiş və onların kompüter şəbəkələrinin təhlükəsizliyinə təsiri analiz edilmişdir. Kompüter şəbəkələrinin təhlükəsizlik trendlərinin müəyyən edilməsi yeni təhdidlərin aşkar edilməsinə və onlara qarşı effektiv mübarizə aparmağa imkan verər.

197. Yunusov T.E. Kompüter sistemlərində informasiya təhlükəsizliyi auditinin aparılması üsulları / **Beynəlxalq Telekommunikasiya İttifaqının 150 illiyinə həsr olunmuş İnformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransı,** Bakı, **14 may 2015**, s. 252-254.

Məqalə kompüter sistemlərində informasiya təhlükəsizliyi auditinin aparılması üsullarına həsr edilmişdir. Məqalədə kompüter sistemlərinin təhlükəsizliyi auditinin bəzi standart və metodları, o cümlədən İSO 27000, kompüter sistemlərində təhlükəsizlik riskləri, kompüter sistemləri təhlükəsizliyi üçün auditin planlaşdırılması analiz edilmiş və mövcud problemlər müəyyən edilmişdir. Həmçinin mövcud təhlükəsizlik audit metodları nümunə göstərilmişdir.

198. Yusifov F.F. Dayanıqlı, etibarlı və təhlükəsiz elektron dövlətin formalaşmasına bəzi konseptual yanaşmalar / **Beynəlxalq Telekommunikasiya İttifaqının 150 illiyinə həsr olunmuş İnformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransı,** Bakı, **14 may 2015**, s. 134-137.

Elektron dövlət sisteminin informasiya təhlükəsizliyinin təmin olunması məsələləri araşdırılır. Elektron dövlətin təhlükəsizliyinə olan təhdidlər, potensial risklər və onların idarə olunması məsələləri tədqiq olunur. E-dövlətin informasiya təhlükəsizliyinin aktual problemləri müəyyən edilir.

199. Агаев Ф.Т., Мамедова Г.А. Проблемы обеспечения безопасности электронного образования в учебных заведениях / **Beynəlxalq Telekommunikasiya İttifaqının 150 illiyinə həsr olunmuş İnformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransı,** Bakı, **14 may 2015,** c. 180-182.

Потребность обучения в виртуальной образовательной среде растёт из года в год. Возрастает число образовательных учреждений, создавших свою информационно-образовательную среду в интернете. В данной статье обсуждаются проблемы обеспечения информационной безопасности в виртуальном образовательном пространстве. Особое внимание уделяется современным педагогическим технологиям как средству обеспечения информационной безопасности обучения в сети.

200. Мамедова М.Г. Проблемы информационной безопасности персональных данных в условиях электронной медицины / **Beynəlxalq Telekommunikasiya İttifaqının 150 illiyinə həsr olunmuş İnformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə II respublika elmi-konfransı,** Bakı, **14 may 2015**, c. 52-55.

Исследованы проблемы защиты персональных данных в электронной медицине. Приведены подходы к

обеспечению информационной безопасности данных о состоянии здоровья в мировой практике, выделены специфические особенности персональных медицинских данных и показаны потенциальные угрозы конфиденциальности и безопасности медицинской и врачебной тайны в информационных системах. Рассмотрены правовые основы защиты персональных медицинских данных в Азербайджане.

201. Allahverdiyeva S.S. Uşaqların İnternetdə təhlükəsizliyinin təmin edilməsi problemləri. **Ekspress-informasiya.** İnformasiya cəmiyyəti seriyası. Bakı: "İnformasiya Texnologiyaları" nəşriyyatı. **2016**, 91 s.

Ekspress-informasiyada uşaqların İnternetdə qarşılaşdığı təhlükələr və onların təsnifatı, uşaqların bu təhlükələrdən qorunması yolları göstərilir. Beynəlxalq aləmdə bu problemlə bağlı mövcud olan yanaşmalar və çağırışlar şərh edilir. Onlayn mühitdə uşaqların yaş xüsusiyyətləri nəzərə alınmaqla, Əşyaların İnterneti, uşaqlar üçün nəzərdə tutulmuş sosial şəbəkələr və s. problemlər identifikasiya olunur. Nəticədə yeni təklif və tövsiyələr irəli sürülür.

202. Ağayev B.S., Mehdiyev Ş.A., Əliyev T.S. Elektron məlumat daşıyıcıları informasiya təhlükəsizliyinin obyekti kimi // **İnformasiya Cəmiyyəti Problemləri, 2016**, № 1, s. 46-55.

Məqalədə bir sıra məlumat daşıyıcılarının informasiya təhlükəsizliyi və mühafizə problemləri araşdırılır. Elektron

tullantıların daşıyıcılarında və kağızda saxlanılan məxfi və dövlət sirri daşıyan məlumatların qorunması, ehtiyat nüsxələrinin yaradılması, utilizasiyası, bərpa metodları və qurğuları analiz edilir. Məlumat daşıyıcılarının idarə edilməsi sisteminin yaradılması məsələsi nəzərdən keçirilir.

203. Fətəliyev T.X. Elektron elmin təhlükəsizliyinin təmin edilməsi məsələləri haqqında // **İnformasiya Cəmiyyəti Problemləri, 2016,** № 1, s. 56-62.

Məqalə Azərbaycan Respublikasında formalaşan e-elmin təhlükəsizliyi məsələlərinə həsr olunmuşdur. E-elmin tərkib hissələrinə baxılmış, təhlükəsizliyinin təmin edilməsinin vacibliyi və dövrün mürəkkəb texnoloji və sosial problemlərindən olması vurğulanmışdır. Bu sahədə görülmüş işlər təhlil olunmuş və e-elmin effektiv mühafizəsi üçün prioritet istiqamətlər göstərilmişdir.

204. Hacırəhimova M.Ş. "Big Data" texnologiyaları və informasiya təhlükəsizliyi problemləri // **İnformasiya Texnologiyaları Problemləri, 2016,** № 1, s. 49-56.

İnformasiyanın emalında yeni eranı əks etdirən "Big Data" mövzusu biznes mühitində, kütləvi informasiya vasitələrində, həmçinin elmi ədəbiyyatda geniş müzakirə olunmaqdadır. "Big data" idarəçilik, səhiyyə, elm, biznes və kommersiya, sənaye və digər sahələrdə inqilabi dəyişikliklər edə biləcək bir texnologiyadır. Bu texnologiya bir tərəfdən cəmiyyət üçün yeni imkanlar açır, digər tərəfdən isə yeni təhlükəsizlik problemləri yaradır. Məqalədə "big data" texnologiyalarının qısa xülasəsi

verilir. "Big data" analitikanın faydaları, bəzi təhlükəsizlik problemləri tədqiq olunur. Fərdi məlumatların qorunması baxımından onun yaratdığı yeni etik problemlərə baxılır və bəzi tövsiyələr verilir.

205. İmamverdiyev Y.N. Sosial media və təhlükəsizlik problemləri // **İnformasiya Cəmiyyəti Problemləri, 2016,** № 2, s. 19-25.

Sosial media təkcə rahat ünsiyyət və fayl paylaşımı platforması deyil, həm də ictimai-siyasi təsir və idarəetmə aləti, qarşıdurma və informasiya müharibəsi meydanıdır. Sosial media onu istifadə edənlərin məqsədlərindən asılı olaraq milli təhlükəsizliyə bir sıra təhdidlər də yarada bilər. Məqalədə sosial medianın milli təhlükəsizliyə təhdid törədə biləcək bir sıra risk ssenariləri təsvir edilir, sosial mediada saxta aktorların – botların yaradılması və idarə edilməsi texnologiyaları və bu sahədə bəzi ölkələrin təcrübəsi analiz olunur. Sosial medianın monitorinqi və analizi üçün mövcud onlayn servislər barəsində məlumat verilir.

206. İmamverdiyev Y.N., Nəbiyev B.R. İnformasiya təhlükəsizliyinin monitorinqi sistemləri üçün kütləvi xidmət modelləri // **İnformasiya Texnologiyaları Problemləri, 2016,** № 1, s. 33-38.

İnformasiya təhlükəsizliyinin idarə edilməsi sistemlərində informasiya təhlükəsizliyi hadisələrinin emalı proseslərinin modelləşdirilməsi üçün kütləvi xidmət modeli təklif edilir. İnformasiya təhlükəsizliyi hadisələrinin emalı prosesi qarışıq

prioritetli xidmət qaydası ilə işləyən M/G/1 modeli ilə təsvir edilir və üç prioritet sinfi – mütləq, nisbi və prioritetsiz xidmət rejimləri üçün orta gözləmə müddətlərinin analitik ifadələri verilir. Alınmış ehtimal xarakteristikaları əsasında informasiya təhlükəsizliyi hadisələrinin emalı üzrə fəaliyyətin effektivliyini qiymətləndirmək üçün cərimə funksiyaları daxil edilməklə model də təklif edilir.

207. Şıxəliyev R.H. Sosial şəbəkələrdə təhlükəsizlik problemləri // **İnformasiya Cəmiyyəti Problemləri, 2016,** № 2, s. 80-88.

Bu gün İnternetdə çoxlu sayda sosial şəbəkələr mövcuddur. Bu sosial şəbəkələr çox populyardır və insanların həyatında vacib rol oynayır. Bununla yanaşı, sosial şəbəkələr informasiya təhlükəsizliyi sahəsində yeni risklərin yaranmasına gətirib çıxarmışdır. Bu risklər ziyanlı proqramların və spamların yayılması, sosial mühəndislik və sosial şəbəkə hesablarına hücumların həyata keçirilməsi, izləmə, aldatma və s. kimi təhlükələrlə bağlıdır. Məqalə sosial şəbəkələrdə mövcud təhlükələrin analizinə və onlardan qorunma məsələlərinə həsr olunmuşdur.

208. Абдуллаева Ф.Д. Анализ требований к автоматизированной информационной безопасности систем репутаций и сценария применимости систем репутаций в среде облачных вычислений // **Проблемы управления и информатики, 2016,** № 4, с. 147-156.

Появление парадигмы облачных технологий оценивается как очередной революционный процесс в Интернет-среде. Согласно определению этой технологии организацией NIST ресурсы предлагаются пользователям через Интернет в виде сервиса, например, программная служба, платформенная служба, инфраструктурная служба.

209. Imamverdiyev Y.N. E-government ınformation security trust assessment model // **International Journal of Research Studies in Computer Science and Engineering, 2016,** vol. 3, no. 2, pp. 29-34.

The establishment of trust in e government information security is of prominent importance for the full use of the actual potential of e-government. In this article, the trust creation mechanism to e-government information security is analyzed, and the model for the assessment of trust is suggested. The model is based on integration of reputation values calculated according to trust data collected from different sources by taking into consideration the weight coefficients.

210. Alguliyev R.M., Aliguliyev R.M., Alakbarova I.Y. Extraction of hidden social networks from wiki-environment involved in information conflict // **International Journal Intelligent Systems and Applications, 2016,** vol. 8, no. 2, pp. 20-27.

Social network analysis is a widely used technique to analyze relationships among wiki-users in Wikipedia. In this paper the

method to identify hidden social networks participating in information conflicts in wiki-environment is proposed. In particular, we describe how text clustering techniques can be used for extraction of hidden social networks of wiki-users caused information conflict. By clustering unstructured text articles caused information conflict we create social network of wiki-users. For clustering of the conflict articles a hybrid weighted fuzzy-c-means method is proposed.

211. Alguliyev R.M., Mahmudov R.Sh. Topical Issues of Regulation of Economic Relations in Internet Environment // **Economics World. 2016,** vol.4, no.1, pp.25-36.

This article examines current issues of regulation of economical relations in the Internet environment. Complexities, created by global and virtual features of the Internet economy, are characterized. Problems associated with the implementation of the tax and customs policy, regulation of e-money circulation, virtual labor, intellectual property rights protection and consumer rights, as well as personal information are analyzed. Specifics of economic crimes and problems of their control in a virtual environment are commented. Also, the ways to address these problems are indicated.

212. Abdullayeva F.D. Analysis of the requirements of the information security of reputation systems and scenario of using reputation systems in the cloud computing

environment // **Journal of Automation and Information Sciences, 2016,** vol. 48, no. 7, pp. 77-87.

The analysis of application areas of reputation systems, their role at management of identifications in the environment of cloud computing, and the works which are carried out in this direction is given. The main components of reputation systems, security requirements, needed while their design, are defined.

213. Mahmudov R.Ş. Big Data və fərdi məlumatların qorunması problemləri / **"Big data: imkanları, multidissiplinar problemləri və perspektivləri" I respublika elmi-praktiki konfransı,** Bakı**, 25 fevral 2016,** s. 99-102.

Məqalədə Big Data texnologiyalarının tətbiqi şəraitində fərdi məlumatların qorunması problemləri araşdırılır. Fərdi məlumatların toplanması və emalı ilə bağlı hüquq normalarının təkmilləşdirilməsi zərurəti göstərilir. Fərdi məlumatlara mülkiyyət hüququnun tanınması probleminə toxunulur. Fərdi məlumatların şəxssizləşdirilməsi, onların emalının legitimləşdirilməsi və məhdudlaşdırılması ilə bağlı hüquqi konsepsiyalarla Big Data texnologiyalarının tətbiqi konsepsiyaları arasındakı ziddiyyətlər şərh olunur.

214. Allahverdiyeva S.S. Uşaqların internet təhlükəsizliyində Big Data texnologiyalarından istifadə məsələləri / **"Big Data: imkanları, multidissiplinar problemləri və perspektivləri" I respublika elmi-praktiki konfransı,** Bakı, **25 fevral 2016,** s. 122-123.

Məqalədə Big Data uşaqların həyatında oynadığı rol, rəqəmsal əşyaların adi əşyalarla müqayisədə fərqlilikləri araşdırılmışdır. Uşaqların rəqəmsal texnologiyalara olan münasibəti göstərilmişdir. Big Data-nın uşaqların şəxsi məlumatlarından istifadədə müsbət və mənfi cəhətləri qeyd olunmuşdur.

215. Əliquliyev R.M., Abdullayeva F.C. Fərdi tibbi məlumatların on-line mühitdə təhlükəsizliyi problemləri / **"Elektron tibbin multidissiplinar problemləri" I respublika elmi-praktiki konfransı,** Bakı, **24 may 2016,** s.104-109.

Təqdim olunan məqalədə fərdi tibbi məlumatların onlayn mühitdə təhlükəsizlik problemləri tədqiq olunur. Elektron tibb qeydləri və sistemləri terminlərinə aydınlıq gətirilir, eSəhiyyə sahəsində fəaliyyət göstərən standartlaşdırma təşkilatları, fərdi tibbi məlumatların toplanmasını həyata keçirən tətbiq modelləri təsvir edilir. Fərdi tibbi məlumatların qorunması üzrə beynəlxalq təcrübə araşdırılır, təhlükəsizlik və gizlilik problemləri müəyyən olunur və onların həlli üçün təklif və tövsiyələr verilir.

216. İmamverdiyev Y.N. E-dövlətin informasiya təhlükəsizliyi üçün Big Data texnologiyaları / **"Big Data: imkanları, multidissiplinar problemləri və perspektivləri" I respublika elmi-praktiki konfransı,** Bakı, **25 fevral 2016**, s. 86-90.

Big Data texnologiyaları bir sıra spesifik informasiya təhlükəsizliyi problemləri yaratmaqla yanaşı, informasiya

təhlükəsizliyinin təmin edilməsi üçün yeni imkanlar da vəd edir. Bu işdə Big Data texnologiyalarının gətirdiyi yeni informasiya təhlükəsizliyi təhdidləri analiz edilir və bu texnologiyaların e-dövlətin informasiya təhlükəsizliyi sistemində tətbiqi imkanları qiymətləndirilir.

217. İmamverdiyev Y.N. İnformasiya təhlükəsizliyi üzrə tədqiqatlar üçün böyük və kiçik verilənlər / **"Big Data: imkanları, multidissiplinar problemləri və perspektivləri" I respublika elmi-praktiki konfransı**, Bakı, **25 fevral 2016**, s. 95-98.

Big Data texnologiyaları informasiya təhlükəsizliyi üzrə tədqiqatlarda böyük verilənlər toplularından istifadə edilməsini tələb edir. Lakin belə verilənlərin toplanması, tədqiqatçıların geniş dairəsi üçün əlyetər edilməsi sahəsində bir sıra hüquqi, təhlükəsizlik, etik, intellektual mülkiyyət, rəqabət və digər problemlər mövcuddur. Məqalədə informasiya təhlükəsizliyi sahəsində aktual tədqiqat istiqamətləri üzrə mövcud verilənlər topluları haqqında məlumat verilir, bu toplulara müraciət modelləri analiz edilir.

218. İmamverdiyev Y.N. Big Data və fərdi məlumatların təhlükəsizliyi / **"Big Data: imkanları, multidissiplinar problemləri və perspektivləri" I respublika elmi-praktiki konfransı,** Bakı, **25 fevral 2016,** s. 109-113.

Big data üçün fərdi məlumatların təhlükəsizliyi kritik əhəmiyyətli məsələdir. Bu işdə Big data texnologiyalarının fərdi məlumatlara yaratdığı təhdidlər və bu təhdidləri qarşılamaq

üçün fərdi məlumatlar sahəsində qanunvericiliyin təkmilləşdirilməsi çağırışları analiz edilir. Big data texnologiyalarında fərdi məlumatların təhlükəsizliyi üçün mövcud texnoloji yanaşmalar analiz edilir və müvafiq elmi tədqiqat istiqamətləri haqqında məlumat verilir.

219. İmamverdiyev Y.N. Elektron kitabxanalarda informasiya təhlükəsizliyinin aktual problemləri / **"E-kitabxanaların formalaşması problemləri" respublika elmi-praktiki konfransı,** Bakı, **15 aprel 2016**, s. 28-33.

Elektron kitabxanalar onlayn kitabxana-informasiya xidməti göstərən mürəkkəb informasiya sistemidir və belə sistemlər üçün informasiya təhlükəsizliyi və fərdi məlumatların konfidensiallığı kritik əhəmiyyət daşıyır. Bu işdə elektron kitabxanalarda informasiya təhlükəsizliyi problemlərini analiz etmək üçün IDEA4SP modeli təklif edilir və aktual problemlər bu modelin səviyyələri üzrə strukturlaşdırılır. Elektron kitabxanalarda fərdi məlumatların təhlükəsizliyi və intellektual mülkiyyətin qorunmasına texnoloji yanaşmalar da analiz edilir.

220. İmamverdiyev Y.N. E-səhiyyə: informasiya təhlükəsizliyinin aktual problemləri / **"Elektron tibbin multidissiplinar problemləri" I respublika elmi-praktiki konfransı,** Bakı**, 24 may 2016,** s. 32-38.

E-səhiyyə keyfiyyətli tibbi xidmətlərin və məlumatların bütün cəmiyyətə əlyetərliyi sahəsində müxtəlif perspektivlər vəd edir.

Bununla yanaşı, şəxsi həyatın toxunulmazlığı və informasiya təhlükəsizliyi baxımından bir sıra təhlükələrə də yol açır. Bu işdə e-səhiyyə sahəsində əsas inkişaf tendensiyalarına qısa nəzər salınır, əsas informasiya təhlükəsizliyi təhdidləri potensial risk baxımından xarakterizə olunur və informasiya təhlükəsizliyinin təmin edilməsinin vacib mexanizmləri analiz edilir. E-səhiyyə sistemlərində, o cümlədən simsiz bədən sensorları şəbəkələrində informasiya təhlükəsizliyinin təmin edilməsinin aktual elmipraktiki problemləri identifikasiya edilir.

221. Məmmədova M.H. Elektron fərdi tibbi məlumatların informasiya təhlükəsizliyi problemləri / **"Elektron tibbin multidissiplinar problemləri" I respublika elmi-praktiki konfransı,** Bakı, **24 may 2016,** s. 192-196.

Elektron tibdə fərdi məlumatların qorunması problemləri tədqiq edilmişdir. Beynəlxalq təcrübədə pasiyentlərin sağlamlıq vəziyyətləri haqqında məlumatların informasiya təhlükəsizliyinin təmin edilməsinə yanaşmalar göstərilmiş, fərdi tibbi məlumatların spesifik xüsusiyyətləri qeyd edilmiş, tibbi informasiya sistemlərində tibbi və həkim sirlərinin konfidensiallığı və təhlükəsizliynə potensial təhlükələr göstərilmişdir. Azərbaycanda fərdi tibbi məlumatların qorunmasının hüquqi əsasları nəzərdən keçirilmiş və Respublikada fərdi tibbi məlumatların qorunmasını tənzimləyən normativ-hüquqi sənədlərin işlənməsinin məqsədəmüvafiqliyi əsaslandırılmışdır.

222. Yunusov T.E. “Big Data” təhlükəsizliyi və həlli yolları / **“Big Data: imkanları, multidissiplinar problemləri və perspektivləri” I respublika elmi-praktiki konfransı,** Bakı, **25 fevral 2016,** s. 137-139.

Məqalə “Big Data” təhlükəsizliyi və həlli yollarına həsr edilmişdir. Məqalədə “Big Data” fenomeni, “Big Data” texnologiyası, verilənlərin təhlükəsizlik məsələləri, o cümlədən verilənlərin idarəedilməsi, icazələrin idarəedilməsi, məlumatın mühafizəsi və konfidensiallığı, şəbəkə təhlükəsizliyi analiz edilmiş və mövcud problemlər müəyyən edilmişdir.

223. Имамвердиев Я.Н., Сухостат Л.В. Вопросы применения методов машинного обучения для решения проблем информационной безопасности / **“Big Data: imkanları, multidissiplinar problemləri və perspektivləri” I respublika elmi-praktiki konfransı**, Bakı, **25 fevral 2016**, с. 127-131.

В статье представлен обзор основных методов обнаружения аномалий на основе машинного обучения для решения проблем информационной безопасности. Рассмотрены методы классификации и кластеризации. Приведены проблемы машинного обучения во враждебной среде.

224. Имамвердиев Я.Н., Сухостат Л.В. Вопросы безопасности киберфизических систем / **“Riyaziyyatın tətbiqi məsələləri və yeni informasiya**

texnologiyaları" III respublika elmi konfransı, Sumqayıt, **15-16 dekabr 2016,** c. 257-259.

Киберфизические системы (cyber-physical systems, CPS) в целом можно охарактеризовать как комплексные сетевые системы управления, которые сочетают в себе физические элементы реального мира с вычислительными элементами в киберпространстве. Ключевые технологии лежащие в основе CPS включают: "Интернет вещей", смарт-технологии (Smart Everything), облачные вычисления, мобильные технологии, "большие данные" и сервисы для управления анализом данных.

225. Меликова Н.Д. Роль Big Data в обеспечении безопасности детей в Интернете / **"Big Data: imkanları, multidissiplinar problemləri və perspektivləri" I respublika elmi-praktiki konfransı,** Bakı, **25 fevral 2016,** c. 140-143.

В данной статье рассматриваются виды рисков, ожидающих ребенка в Интернете, определение термина Big Data, а также роль Big Data в предотвращении рисков и обеспечении безопасности детей в Интернете.

226. Шыхалиев Р.Г. Об одной модели анализа данных большого сетевого трафика / **"Big Data: imkanları, multidissiplinar problemləri və perspektivləri" I respublika elmi-praktiki konfransı,** Bakı, **25 fevral 2016**, c. 28-30.

Сегодня сложность конфигурации компьютерных сетей продолжает расти. Кроме того, объем трафика, передаваемого по этим сетям, также увеличивается. При этом анализ трафика является перспективным методом для обеспечения эффективности работы и безопасности компьютерных сетей. В статье исследованы возможности применения Big Data-технологий для анализа больших сетевых трафиков. В результате анализа существующих методов анализа Big Data предложена модель анализа большого сетевого трафика компьютерных сетей.

227. Шыхалиев Р.Г. Проблемы информационной безопасности беспроводных систем мониторинга здоровья пациентов / **"Elektron tibbin multidissiplinar problemləri" I respublika elmi-praktiki konfransı,** Bakı, **24 may 2016,** с. 96-98.

Беспроводной мобильный мониторинг здоровья пациентов является очень важным сервисом здравоохранения. При этом обеспечение информационной безопасности систем беспроводного мобильного мониторинга здоровья пациентов является жизненно важной задачей. В статье рассматриваются проблемы безопасности, угрозы безопасности, а также меры по обеспечению безопасности систем беспроводного мобильного мониторинга здоровья пациентов.

228. Abdullayeva F.D. CPTrustworthiness: new robust model for trust evaluation in cloud computing / **IEEE 10th International Conference on Application of Information and Communication Technologies (AICT),** Baku, **12-14 October 2016,** pp. 482-487.

In this paper trustworthiness evaluation issue of cloud provider is considered. A new architectural approach for the trust assessment system is proposed. According to the approach the cloud provider"s trust level is calculated by aggregating provider"s risk and reputation values. For the demonstration of the capabilities of the proposed method the experimental tests are conducted in Matlab program environment.

229. Imamverdiyev Y.N. E-services security assessment model / **10th IEEE International Conference on Application of Information and Communication Technologies,** Baku, **12-14 October 2016,** pp. 595-598.

Information security plays an extremely important role in e-services, as the e-services are vulnerable to various kinds of security and privacy threats on the Internet. The paper presents a formal model of e-services considering four different abstraction levels: application, middleware, operating system and network. Various security threats to e-services and security services to prevent these threats are described. The security level of e-services is determined by the weighted sum of security ratings of individual security services.

230. Imamverdiyev Y.N., Sukhostat L.V. Anomaly detection in network traffic using extreme learning machine / **10th IEEE International Conference on Application of Information and Communication Technologies,** Baku, **12-14 October 2016**, pp. 418-421.

Intrusion detection systems are one of the most relevant security features against network attacks. Machine learning methods are used to analyze network traffic parameters for the presence of an attack signs. In this paper, extreme learning machine method is considered for intrusion detection in network traffic. The experimental results lead to the conclusion of practical significance of the proposed approach for attacks detection in network traffic.

231. Şıxəliyev R.H. **Şəbəkə texnologiyaları.** Bakı: "İnformasiya Texnologiyaları" nəşriyyatı**, 2017,** 238 s.

Kitabda kompüter şəbəkələrinin əsas anlayışları, açıq sistemlərin qarşılıqlı əlaqə modeli, standart şəbəkə protokolları stekləri, şəbəkə əlaqə kanallarına giriş metodları, şəbəkə ünvanlama, şəbəkə marşrutlama, lokal, qlobal, naqilsiz, SDN, multiservis, intellektual, virtual xüsusi şəbəkələrə, İnternet, multiagent və şəbəkə təhlükəsizliyi texnologiyalarına baxılır. Kitab kompüter mühəndisliyi sahəsində bakalavr və magistrlərin hazırlanması üçün istifadə edilə bilər.

232. Əliquliyev R.M., İmamverdiyev Y.N., Mahmudov R.Ş. İnformasiya təhlükəsizliyinin multidissiplinar elmi-

nəzəri problemləri // **İnformasiya Cəmiyyəti Problemləri, 2017,** № 2, s. 32-43.

Məqalədə informasiya təhlükəsizliyinin multidissiplinar elmi-nəzəri problemləri araşdırılır. O cümlədən problemin beynəlxalq, siyasi, psixoloji, hüquqi, iqtisadi, mədəni-etik, kadr hazırlığı və uşaqlarla bağlı aspektləri analiz edilir. Həmin sahələr üzrə aktual elmi tədqiqat istiqamətləri müəyyənləşdirilir.

233. İmamverdiyev Y.N. E-səhiyyədə informasiya təhlükəsizliyinin aktual problemləri // **İnformasiya Cəmiyyəti Problemləri, 2017**, № 1, s. 24-34.

E-səhiyyə keyfiyyətli tibbi xidmətlərin və məlumatların bütün cəmiyyətə əlyetərliyi sahəsində müxtəlif perspektivlər vəd edir. Bununla yanaşı, şəxsi həyatın toxunulmazlığı və informasiya təhlükəsizliyi baxımından bir sıra təhlükələrə də yol açır. Bu işdə e-səhiyyə sahəsində əsas inkişaf tendensiyalarına qısa nəzər salınır, əsas informasiya təhlükəsizliyi təhdidləri potensial risk baxımından xarakterizə olunur və informasiya təhlükəsizliyinin təmin edilməsinin vacib mexanizmləri analiz edilir. E-səhiyyə sistemlərində, o cümlədən simsiz bədən sensorları şəbəkələrində informasiya təhlükəsizliyinin təmin edilməsinin aktual elmi-praktiki problemləri identifikasiya edilir.

234. İmamverdiyev Y.N., Nəbiyev B.R. Şəbəkə təhlükəsizliyinin intellektual monitorinqi üçün

konseptual model // **İnformasiya Cəmiyyəti Problemləri, 2017,** № 1, s. 81-89.

Məqalədə şəbəkə təhlükəsizliyinin prinsipial baxımdan yeni və daha effektli olan intellektual monitorinqinin konseptual modeli təklif olunur. Modeldə monitorinq prosesinin ümumi intellektual arxitekturuna, funksional bloklarına, emal proseslərinə və tətbiq istiqamətlərinə baxılır. Bundan başqa, monitorinq sisteminin boşluqları və zəif nöqtələri araşdırılır. Göstərilən problemlərin aradan qaldırılması üçün təklif olunan model problemyönümlü informasiya monitorinqi, toplanan verilənlərin ilkin emalı, verilənlərin indeksləşdirilməsi və strukturlaşdırılması, toplanan informasiyanın saxlanılması və idarə olunması, qərar qəbul edən şəxslərin tələblərinə uyğun informasiyanın seçilməsi və oxunaqlı, analiz edilə bilən hesabatların generasiyası kimi funksional imkanları özündə birləşdirir.

235. Alguliyev R.M., Aliguliyev R.M., Imamverdiyev Y.N., Sukhostat L.V. An anomaly detection based on optimization // **International Journal of Intelligent Systems and Applications, 2017,** vol. 9, no. 12, pp. 87-96.

At present, an anomaly detection is one of the important problems in many fields. The rapid growth of data volumes requires the availability of a tool for data processing and analysis of a wide variety of data types. The methods for anomaly detection are designed to detect object's deviations from normal behavior. However, it is difficult to select one tool

for all types of anomalies due to the increasing computational complexity and the nature of the data. In this paper, an improved optimization approach for a previously known number of clusters, where a weight is assigned to each data point, is proposed. The aim of this article is to show that weighting of each data point improves the clustering solution. The experimental results on three datasets show that the proposed algorithm detects anomalies more accurately. It was compared to the k-means algorithm. The quality of the clustering result was estimated using clustering evaluation metrics. This research shows that the proposed method works better than k-means on the Australia (credit card applications) dataset according to the Purity, Mirkin and F-measure metrics, and on the heart diseases dataset according to F-measure and variation of information metric.

236. Alguliyev R.M., Aliguliyev R.M., Sukhostat L.V. Anomaly detection in big data based on clustering // **Statistics, Optimization and Information Computing, 2017,** vol. 5, no. 4, pp. 325-340.

Selection of the right tool for anomaly (outlier) detection in Big data is an urgent task. In this paper algorithms for data clustering and outlier detection that take into account the compactness and separation of clusters are provided. We consider the features of their use in this capacity. Numerical experiments on real data of different sizes demonstrate the effectiveness of the proposed algorithms.

237. Алгулиев Р.М., Имамвердиев Я.Н., Сухостат Л.В. Киберфизические системы: основные понятия и вопросы обеспечения безопасности // **Информационные технологии, 2017,** том 23, № 7, с. 517-526.

Данное исследование нацелено на выявление, классификацию и анализ существующих исследований по вопросам безопасности киберфизических систем, чтобы лучше понять, как безопасность на самом деле осуществляется при работе с киберфизическими системами. Рассматриваются оценка последствий кибератак, моделирование и обнаружение атак и разработка архитектуры безопасности. Описаны основные типы атак и классификация угроз на киберфизические системы. Показаны направления будущих исследований.

238. Əliquliyev R.M., Alıquliyev R.M., Abdullayeva F.C. Bulud infrastrukturunun keyfiyyət göstəricilərində anomaliyaların real zamanda aşkarlanması metodu / **"Proqram mühəndisliyinin aktual elmi-praktiki problemləri" I respublika elmi-praktiki konfransı,** Bakı, **17 may 2017,** s. 30-36.

Bulud istifadəçilərə sorğu əsasında miqyaslanan resurslar təqdim edən texnologiyadır. Bulud infrastrukturuna istənilən qurğu vasitəsi ilə daxil olmağın mümkünlüyü və açıq şəbəkələrdən istifadə etməsi bu mühiti müxtəlif tipli

kiberhücumların təsirinə məruz qoymuşdur. Burada informasiya təhlükəsizliyi hücumlarının reallaşması bulud infrastrukturunun serverlərinin yaddaş, CPU resurslarında anomal davranışın yaranmasına səbəb olur. Bu sistemlərin generasiya etdiyi böyük həcmdə verilənlərin təsnif edilməsi prosesi böyük xərc və vaxt tələb etdiyi üçün burada bu məsələnin həllində anomaliyaların yarım-öyrədilən (semi-supervised) metodların köməyilə aşkarlanması qənaətbəxş hesab olunur. Məqalədə bulud infrastrukturunun keyfiyyət göstəricilərində anomaliyaların aşkarlanması üçün yarım-öyrədilən metod təklif edilir. Burada anomal davranışı aşkarlamaq üçün keyfiyyət göstəriciləri üzrə Google və Yahoo! şirkətlərinin açıq verilənləri, Python 2.7, Matlab, Weka və Google Cloud SDK Shell proqramları istifadə edilmişdir. Modelin eksperimental tədqiqi nəticəsində 0.99% aşkarlama dəqiqliyi əldə edilmişdir.

239. Əliyev E.R., İmamverdiyev Y.N. Proqram təminatı və fərdi məlumatların təhlükəsizliyi məsələləri / **"Proqram mühəndisliyinin aktual elmi-praktiki problemləri" I respublika elmi-praktiki konfransı,** Bakı, **17 may 2017**, s. 284-286.

Bu məqalədə "proqram təminatı" və "fərdi məlumatların təhlükəsizliyi" sahələrinə aid məsələlər qoyulur. Bunun üçün: həmin anlayışlar və onların predmetini formalaşdıran komponentlər identifikasiya edilir; bu predmet komponentləri arasında səbəb-nəticə və digər qarşılıqlı təsir əlaqələri

dəqiqləşdirilir; bu sahələrə aid normativ hüquqi və texniki aktlar əsasında informasiya təhlükəsizliyi tələbləri və səlahiyyətlər bölgüsü aləti araşdırılır.

240. İmamverdiyev Y.N. İnformasiya təhlükəsizliyi üçün açıq kodlu alətlər / **"Proqram mühəndisliyinin aktual elmi-praktiki problemləri" I respublika elmi-praktiki konfransı,** Bakı, **17 may 2017**, s. 46-49.

Hazırda açıq kodlu proqram təminatı informasiya texnologiyalarına böyük təsir göstərir, bir sıra yeni sahələrin meydana çıxmasına imkan verir. İnformasiya təhlükəsizliyinin bir çox istiqaməti üzrə kommersiya analoqları ilə rəqabət apara bilən yüksək keyfiyyətli açıq kodlu proqram sistemləri mövcuddur. Bu məqalədə azad proqram təminatının əsas konsepsiyalarına nəzər salınır, informasiya təhlükəsizliyi üzrə açıq kodlu alətlər analiz edilir və onların tətbiqi üzrə bir sıra tövsiyələr işlənir.

241. İmamverdiyev Y.N., Muradova G.M. Qlobal kibertəhlükəsizlik sənayesinin analizi / **"Proqram mühəndisliyinin aktual elmi-praktiki problemləri" I respublika elmi-praktiki konfransı,** Bakı, **17 may 2017**, s. 89-91.

Məqalədə qlobal kibertəhlükəsizlik sənayesinin formalaşması və inkişafı problemləri araşdırılır. Kibertəhlükəsizliyin müasir mənzərəsinə qısa nəzər salınır, kibertəhlükəsizlik sənayesinin seqmentləri müxtəlif meyarlara görə təsnif olunur, yaxın illər üçün bu seqmentlərin inkişaf proqnozları və əsas trendləri

müəyyən edilir, sənayenin əsas oyunçuları arasında bazarın paylaşılması analiz edilir. Kibertəhlükəsizlik sənayesinin əsas trendləri kimi məhsullarda süni intellekt inqilabının baş verməsi, mürəkkəb, smart silahların yaradılmasında sistemli, layihə yanaşmalarının istifadə edilməsi göstərilir.

242. Kazımov T.H., Ocaqverdiyeva S.S. İnternetdə uşaqların təhlükəsizliyini təmin edən proqram vasitələrinin təhlili / **"Proqram mühəndisliyinin aktual elmi-praktiki problemləri" I respublika elmi-praktiki konfransı**, Bakı, **17 may 2017,** s. 305-307.

Məqalədə uşaqların İnternet mühitində təhlükəsizliyinin təmin olunması üçün mövcud proqram təminatları araşdırılır. Geniş istifadəçi auditoriyası qazanmış proqram vasitələri analiz olunur və onların üstün cəhətləri göstərilir.

243. Əliquliyev R.M., Alıquliyev R.M., İmamverdiyev Y.N., Abdullayeva F.C. Böyük verilənlərdə anomaliyaların aşkarlanması üçün çoxkriteriyalı optimallaşdırma üsulu / **"İnformasiya təhlükəsizliyinin aktual problemləri" III respublika elmi-praktiki seminarı**, Bakı, **08 dekabr 2017,** s. 7-11.

Anomaliyaların aşkarlanmasında klasterləşmə üsullarının tətbiqi effektiv yanaşmalardan hesab edilir. Məşhur k-orta və digər klassik klasterləşmə alqoritmlərində klasterin ilkin mərkəzinin seçilməsi və lokal optimumun tapılması əsas problemlərdən biridir və anomaliyaların aşkarlanmasında dəqiq nəticələr əldə etməyə imkan vermir. Məqalədə anomaliyaların

aşkarlanmasında dəqiqliyi artırmaq üçün PSO (particle swarm optimization) və k-orta alqoritmlərinin birləşməsinə əsaslanan yeni çəkili klasterləşmə üsulu təklif edilmişdir. Təklif edilmiş üsul Yahoo! S5 verilənlər bazası üzərində test edilmişdir və alınmış nəticələrin k-orta alqoritmi ilə müqayisəli təhlili aparılmışdır. Eksperimentlərin nəticəsi göstərir ki, təklif edilmiş üsul k-means alqoritmi ilə müqayisədə daha dayanıqlıdır və dəqiq nəticələr əldə etməyə imkan verir.

244. Yusifov F.F. Elektron səsvermə sistemlərində təhlükəsizlik təhdidlərinin qiymətləndirilməsi / **"İnformasiya təhlükəsizliyinin aktual problemləri" III respublika elmi-praktiki seminarı,** Bakı, **08 dekabr 2017**, s. 19-23.

E-səsvermə e-demokratiyanın ən mühüm komponentlərindən biri hesab edilir. E-səsvermə sistemlərinin tətbiqində və inkişaf etdirilməsində təhlükəsizlik məsələləri həlledici rola malikdir. Məqalədə e-səsvermə sisteminə dair yanaşmalar və sistemin təhlükəsizliyinə olan təhdidlər araşdırılır. Çoxmeyarlı qərar qəbul etmə modeli əsasında e-səsvermə sisteminin təhlükəsizliyinə olan təhdidlərin empirik qiymətləndirilməsi məsələsinə baxılır.

245. Ələkbərov R.Q., Ələkbərov O.R. Mobil hesablama buludlarında təhlükəsizlik məsələləri / **"İnformasiya təhlükəsizliyinin aktual problemləri" III respublika elmi-praktiki seminarı**, Bakı, **08 dekabr 2017,** s. 29-33.

Məqalədə mobil hesablama buludlarında istifadə edilən bulud platformalarında təhlükəsizlik problemləri tədqiq edilmişdir. Mobil hesablama buludlarında istifadəçilərin məlumatlarının kənar şəxslərdən zəmanətli qorunması və şəbəkənin təhlükəsizliyi istiqamətində meydana çıxan təhdidlər analiz olunmuşdur. Eyni zamanda, məqalədə mobil hesablama buludlarında informasiya təhlükəsizliyi, konfidensiallıq, məlumatların yerləşdirilməsi və yerdəyişməsi, məlumatların tamlığı, kiber hücumlar və s. məsələlər də geniş analiz olunmuşdur.

246. Alıquliyev R.M., Adıgözəlova N.A. İnformasiya təhlükəsizliyi üzrə aparılan tədqiqatların bibliometrik analizi (2007-2016-cı illər) / **"İnformasiya təhlükəsizliyinin aktual problemləri" III respublika elmi-praktiki seminarı,** Bakı, **08 dekabr 2017**, s. 56-58.
Hazırda informasiya təhlükəsizliyi kompüter elmləri sahəsində aktual elmi istiqamətlərdən biridir. Məqalədə Web of Science elmi bazasında indeksləşən informasiya təhlükəsizliyi sahəsindəki əsərlərin bibliometrik analizi aparılmışdır. Analiz nəticələri göstərir ki, bu sahədə çap olunan əsərlərin və istinadların sayında, eləcə də, jurnalların İF qiymətlərində artım müşahidə olunur.

247. Əliyev E.A., İmamverdiyev Y.N. İnformasiya təhlükəsizliyinin menecmenti standartlarının əlaqəli standartlarla harmonizasiyası xəritəsi: təkliflər / **"İnformasiya təhlükəsizliyinin aktual problemləri" III**

respublika elmi-praktiki seminarı, Bakı, **08 dekabr 2017,** s. 59-62.

Məqalədə informasiya təhlükəsizliyinin menecmenti standartlarının və sisteminin digər sahələrin menecment standartları və sistemləri arasında koordinasiya məsələləri qoyulur. Bunun üçün informasiya təhlükəsizliyinin və digər əlaqəli sahələrin menecment standartları identifikasiya edilir; bu menecment prosesləri PDCA modeli üzrə təsnifatlaşdırılır; informasiya təhlükəsizliyinin menecmenti standarlarının əlaqəli standartlarla harmonizasiyası, o cümlədən səbəb-nəticə asılılıqları, terminologiyada uyğunsuzluqlar barədə problemlər qoyulur; "ISMS" (ISO/IEC-27001) və "SMS" (ISO/IEC-20000) arasında "maraqların münaqişəsi"nin "maraqların uzlaşdırılması"na transferi məsələsi üçün həll variantları verilir.

248. Fətəliyev T.X., Verdiyeva N.N. Elektron elm infrastrukturunun təhlükəsizliyi problemlərinin analizi / **"İnformasiya təhlükəsizliyinin aktual problemləri" III respublika elmi-praktiki seminarı,** Bakı**, 08 dekabr 2017**, s. 63-66.

Müvafiq e-elm infrastrukturu müasir elmi-tədqiqat fəaliyyətinin zəruri tərkib hissəsidir. İnfrastrukturun layihələndirilməsi və reallaşdırılmasında informasiya təhlükəsizliyi problemlərinin təhlili mühüm məsələdir. Məqalədə e-elmin təhlükəsizlik problemləri, onun qrid infrastrukturunun təhlükəsizliyinin konseptual məsələləri

araşdırılmış və Globus Toolkit təhlükəsizlik vasitələrinin problemlərin həllində rolu müəyyənləşdirilmişdir.

249. Alıquliyev R.M., İsmayılova N.Ə. Sosial mediada milli informasiya təhlükəsizliyinə təhdidlərin aşkarlanması üçün yanaşma / **"İnformasiya təhlükəsizliyinin aktual problemləri" III respublika elmi-praktiki seminarı,** Bakı**, 08 dekabr 2017,** s .70-72.

Məqalədə sosial mediada dövlət əleyhinə və milli informasiya təhlükəsizliyinə qarşı təhdidlərin, kibercinayətkarlığın və terrorist qruplarının bədniyyətli fəaliyyətlərinin aşkarlanması üçün texnologiyalar analiz edilmiş və yanaşma təklif olunmuşdur.

250. İmamverdiyev Y.N. İnformasiya təhlükəsizliyi üzrə beynəlxalq koalisiyanın formalaşdırılması problemləri / **"İnformasiya təhlükəsizliyinin aktual problemləri" III respublika elmi-praktiki seminarı,** Bakı, **08 dekabr 2017,** s. 77-80.

Qarşılıqlı əlaqəli və qarşılıqlı asılı dünyada informasiya təhlükəsizliyinin etibarlı təmin edilməsi dövlətlərin sıx əməkdaşlığını tələb edir. Lakin bu sahədə dövlətlərin səmərəli əməkdaşlıq etmələri üçün bir sıra maneələr mövcuddur, ilk növbədə bu məsələdə dövlətlərin strateji maraqları nəzərə alınmalıdır. Bu olduqca çətin məsələdir və nəticədə informasiya təhlükəsizliyi sahəsində beynəlxalq əməkdaşlığın və tənzimləmənin yalnız məhdud formaları məlumdur. Bu məqalədə informasiya təhlükəsizliyi sahəsində beynəlxalq

koalisiyaların formalaşdırılması problemlərini analiz etmək üçün kooperativ oyunlar əsasında nəzəri-oyun modeli təklif edilir.

251. Əliquliyev R.M., Ocaqverdiyeva S.S. Uşaqların İnternetdə informasiya təhlükəsizliyini təmin edən sistemin konseptual modeli / **"İnformasiya təhlükəsizliyinin aktual problemləri" III respublika elmi-praktiki seminarı**, Bakı, **08 dekabr 2017,** s. 84-87.
Məqalədə verilənlərin sanitarizasiyası metodundan istifadə etməklə ziyanlı informasiyanın qarşısının alınması üçün konseptual model təklif olunmuşdur. Məqsəd - intellektual analiz metodlarından istifadə etməklə İnternet şəbəkəsində uşaqların təhlükəsizliyinin təmin edilməsini nəzərdə tutan sistemin yaradılmasıdır.

252. Ələkbərov R.Q., Dursunov S.M. Qrid sistemlərində təhlükəsizlik texnologiyalarının analizi / **"İnformasiya təhlükəsizliyinin aktual problemləri" III respublika elmi-praktiki seminarı,** Bakı**, 08 dekabr 2017,** s. 88-90.
Məqalədə böyük hesablama resursları tələb edən mürəkkəb məsələlərin həllində istifadə olunan paylanmış hesablama sistemlərinin təhlükəsizlik sistemləri təhlil olunmuşdur. Qrid sistemlərində istifadə edilən təhlükəsizlik standartları, paylanmış hesablama mühitində təhlükəsizlik sistemlərinə olan tələblər və Qrid sistemlərinin təhlükəsizlik arxitekturası haqqında geniş məlumat verilmişdir.

253. Hacırəhimova M.Ş., Alıquliyev R.M. Big Data analitika əsasında informasiya təhlükəsizliyi obyektində anomaliyaların aşkarlanması modeli / **"İnformasiya təhlükəsizliyinin aktual problemləri" III respublika elmi-praktiki seminarı**, Bakı, **08 dekabr 2017,** s. 96-99.

Anomaliyaların aşkarlanması verilənlərin analizində əsas məsələlərdəndir və şəbəkə təhdidlərinin aşkarlanmasında geniş istifadə olunur. Məqalədə Big Data analitika əsasında şəbəkə trafikində anomaliyaların aşkarlanması üçün daha dəqiq və sadə multi-klassifikator modeli təklif olunmuşdur. Eksperimentlər NSL-KDD verilənlər dəsti üzrə WEKA proqram təminatında aparılmışdır. Anomaliyaların aşkarlanmasının dəqiqliyi baxımından təklif olunan model yaxşı nəticələr göstərmişdir.

254. Nəbiyev B.R. Şəbəkə təhlükəsizliyi əməliyyat mərkəzinin arxitektur modeli / **"İnformasiya təhlükəsizliyinin aktual problemləri" III respublika elmi-praktiki seminarı**, Bakı, **08 dekabr 2017**, s. 100-103.

Məqalədə, şəbəkənin daha səmərəli və təhlükəsiz idarə edilməsini təmin etmək üçün yeni şəbəkə təhlükəsizliyi əməliyyat mərkəzi arxitekturu yaradılmışdır. Bunun üçün aparılan araşdırmalar göstərir ki, hal-hazırda mövcud olan yanaşmaların bir çox zəif cəhətləri vardır. Mövcud olan yanaşmaların əsas zəif cəhətlərindən biri insan faktorunun iş prosesinin operativliyinə mənfi təsir göstərməsidir. Təqdim olunan arxitektur, şəbəkənin səmərəli və təhlükəsiz idarə

edilməsi üçün müəyyən qərarların qəbul edilməsində köməklik göstərən və gələcəkdə baş verə biləcək hadisələrin qarşısında adaptiv qərarvermə qabiliyyətinə malikdir.

255. Həşimov M.A. Əşyaların İnternetinin təhlükəsizlik məsələləri / **"İnformasiya təhlükəsizliyinin aktual problemləri" III respublika elmi-praktiki seminarı,** Bakı, **08 dekabr 2017**, s. 108-111.

Əşyaların interneti dedikdə, müxtəlif əşyaların internet üzərindən bir-birilə əlaqə qura bilməsi başa düşülür. Bunun üçün müxtəlif arxitektur səviyyələrindən istifadə olunur. Məqalədə əşyaların internetinin arxitekturası təhlil edilmiş və əsas səviyyələri (sensor, şəbəkə, tətbiqi) haqqında məlumat verilmişdir. Qeyd edilən səviyyələrdə meydana çıxan bir sıra təhlükəsizlik məsələləri analiz edilmiş və onların həlli yolları göstərilmişdir.

256. Mənsimzadə O.R. SDN texnologiyalarının təhlükəsizliyi problemləri / **"İnformasiya təhlükəsizliyinin aktual problemləri" III respublika elmi-praktiki seminarı**, Bakı, **08 dekabr 2017**, s. 120-122.

Proqramla idarə olunan şəbəkə texnologiyası (SDN – Software Defined Network) şəbəkə proqram təminatı olaraq gələcək şəbəkə arxitekturasını ənənəvi şəbəkələrdə tətbiq edir, SDN şəbəkə idarəçiliyi üçün sadəlik, proqramlaşdırma və elastiklik baxımından perspektiv imkanlar yaradır. SDN texnologiyasını tətbiq edərkən öndə duran ən vacib məsələlərdən biri də təhlükəsizlikdir. Məqalədə OpenFlow əsasında qurulan SDN

texnologiyasının təhlükəsizlik məsələləri və həlli yolları haqqında məlumat verilmişdir. SDN texnologiyası əsasında qurulan şəbəkəyə edilən hücumlar və bu hücumlardan mudafiə olunmaq üçün tətbiq olunan üsullar təhlil edilmişdir.

257. Алгулиев R.M., Алыгулиев R.M., Имамвердиев Y.N., Сухостат Л.В. Обнаружение DoS атак с применением ансамбля классификаторов / **"İnformasiya təhlükəsizliyinin aktual problemləri" III respublika elmi-praktiki seminarı,** Bakı, **08 dekabr 2017**, с. 12-18.

За последние два десятилетия в мире, ориентированном на «большие» данные, их обработка и аналитика стали важным инструментом обеспечения информационной безопасности. Таким образом, повышение уровня сетевой безопасности является одним из приоритетов исследователей. Чтобы противостоять атакам в сети, были успешно применены ансамбли классификаторов. Хотя существует множество подходов на основе ансамблей классификаторов, остается сложной задачей найти нужную конфигурацию ансамбля для конкретного набора данных. В этой статье предлагается новый метод построения ансамбля классификаторов. Эксперименты проводятся на наборе данных NSL-KDD. Экспериментальные результаты показывают, что предлагаемый подход может генерировать ансамбли классификаторов, превосходящие единичные классификаторы с точки зрения точности.

258. Алгулиев Р.М., Имамвердиев Я.Н., Сухостат Л.В. Обеспечение информационной безопасности киберфизических систем / **"Proqram mühəndisliyinin aktual elmi-praktiki problemləri" I respublika elmi-praktiki konfransı,** Bakı, **17 may 2017**, с. 40-45.

В статье представлен обзор решений обеспечения безопасности киберфизических систем. Описывается принцип работы киберфизической системы. Рассматриваются основные типы атак на киберфизические системы. Приводятся направления будущих исследований.

259. Алыгулиев Р.М., Имамвердиев Я.Н., Абдуллаева Ф.Д. Обнаружение аномалий в облачных Big Data данных / **XIII международная научно-техническая конференция «Оптико-электронные приборы и устройства в системах распознавания образов, обработки изображений и символьной информации» (Распознавание-2017),** Курск, **16-19 мая 2017**, с. 35-37.

В статье предлагается метод обнаружения аномалий на уровне гипервизора инфраструктуры облачных вычислений. Для повышения точности обнаружения аномалий в предложенном подходе используется гибридный алгоритм, полученный комбинированием алгоритма плотностной кластеризации и алгоритмов классификации дерева решений (J48) и проективной

адаптивной теории резонанса (PART-Projective Adaptive Resonance Theory).

260. Алыгулиев Р.М., Имамвердиев Я.Н., Сухостат Л.В. Оптимизационный подход к обнаружению аномалий в Big data / **XIII международная научно-техническая конференция «Оптико-электронные приборы и устройства в системах распознавания образов, обработки изображений и символьной информации» (Распознавание-2017),** Курск, **16-19 мая 2017**, с. 38-40.

Трудность кластеризации больших объемов данных связана с вычислительной сложностью. В работе предлагается оптимизационный подход для обнаружения аномалий в сетевом трафике. Он применяется для заранее известного числа кластеров. Экспериментальные результаты показывают, что предложенный алгоритм точнее обнаруживает аномалии по сравнению с k-means. Доказывается практическая значимость предложенного подхода к обнаружению аномалий в сети.

261. Фаталиев Т.Х., Мехтиев Ш.А. Некоторые вопросы безопасности киберфизических корпоративных систем / **"İnformasiya təhlükəsizliyinin aktual problemləri" III respublika elmi-praktiki seminarı,** Bakı, **08 dekabr 2017**, с. 34-37.

Статья посвящена вопросам обеспечения безопасности киберфизических корпоративных систем.

Проанализированы принципы функционирования инфраструктуры э-науки как киберфизической системы, приведена ее концептуальная модель и рассмотрены ключевые вопросы технического обслуживания для поддержания ее безопасности. Информация, генерируемая системой, может использоваться для планирования технического обслуживания и оптимизированного управления для достижения более высокой общей производительности и безопасности.

262. Шыхалиев Р.Г. О методах мониторинга компьютерных сетей / **"İnformasiya təhlükəsizliyinin aktual problemləri" III respublika elmi-praktiki seminarı,** Bakı, **08 dekabr 2017**, с. 38-41.

Сегодня принятие эффективных решений по управлению и безопасности компьютерных сетей (КС) невозможно без их мониторинга. Мониторинг различных показателей КС позволяет получить необходимую информацию об их состоянии. В работе проводится анализ методов мониторинга КС в различных аспектах, таких как распределенный мониторинг, классификация сетевого трафика, визуализация сетевого мониторинга, QoS (Quality of Service) мониторинг.

263. Шыхалиев Р.Г. О методах идентификации сетевых трафиков / **"İnformasiya təhlükəsizliyinin aktual**

problemləri" III respublika elmi-praktiki seminarı, Bakı, **08 dekabr 2017**, c. 104-107.

Точная идентификация сетевых трафиков является очень важным элементом управления и обеспечения безопасности сетей. В литературе имеется множество методов для идентификации сетевых трафиков и в зависимости от типов, используемых для идентификации информации, точность и полнота этих методов различаются. В статье проводится анализ как традиционных методов идентификации сетевых трафиков, так и методов, основанных на машинном обучении.

264. Шыхалиев Р.Г. О методах верификации и мониторинга программных продуктов / **"Proqram mühəndisliyinin aktual elmi-praktiki problemləri" I respublika elmi-praktiki konfransı**, Bakı, **17 may 2017**, c. 50-53.

В работе представлен анализ методов верификации и мониторинга программных продуктов. Рассматриваются метрики программных продуктов и основные методы верификации программных продуктов, в частности, методы статической, формальной и динамической верификации.

265. Aliguliyev R.M., Imamverdiyev Y.N., Hajirahimova M.Sh. Multidisciplinary problems of big data in information security / **II Международная научно-техническая**

конференция «Информационная безопасность и компьютерные технологии», Кропивницкий, **20-22 апреля 2017,** с. 10-11.

In recent years, in data-centric world, big-data processing and analytics have become an important tool for information security. Big Data problems in the field of information security are: privacy protection, Big data analytics for information security; high-speed cryptography; Big data collections for tests/scientific research; visualization for information security; fostering hacker-minded Data Scientists

266. Ələkbərov R.Q., Ələkbərov O.R. Mobil hesablama buludlarında təhlükəsizlik və konfidensiallıq məsələləri // **İnformasiya Texnologiyaları Problemləri, 2018**, № 1, s. 92–102.

Məqalədə mobil hesablama buludlarında istifadə edilən bulud platformalarda təhlükəsizlik və məxfilik problemləri tədqiq edilmişdir. Mobil hesablama buludlarında istifadəçilərin məlumatlarının kənar şəxslərdən zəmanətli qorunması və şəbəkə təhlükəsizliyi istiqamətində meydana çıxan təhdidlər analiz olunmuşdur. Eyni zamanda məqalədə mobil hesablama buludlarında informasiya təhlükəsizliyi, konfidensiallıq, məlumatların yerləşdirilməsi və yerdəyişməsi, məlumatların tamlığı, kiber hücumlar və s. məsələlər də geniş təhlil olunmuşdur. Mobil hesablama buludlarının informasiya təhlükəsizliyi və konfidensiallığı məsələlərinin elmi-nəzəri

problemləri araşdırılmış və bu istiqamətdə elmi-tədqiqat işlərinin vəziyyəti analiz edilmişdir.

267. İmamverdiyev Y.N. E-dövlətin informasiya təhlükəsizliyi təhdidlərinin konsensus ranqlaşdırılması metodu // **İnformasiya Texnologiyaları Problemləri, 2018,** № 2, s. 34–45.

E-dövlətin informasiya təhlükəsizliyi təhdidləri informasiya sahəsində milli maraqlara qarşı yönəlir. İnformasiya sahəsində milli maraqlara çoxsaylı təhdidlər mövcuddur və kiber-müdafiəyə ayrılan resursların məhdudluğu şəraitində təhdidlərə qarşı effektiv əks-tədbirlər görmək üçün bu təhdidlərin çoxkriteriyalı ranqlaşdırılması zəruridir. Təklif edilən modeldə təhdidlər milli maraqlara yaratdıqları təhlükə səviyyələrini xarakterizə edən ekspert qiymətləndirmələri əsasında ranqlaşdırılır. Təhdidlərin konsensus ranqlaşdırılması üçün optimallaşdırma modeli təklif edilir.

268. İmamverdiyev Y.N. İnformasiya təhlükəsizliyi insidentlərinin emalı proseslərinin optimal planlaşdırılması // **İnformasiya Texnologiyaları Problemləri, 2018,** № 2, s. 80–91.

İnformasiya təhlükəsizliyi insidentlərinə tez və adekvat reaksiya verilməsi biznes-proseslərin fasiləsizliyinin təmin edilməsi üçün həlledici əhəmiyyət daşıyır. Belə insidentlərin emalı üçün xüsusi CERT-komandaların təşkil olunması tələb edilir, lakin onların saxlanması xərcləri əksər təşkilatlar üçün ağır yükdür və təşkilatlar xüsusi CERT-provayderlərin

xidmətlərindən istifadə etməyə üstünlük verirlər. Bu işdə informasiya təhlükəsizliyi insidentlərinin emalı üzrə əməliyyatların operativ planlaşdırılması və CERT-qrupları arasında paylanması modeli optimallaşdırma məsələsi kimi ifadə edilmiş və onun həlli üçün diferensial evolyusiya yanaşması əsasında alqoritm işlənmişdir.

269. İmamverdiyev Y.N. Milli kibertəhlükəsizlik üçün entropiya çəkiləri və dinamik indeks // **İnformasiya Cəmiyyəti Problemləri. 2018,** № 2, s. 16-27.

Hazırda kibertəhlükəsizlik milli təhlükəsizliyin vacib komponentlərindən birinə çevrilmişdir və onun effektiv təmin edilməsi üçün milli kibertəhlükəsizlik səviyyəsinin qiymətləndirilməsi vacib məsələdir. Bu məsələnin həlli üçün bir sıra təşkilatlar tərəfindən milli kibertəhlükəsizlik indeksləri təklif edilmişdir. Lakin milli kibertəhlükəsizlik indeksinin işlənməsi sahəsində elmi tədqiqatlar və praktiki işlər erkən mərhələdədir, onların metodoloji əsaslandırılması qənaətbəxş və tam deyil. Bu işdə mövcud milli kibertəhlükəsizlik indeksləri müqayisəli analiz edilir, onların üstün və nöqsanlı cəhətləri göstərilir, onların təkmilləşdirilməsi üçün təkliflər irəli sürülür. Kompozit milli kibertəhlükəsizlik indekslərinə daxil olan indikatorların çəkilərinin entropiya əsasında qiymətləndirilməsi metodu təklif edilir. Nəhayət, statik və dinamik kibertəhlükəsizlik indeksləri daxil edilir və təklif edilən yanaşmaların real verilənlər əsasında qiymətləndirilməsi aparılır.

270. Mahmudov R.Ş. Big data erasında fərdi məlumatların hüquqi rejiminin müəyyənləşdirilməsi problemləri // **İnformasiya Cəmiyyəti Problemləri, 2018,** №2, s.28-32.

Big Data texnologiyalarının inkişaf etdiyi və iqtisadi əhəmiyyətinin artdığı müasir dövrdə fərdi məlumatların hüquqi rejiminin müəyyən edilməsinə yeni yanaşma tələb edilir. Mövcud situasiya Big Data-nın iqtisadi potensialından maksimum faydalanmaqla yanaşı, insanların şəxsi həyatının etibarlı mühafizəsini təmin etmək üçün optimal, balanslaşdırılmış həll yollarını tələb edir. Məqalədə Big Data erasında fərdi məlumatların toplanması və emalı ilə bağlı hüquq normalarının təkmilləşdirilməsi zərurəti əsaslandırılır. Fərdi məlumatlara mülkiyyət hüququnun tanınması probleminin aktuallığına diqqət çəkilir. İnsanların özəl həyatı ilə bağlı məlumatların şəxssizləşdirilməsi, onların emalının legitimləşdirilməsi və məhdudlaşdırılması ilə bağlı hüquqi konsepsiyalarla Big Data texnologiyalarının tətbiqi konsepsiyaları arasındakı ziddiyyətlər şərh olunur.

271. Alguliyev R.M., Aliguliyev R.M., Yusifov F.F. Role of social networks in e-government: risks and security threats **// Online journal of communication and media technologies**, **2018**, vol. 8, № 4, pp. 363-376.

Social networks are becoming an important intermediary for interaction between governments, citizens, governmental agencies and business sectors. The popularization of social networks among users allows transforming public

administration into open governance form and changing government-citizen relationships. There are various applications of social media to enable communication between users and share personal information. Currently, different attacks on social networks targeting the e-government system pose a great risk for users. In paper the role of social networks and security in e-government is examined. Potential threats targeting the confidentiality and security of each social network user are analyzed and classified. A multi-criteria evaluation method is proposed for analysis of social networks security threats. Potential threats are ranked according to the criteria determined by the Fuzzy TOPSIS method. In the numerical study, the social network security threats are evaluated and ranked according to selected criteria (such as interception of confidential information, reputation loss in government-citizen (G2C) relations and organization of social-political conflicts).

272. Alguliyev R.M., Aliguliyev R.M., Imamverdiyev Y.N., Sukhostat L.V. Weighted clustering for anomaly detection in big data // **Statistics optimization and information computing, 2018**, vol. 6, no. 2, pp. 178-188.

In this paper, a new method for anomaly detection based on weighted clustering is proposed. The weights that were obtained by summing the weights of each point from the data set are assigned to clusters. The comparison is made using seven datasets (of large dimensions) with the k-means algorithm. The proposed approach increases the reliability of

data partitioning into groups. Experimental results show that the proposed approach becomes more efficient with increasing size of the analysed dataset.

273. Alguliyev R.M., Yusifov F.F. Multi-criteria evaluation of electronic voting system security threats // **Вопросы кибербезопасности. 2018,** vol. 3, no. 27, pp. 16-21.

E-voting system is one of the most important components of e-democracy. Implementation of the e-voting system has various purposes. Its main advantages are the selection of candidates with the appropriate competencies, increased activity and mobility of voters, participation of citizens in abroad and operative proclamation of election results and etc. Nowadays, security risks, threats play a vital role in the implementation and development of e-voting systems. There are many vulnerabilities related to different e-voting systems. In paper analysed the approaches to e-voting systems and the system security threats evaluation. An empirical evaluation of e-voting system security threats based on the multi-criteria evaluation approach (worst-case method and TOPSIS) is reviewed and the security threats are ranked based on appropriate criteria.

274. Alguliyev R.M., Aliguliyev R.M., Niftaliyeva G.Y. Filtiration of terrorism-related texts in the e-government environment **// International Journal of Cyber Warfare and Terrorism, 2018,** vol. 8, no. 4, pp. 35-48.

E-government expressesthe process of utilizing advanced information and communication technologies to automate internal activities of government agencies and their external relations with citizens and businesses. All these interactions provide better, faster and more secure public services. In this article, a method for the detection of terrorism-related activities in the e-government environment has been suggested. In the proposed method, terrorism-related activities are defined based on the similarity between the users' opinions and the vocabulary database created linked to terrorism.

275. Alguliyev R.M., Aliguliyev R.M., Imamverdiyev Y.N., Sukhostat L.V. An improved ensemble approach for DOS attacks detection // **Radio Electronics, Computer Science, Control, 2018,** no. 2, pp. 73-82.

The task of using the ensemble of classifiers to detect DoS attacks in large arrays of network traffic data is solved to withstand attacks on the network.

276. Alakbarov R.G., Hashimov M.A. Application and security issues of internet of things in oil-gas industry // **International Journal Education and Management Engineering, 2018,** vol. 6, pp. 24-36.

Article proposes an architecture based on new Internet of Things (IoT) for easy, safe, reliable and rapid data collection from sensors installed in oil and gas industry. Use of several Wireless Sensor Networks in management of oil and gas platforms is researched. New opportunities created by

processing of data collected via sensors for improvement of safety of oil platforms (deposits), optimization of operations, prevention of problems, troubleshooting and reduction of exploitation costs in oil and gas industry. At the same time, the article analyses safety issues of different layers of monitoring system with IoT architecture.

277. Imamverdiyev Y.N., Abdullayeva F.J. Deep Learning Method for Denial of Service Attack Detection Based on Restricted Boltzmann Machine // **Big Data, 2018**, vol. 6, iss. 2, pp. 159-169.

The paper proposes a sentiment classification method for short texis based on deep learning methods and self-attention mechanisms.

278. Əliquliyev R.M., Alıquliyev R.M., Mahmudov R.Ş. Plagiatlıqla mübarizə informasiya təhlükəsizliyinin mühüm komponenti kimi / **"İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri" IV respublika konfransı,** Bakı, **14 dekabr 2018,** s. 38-41.

Məqalədə müəllif hüququnun pozulmasının xüsusi halı olan plagiatlıqla mübarizənin informasiya təhlükəsizliyinin mühüm istiqaməti olduğu əsaslandırılmışdır. Azərbaycanda plagiatlıqla mübarizəyə dair təkliflər irəli sürülmüşdür. Bunun üçün zəruri olan milli elektron kontentin formalaşdırılmasının, milli antiplagiat sisteminin yaradılmasının konseptual əsasları işlənmişdir. Plagiatlıqla mübarizənin hüquqi, ictimai qınaq və

maarifləndirmə metodlarının tətbiqinə dair tövsiyələr verilmişdir.

279. Əliquliyev R.M., Alıquliyev R.M., Ələkbərova I.Y. Elektron dövlət mühitində sosial münasibətlərin təhlükəsizliyi / **"İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri" IV respublika konfransı,** Bakı, **14 dekabr 2018**, s. 64-67.
İnformasiya texnologiyalarının vətəndaşın gündəlik həyatına və davranışına intensiv və dinamik təsiri cəmiyyətdə yeni münasibətlərin yaranmasına, ənənəvi münasibətlərdə müəyyən dəyişikliklərin baş verməsinə səbəb olmuşdur. Tədqiqatda insanlar arasında münasibətlərin xüsusiyyəti analiz olunmuş, münasibətlər forma və tipinə görə təsnifatlandırılmış, münasibətlərə təsir edən əsas faktorlar müəyyənləşdirilmişdir. E-dövlət mühitində münasibətlərin idarə olunması və təhlükəsizliyi məsələlərinin səmərəli həlli üçün təkliflər verilmişdir.

280. Şıxəliyev R.H. Müasir şəbəkə təhlükəsizliyi və inam problemləri / **"İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri" IV respublika konfransı,** Bakı, **14 dekabr 2018,** s. 72-74.
Məqalədə müasir şəbəkə təhlükəsizliyi və inam məsələləri analiz olunmuşdur. Əsasən, İnternetdə mövcud olan yeni şəbəkə xidmətlərinin təhlükəsizlik və inam məsələləri analiz edilmişdir. Xüsusilə də bulud hesablamaları, əşyaların

İnterneti və sosial şəbəkə xidmətlərində meydana çıxan təhlükəsizlik məsələləri analiz edilmişdir.

281. Mahmudova Ş.C. Proqram təminatının təhlükəsizliyinin təmin olunmasının bəzi üsulları haqqında / **"İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri" IV respublika konfransı,** Bakı, **14 dekabr 2018**, s. 75-78.

Bu işdə proqram təminatının təhlükəsizliyi və s. haqqında məlumat verilmişdir. Proqram təminatının təhlükəsizliyinin təmin olunmasının analiz metodları öyrənilmişdir. Proqram təminatının qorunması üçün vacib olan problemlər müəyyənləşdirilmişdir. Proqram layihələri üçün risklər, onların idarəolunması, təyin olunması, kateqoriyaları və s. araşdırılmışdır.

282. Fətəliyev T.X., Mansurova Ş.F. Enerji sektorunda kibertəhlükəsizliyin təmin olunması məsələləri haqqında / **"İnformasiya təhlükəsizliyinin aktual multidis-siplinar elmi-praktiki problemləri" IV respublika konfransı,** Bakı, **14 dekabr 2018,** s. 121-124.

Məqalə milli təhlükəsizliyin kritik tərkib hissəsi kimi enerji sektorunda kibertəhlükəsizlik problemlərinin tədqiqinə həsr olunub. Enerji təhlükəsizliyi problemləri araşdırılmış, parametrik göstəricilərin təsnifatı, enerji sektorunda kibertəhlükəsizliyin xüsusiyyətləri və təmin olunması məsələləri təqdim edilmişdir. Azərbaycanda bu sahədə siyasət və alternativ enerji perspektivləri verilmişdir.

283. Ocaqverdiyeva S.S. Verilənlərin sanitarizasiyasının informasiya təhlükəsizliyinin təmin olunmasında rolu / **"İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri" IV respublika konfransı,** Bakı, **14 dekabr 2018**, s. 127-130.

Məqalədə verilənlərin sanitarizasiyasının mahiyyəti və kateqoriyaları haqqında məlumat verilmişdir. Verilənlərin sanitarizasiyasının alqoritmləri analiz edilmişdir. Həssas verilənlərin konfidensionallığının təmin olunmasında və İnternetdə uşaqların təhlükəsizliyinin təmin edilməsində onun rolu göstərilmişdir.

284. Haşımova K.K. İnternet-reklam marketinqində informasiya təhlükəsizliyi problemləri / **"İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri" IV respublika konfransı,** Bakı, **14 dekabr 2018**, s. 147-149.

Müasır dövrdə İnternetin qlobal sahəsi genişləndikcə, imkanları çoxaldıqca, internet reklamlara tələb artır. Tədqiqatda İnternet üçün nəzərdə tutulmuş reklammarketinqin imkanları, tövsiyə sistemlərindən istifadənin perspektivləri araşdırılmış, təhlükələr müəyyənləşdirilmişdir. Həmçinin veb saytlarda yerləşdirilən reklam-marketinq sistemlərindən səmərəli istifadə üçün təkliflər verilmişdir.

285. Əliyev Ə.Q. İnformasiya iqtisadiyyatının kibertəhlükəsizliyinin təminatı istiqamətləri və texnologiyaları / **"İnformasiya təhlükəsizliyinin aktual multidissiplinar**

elmi-praktiki problemləri" IV respublika konfransı, Bakı, **14 dekabr 2018,** s. 150-154.

Məqalədə İKT-yə əsaslanan yeni tipli iqtisadiyyatın formalaşma xüsusiyyətləri təhlil olunmuş və iqtisadiyyatın inkişafına olan əsas risklər və təhlükələr göstərilmişdir. İqtisadi təhlükəsizlik səviyyəsini xarakterizə edən göstəricilər sistemi şərh edilmişdir. Yeni iqtisadiyyatda informasiya infrastrukturu və texnologiyalarının vəzifələri müəyyənləşdirilmişdir. Rəqəmsal iqtisadiyyat sektorlarında informasiya təlükəsizliyi mənbələri və baza texnologiyaları araşdırılmışdır. İnformasiya iqtisadiyyatının kibertəhlükəsizliyi istiqamətləri və müvafiq texnologiyaları təklif edilmişdir.

286. Ağayeva S.R. İnternet-medianın monitorinqi alətləri və informasiya təhlükəsizliyi məsələləri / **"İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri" IV respublika konfransı,** Bakı, **14 dekabr 2018,** s. 177-180.

Məqalədə İnternet-media resurslarında informasiya təhlükəsizliyinin təmin olunmasında media monitorinqin rolu araşdırılır, mediada təhlükəsizliyə təhdid törədə biləcək risklərdən qorunmaq üçün təkliflər irəli sürülür. Həmçinin İnternet-media və sosial mediada informasiya təhlükəsizliyinin təmin olunmasına imkan verən monitorinq və qiymətləndirmə xidmətləri göstərən şirkətlər haqqında məlumat verilir.

287. Əliyev Ə.Q. İqtisadi inkişafın inklüzivlik səviyyəsinin yüksəldilməsində İKT və onun təhlükəsizliyi problemləri

/ **“İnformasiya təhlükəsizliyinin aktual multi-dissiplinar elmi-praktiki problemləri” IV respublika konfransı,** Bakı, **14 dekabr 2018,** s. 185-189.

Məqalə iqtisadi inkişafın inklüzivlik səviyyəsinin yüksəldilməsində İKT vasitələrinə və onların təhlükəsizliyi problemlərinə həsr olunmuşdur. İqtisadiyyatda yeni inkişaf meylləri və istiqamətləri təhlil olunmuşdur. Cəmiyyətin və iqtisadiyyatın inklüziv inkişafının əhəmiyyətliliyi şərh olunmuşdur. İnklüziv cəmiyyətin və iqtisadiyyatın formalaşması səviyyəsinin regional-sektorial və beynəlxalq qiymətləndirilməsi məsələləri araşdırılmışdır. Azərbaycanda inkişafın inklüzivliyinin beynəlxalq qiymətləndirilməsinə baxılmışdır. İqtisadi inkişafın inklüzivlik səviyyəsinin yüksəldilməsi mexanizmləri müəyyənləşdirilmişdir. İnklüzivlik səviyyəsinin yüksəldilməsində İKT və onun təhlükəsizliyi üzrə bəzi tövsiyələr verilmişdir.

288. Şahverdiyeva R.O. Elmi-texnoloji innovasiya parklarının informasiya təhlükəsizliyi problemləri / **“İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri” IV respublika konfransı**, Bakı, **14 dekabr 2018,** s. 199-203.

Məqalədə elmi-texnoloji innovasiya texnoparklarının fəaliyyətinin informasiya və proqram təminatının formalaşması məsələlərinin aktuallığı əsaslandırılmışdır. Texnoparkların müasir informasiya təminatı sisteminin struktur komponentləri haqqında məlumatlar verilmiş və onların

formalaşmasında mövcud problemləri tədqiq olunmuşdur. Texnoparkların proqram mühəndisliyi sahəsində ixtisaslaşma istiqamətləri təhlil olunmuşdur. Onların informasiya və proqram təminatının işlənilməsində iqtisadi-riyazi və ekonometrik modellər və metodlar, həmçinin proqram paketləri kompleks şəkildə tədqiq edilmişdir.

289. Fətəliyev T.X., Verdiyeva N.N. Vətəndaş elminin informasiya təhlükəsizliyi haqqında / **"İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri" IV respublika konfransı,** Bakı, **14 dekabr 2018,** s. 209-212.

Çoxlu sayda könüllünün geniş məkan və zaman kateqoriyalı kəmiyyət ölçmələri və müşahidələrdə iştirakı ilə xarakterizə olunan vətəndaş elmi informasiya texnologiyalarının tətbiqi ilə sürətlə inkişaf edir. Məqalə onun səmərəli fəaliyyətini təmin etmək məqsədi ilə informasiya təhlükəsizliyi məsələlərinin tədqiqinə həsr olunmuşdur. İnformasiya təhlükəsizliyinin konfidensiallıq, tamlıq, əlyetənlik və fərdi məlumatların qorunması kimi məsələləri araşdırılmış, vətəndaş elminin effektiv mühafizəsi üçün prioritet istiqamətlər göstərilmişdir.

290. Paşayeva G.N. Yeni media təhsili və informasiya təhlükəsizliyi / **"İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri" IV respublika konfransı,** Bakı, **14 dekabr 2018**, s. 213-215.

Yeni medianın vəzifələri və Azərbaycanın media sahəsində informasiya təhlükəsizliyinin təmin olunması məsələlərinə

baxılmışdır. İnformasiya təhlükəsizliyinin media sahəsindəki rolu, informasiya müharibəsinin jurnalistikaya, eləcə də cəmiyyətə təsiri məsələləri araşdırılmışdır.

291. Hacırəhimova M.Ş., Əliyeva A.S. Big Data texnologiyalarının təhlükəsizlik problemləri və həlli yolları / **"İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri" IV respublika konfransı**, Bakı, **14 dekabr 2018,** s. 216-220.

Big data texnologiyalarının meydana gəlməsi verilənlərin təhlükəsizliyi və məxfiliyi üçün yeni problemlər yaradır. Ənənəvi texnologiyalar və metodlar bu problemlərin həlli üçün uyğun və səmərəli deyildir. İşdə böyük verilənlərin təhlükəsizlik problemləri tədqiq olunur. Böyük verilənlərin təhlükəsizliyi və məxfiliyi üçün istifadə olunan texnoloji həllər təhlil olunur və onların cari vəziyyəti nəzərdən keçirilir.

292. Hacırəhimova M.Ş., İsmayılova M.İ. NoSQL verilənlər bazalarında təhlükəsizlik problemləri haqqında / **"İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri" IV respublika konfransı**, Bakı, **14 dekabr 2018**, s. 224-227.

Məqalə böyük verilənlər (Big data) və NoSQL verilənlər bazalarında təhlükəsizlik problemlərinə həsr olunmuşdur. Böyük həcm, sürət və müxtəliflik kimi xüsusiyyətlərlə xarakterizə olunan böyük verilənlərdə təhlükəsizlik və məxfilik ciddi problemlər yaradır. Ənənəvi təhlükəsizlik modelləri bu cür geniş miqyaslı verilənlərlə işləyən zaman çətinliklərlə

rastlaşır. Məqalədə böyük verilənlər və NoSQL verilənlər bazalarında təhlükəsizlik və məxfilik problemləri araşdırılmışdır.

293. Ocaqverdiyeva S.S. Elektron dövlət mühitində uşaqların İnternet təhlükəsizliyinin qanunvericilik bazasının formalaşdırılması problemləri / **"İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri" IV respublika konfransı,** Bakı, **14 dekabr 2018**, s. 228-232.

Məqalədə uşaqların İnternet mühitində qarşılaşdığı təhlükələr analiz olunaraq təsnifatlandırılır. Uşaqların İnternet mühitində təhlükəsizliyinin təmin olunması ilə əlaqədar dünyanın müxtəlif ölkələrində və Azərbaycanda dövlət səviyyəsində, qanunvericilik əsasında qəbul edilmiş normativ sənədlər haqqında məlumat verilir.

294. Əliyev Ə.Q., Səmidov A.F., Şahverdiyeva R.O., Əkbərova L.Ə. İnformasiya iqtisadiyyatı şəraitində nəşriyyat poliqrafiya sektorunun formalaşmasında müasir İKT və onların təhlükəsizliyi məsələləri / **"İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri" IV respublika konfransı,** Bakı, **14 dekabr 2018,** s. 236-240.

Məqalə informasiya iqtisadiyyatı şəraitində innovativ nəşriyyat-poliqrafiya sektorunun formalaşmasında müasir İKT proqram-texniki vasitələrinə, sistemlərinə, resurslarına və onların təhlükəsizliyi problemlərinə həsr olunmuşdur. İqtisadi

inkişafda İKT, bilik və innovasiyaların roluna baxılmış və əhəmiyyəti göstərilmişdir. İnformasiya iqtisadiyyatında nəşriyyat-poliqrafiya sektorunun rolu və yeri aydınlaşdırılmışdır. Nəşriyyat-poliqrafiya sektorunun innovativ xüsusiyyətləri, institutsional strukturu və inkişaf mərhələləri izah olunmuşdur. Nəşriyyat-poliqrafiya sektorunun effektivliyinin yüksəldilməsində innovativ İKT vasitələri və onların təhlükəsizliyi problemləri araşdırılmışdır. Həmin problemlərin həlli üzrə bəzi tövsiyələr verilmişdir.

295. Сухостат Л.В. Обнаружение атак на киберфизические системы на основе глубокого обучения / **"İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri" IV respublika konfransı**, Bakı, **14 dekabr 2018**, s. 42-46.

Частота и серьезность атак на киберфизические системы требуют разработки новых подходов обнаружения и локализации кибератак. В работе предлагается подход, сочетающий в себе преимущества вариационного автоэнкодера и «остаточной» нейронной сети. Предлагаемый подход тестируется на наборе данных системы газопроводов, собранном в Центре защиты критически важных инфраструктур штата Миссисипи (США). Он сравнивается с логистической регрессией и конволюционной нейронной сетью. Сравнительный анализ показывает, что предлагаемый

подход может идентифицировать практически все атаки, присутствующие в наборе данных.

296. Imamverdiyev Y.N., Hajirahimova M.Sh., Bagirov E.O. Implementation of support vector machines for prediction of PVT properties in crude oil systems / **XIV международная научно-техническая конференция «Оптико-электронные приборы и устройства в системах распознавания образов, обработки изображений и символьной информации» (Распознавание–2018),** Курск, **25-28 September 2018**, pp. 25-28.

For the development of advanced strategies of the oil reservoir, the importance of the accurate prediction of the PVT (pressure-volumetemperature) features is great. .In the paper, Support Vector Regression (SVR) machine learning method is used for the prediction of Pb which is one of the most important parameter of Pressure-Volume-Temperature (PVT) properties in oil fields.

297. Alguliyev R.M., Aliguliyev R.M, Sukhostat L.V. Purity-Based consensus clustering for anomaly detection in Big Data / **XIV международная научно-техническая конференция «Оптико-электронные приборы и устройства в системах распознавания образов, обработки изображений и символьной информации» (Распознавание–2018),** Курск, **25-28 сентября 2018**, pp. 16-19.

A consensus approach is widely used to increase the accuracy and stability of clustering results. The paper proposes a weighted consensus clustering for efficient integration of single clustering methods. The proposed method uses a purity-based utility function to aggregate the single clustering methods into a consensus one. The experimental results show that the proposed approach compensates for the shortcomings of each clustering method.

298. Alguliyev R.M., Aliguliyev R.M., Yusifov F.F. MCDM model for evaluation of social network security threats / **Proceedings of the 18th European Conference on Digital Government ECDG 2018,** Spain**, 25-26 October 2018,** pp. 1-7.

The popularity of social networks creates a high risk for the users. A large amount of personal data that users share on social networks makes them a target for a malicious person. A malicious person can obtain sensitive personal data simply by using social networks and can carry out many kinds of attacks, such as spam, malware, worms, sensitive data theft and so on. In this paper, the risks and security issues of social networks are explored. Various security and privacy threats targeted at each user of social networks are classified. Evaluation of social network security threats based on multi-criteria *evaluation method is reviewed. This paper also proposes a fuzzy TOPSIS model for the evaluation of security threats. Social networks security threats are evaluated and ranked based on criteria such*

as interception of confidential information, reputation loss in government-citizen (G2C) relations and organization of social-political conflicts. In the numerical study, the social network security threats are evaluated and ranked according to selected criteria.

299. İmamverdiyev Y.N. E-dövlətin informasiya təhlükəsizliyi üzrə koordinasiya sisteminin çoxmeyarlı qiymətləndirilməsi modeli // **İnformasiya Texnologiyaları Problemləri, 2019,** № 1, s. 47-58.

E-dövlətin informasiya təhlükəsizliyinin təmin edilməsində iştirak edən aktorların (dövlət təşkilatları, özəl sektor, ictimai təşkilatlar və vətəndaşlar) fəaliyyətinin effektiv koordinasiyası aktorlar arasında vaxtında və keyfiyyətli informasiya mübadiləsindən birbaşa asılıdır. Buna görə müvafiq informasiya axınlarının topoloji strukturunu əsas götürməklə və onun analizini aparmaqla koordinasiya sisteminin reinjinerinqini həyata keçirmək və onun iş effektivliyini yüksəltmək mümkündür. Bu məqsədlə təqdim olunan məqalədə e-dövlətin informasiya təhlükəsizliyi üzrə koordinasiya sistemini modelləşdirmək üçün sistem iyerarxik dördsəviyyəli struktura dekompozisiya edilir və onun multi-agent şəbəkə modeli qurulur. Baxılan koordinasiya sisteminın operativliyinin və effektivliyinin qiymətləndirilməsi üçün bu şəbəkə modeli əsasında koordinasiya sisteminin iyerarxiklik indeksi, inersiya dərəcəsi və bir sıra digər indekslər təklif edilir.

300. İmamverdiyev Y.N. İnformasiya təhlükəsizliyi üzrə beynəlxalq koalisiya modeli // **İnformasiya Cəmiyyəti Problemləri, 2019**, № 1, s. 14-20.

Qarşılıqlı əlaqəli və qarşılıqlı asılı dünyada informasiya təhlükəsizliyinin etibarlı təmin edilməsi dövlətlərin sıx əməkdaşlığını tələb edir. Lakin bu sahədə dövlətlərin səmərəli əməkdaşlıq etmələri üçün bir sıra maneələr mövcuddur, ilk növbədə, bu məsələdə dövlətlərin strateji maraqları nəzərə alınmalıdır. Bu olduqca çətin məsələdir və informasiya təhlükəsizliyi sahəsində beynəlxalq əməkdaşlığın və tənzimləmənin yalnız məhdud formaları məlumdur. Məqalədə informasiya təhlükəsizliyi sahəsində beynəlxalq koalisiyaların formalaşdırılması üçün model təklif edilir.

301. Имамвердиев Я.Н. Метод оценки рисков информационной безопасности во взаимосвязанных информационных инфраструктурах // **Информационные системы и технологии, 2019,** №1(111), с. 102-112.

В работе предлагается метод количественной оценки рисков информационной безопасности во взаимосвязанных информационных инфраструктурах электронного правительства. В существующих методологиях риски рассчитываются по отдельным инфраструктурам и, как правило, взаимозависимости инфраструктур не учитываются. Взаимозависимости позволяют рискам безопасности перейти в разные

инфраструктуры и оказать потенциально значительное влияние на них. Предложенный метод построен на основе актуарного подхода, широко используемого для оценки операционных рисков в финансовых организациях. Даются рекомендации по обоснованному выбору соответствующих функций распределения при моделировании частоты потерь и размера потерь. Экстремальные потери моделируются обобщенным распределением Парето.

302. Шыхалиев Р.Г. О методе извлечения классификационных признаков сетевых трафиков на основе анализа сигналов // **İnformasiya Texnologiyaları Problemləri, 2019**, № 1, s. 78–86.

Современные сетевые трафики имеют множество признаков и динамических свойств, которые отражают поведение сети и активность пользователей. Признаки сетевых трафиков играют важную роль в их классификации. Известно, что сетевые трафики имеют нестационарный характер и нелинейные динамические характеристики, такие, как самоподобие, мультифрактальность, долговременная зависимость и периодичность. Поэтому очень актуально извлечение новых робастных классификационных признаков, которые повысят точность классификации сетевых трафиков. Для решения этой проблемы наиболее перспективным методом является спектральный анализ

сигналов сетевых трафиков. В работе для спектрального анализа сигналов сетевых трафиков предлагается использовать вейвлет-преобразование, через которое можно определить энергетические характеристики сигналов сетевых трафиков, используемых в качестве классификационных признаков.

303. Alguliyev R.M., Aliguliyev R.M., Abdullayeva F.J. Deep learning method for prediction of DDoS attacks on social media // **Advances in Data Science and Adaptive Analysis, 2019,** vol. 11, no. 1, pp. 1-19.

Recently, data collected from social media enable to analyze social events and make predictions about real events, based on the analysis of sentiments and opinions of users. Most cyber-attacks are carried out by hackers on the basis of discussions on social media. This paper proposes the method that predicts DDoS attacks occurrence by finding relevant texts in social media. To perform high-precision classification of texts to positive and negative classes, the CNN model with 13 layers and improved LSTM method are used. In order to predict the occurrence of the DDoS attacks in the next day, the negative and positive sentiments in social networking texts are used. To evaluate the efficiency of the proposed method experiments were conducted on Twitter data. The proposed method achieved a recall, precision, F-measure, training loss, training accuracy, testing loss, and test accuracy of 0.85, 0.89, 0.87, 0.09, 0.78, 0.13, and 0.77, respectively.

304. Alguliyev R.M., Aliguliyev R.M., Niftaliyeva G.Y. Extracting social networks from e-government by sentiment analysis of users' comments // **Electronic Government, an International Journal, 2019,** vol. 15, no. 1, pp. 91-106.

Nowadays, the improvement of governance, ensurance the security and the timely detection of propaganda against the government are major problems of e-government. Extraction of hidden social networks is one of the most actual problems in the term of government security. The extraction of hidden social networks operating against the state in e-government is one of the key factors to ensure the security in e-government. In the paper, a method has been proposed for extracting hidden social networks to improve management in e-government, prevent promotion against the government and ensure the security. In this approach, hidden social networks are extracted through the analysis of user's comments via opinion and text mining technologies.

305. Alguliyev R.M., Aliguliyev R.M., Abdullayeva F.J. Hybridisation of classifiers for anomaly detection in Big Data // **International Journal of Big Data Intelligence, 2019,** vol. 6, no. 1, pp. 11-19.

Recently, the widespread use of cloud technologies has led to the rapid increase in the scale and complexity of this infrastructure. The degradation and downtimes in the performance metrics of these large-scale systems are considered

to be a major problem. The key issue in addressing these problems is to detect anomalies that can occur in hardware, software and state of the systems of cloud infrastructure. In this paper, for the detection of anomalies in performance metrics of cloud infrastructure, a semi-supervised classification method based on an ensemble of classifiers is proposed. In the proposed method, to build ensemble Naive Bayes, J48, SMO, multilayer perceptron, IBK and PART algorithms are used. To detect anomalous behaviour on the performance metrics the public data of the Google and Yahoo! companies, Python 2.7, MATLAB, Weka and Google Cloud SDK Shell applications are used. In the result of the experimental study of the model, 90% detection accuracy is obtained.

306. Alguliyev R.M., Aliguliyev R.M., Abdullayeva F.J., PSO+k-means algorithm for anomaly detection in Big Data // **Statistics, Optimization and Information Computing, 2019**, vol. 7, no. 2, pp. 1-13.

The use of clustering methods in anomaly detection is considered as an effective approach. The choice of the cluster primary center and the finding of local optimum in the well-known k-means and other classic clustering algorithms are considered as one of the major problems and do not allow to get accurate results in anomaly detection. In this paper to improve the accuracy of anomaly detection based on the combination of PSO (particle swarm optimization) and k-means algorithms, the new weighted clustering method is proposed. The proposed

method is tested on Yahoo! S5 dataset and a comparative analysis of the obtained results with the k-means algorithm is performed. The results of experiments show that compared to the k-means algorithm the proposed method is more robust and allows to get more accurate results.

307. Əliquliyev R.M., İmamverdiyev Y.N., Mahmudov R.Ş. İnformasiya təhlükəsizliyi milli təhlükəsizliyin mühüm komponenti kimi // **İnformasiya Cəmiyyəti Problemləri, 2020,** № 1, s. 3-25.

Məqalədə milli təhlükəsizliyin mahiyyətinə, məzmununa dair müxtəlif yanaşmalar araşdırılır. Milli təhlükəsizliyin vəzifələri, təmin olunması metodları şərh olunur. Milli təhlükəsizliyin obyekti olan həyati vacib maraqlar, müxtəlif sahələr təsnif edilir. Bu təsnifata uyğun olaraq milli təhlükəsizliyin ictimai-siyasi təhlükəsizlik, hərbi təhlükəsizlik, informasiya təhlükəsizliyi, qida təhlükəsizliyi, enerji təhlükəsizliyi, təhsil sisteminin təhlükəsizliyi, elmi-texnoloji təhlükəsizlik, səhiyyə sisteminin təhlükəsizliyi, nəqliyyat sisteminin təhlükəsizliyi, ekoloji təhlükəsizlik, KİV-in təhlükəsizliyi, mədəni-mənəvi təhlükəsizlik kimi komponentləri fərqləndirilir. İKT-nin inkişafı, informasiya təhlükəsizliyinin formalaşması ilə əlaqədar milli təhlükəsizlik sistemində informasiya cəmiyyətinin artan rolu və vəzifələri göstərilir. İnformasiya təhlükəsizliyi ilə milli təhlükəsizliyin digər komponentləri arasında qarşılıqlı münasibətlər analiz edilir. Hər bir milli təhlükəsizlik komponentində İKT-nin tətbiq sahələri,

informasiya təhlükəsizliyi təhdidləri müəyyən edilir və onların aradan qaldırılması yolları göstərilir. İşin yerinə yetirilməsində analiz və sintez, müqayisə, ümumiləşdirmə, sistemli yanaşma metodlarından istifadə edilmişdir. Məqalədə əldə edilən nəticələr informasiya cəmiyyəti şəraitində milli təhlükəsizlik üzrə yeni konsepsiyaların, strategiyaların və digər normativ sənədlərin hazırlanması üçün istifadə edilə bilər.

308. Imamverdiyev Y.N., Abdullayeva F.J. Deep Learning in Cybersecurity: Challenges and Approaches // **International Journal of Cyber Warfare and Terrorism,** vol. 10, ıssue 2, **April-June 2020**, pp. 82-84.

In this article, a review and summarization of the emerging scientific approaches of deep learning (DL) on cybersecurity are provided, a structured and comprehensive overview of the various cyberattack detection methods is conducted, existing cyberattack detection methods based on DL is categorized. Methods covering attacks to deep learning based on generative adversarial networks are investigated. The datasets used for the evaluation of the efficiency proposed by researchers for cyberattack detection methods are discussed. The statistical analysis of papers published on cybersecurity with the application of DL over the years is conducted. Existing commercial cybersecurity solutions developed on deep learning are described.

309. Fataliyev T.Kh., Mehdiyev Sh.A. Industry 4.0: The Oil and Gas Sector Security and Personal Data Protection // **I.J. Engineering and Manufacturing, 2020,** no. 2, pp.1-14.
In Industry 4.0, a significant increase in data volumes brought to the forefront data protection issues, including in such a sensitive area as personal data. Illegitimate methods of using personal data to obtain additional preferences have become the goal of some communities of people. Video surveillance data are an integral part of personal data, therefore protection of personal data processed in video surveillance systems has been given increased attention. The video surveillance system includes video cameras, information and communication channels for data transmission, processing devices, analytics and personal data storage. The proposed model is a subsystem of smart video surveillance in the oil and gas sector, that consisting of such subsystems as a smart field, smart grid, smart maintenance, smart transportation, smart security, etc. Conceptual tasks are considered and recommendations for their solution are given.

310. Alguliyev R.M., Imamverdiyev Y.N., Mahmudov R.S., Aliguliyev R.M. Information security as a national security component // **Information Security Journal: A Global Perspective, 2020**, no. 29, pp. 1-18.
The essence and different approaches to the national security are explored in the article. The article interprets the objectives and provision methods of the national security. Different areas

and vital interests that are the objects of the national security are classified. According to this classification, the components of the national security, such as socio-political security, military security, information security, food security, energy security, education system security, scientific and technological security, health system security, transport system security, environmental security, mass media security, and cultural-moral security are differentiated. The development of ICT, the growing role and responsibilities of the information society in the national security system in connection with the formation of information security are described. The article also analyzes the relationship between the information security and other components of the national security. Application areas of ICT in each national security component and information security threats are identified. Their solution ways are described. The article uses analysis and synthesis, comparison, generalization and systematic approach. The results obtained in the article can be used for the development of new security concepts, strategies and other regulatory documents for the national security in the context of the information society.

311. İmamverdiyev Y.N., Abbasov H.H. Milli e-imza infrastrukturunun aktual elmi-tədqiqat problemləri // **İnformasiya Texnologiyaları Problemləri, 2021,** №1, s. 33-45.

Təqdim olunan işdə e-imza ilə bağlı milli e-imza infrastrukturunun mövcud texniki və məntiqi imkanlarını

araşdırmaqla, sistemə düşən yükün optimal idarə edilməsi və problemlərin araşdırılması müəyyən edilib. E-imza vətəndaşların elektron mühitdə identikləşdirilməsi üçün şəxsiyyət vəsiqəsi rolunu təmin etdiyi üçün e-dövlət ekosistemində formalaşdırılan informativ və interaktiv elektron xidmətlərə əlçatanlığın təmin edilməsi və bu xidmətlərdən təhlükəsiz istifadə edilməsi e-imza vasitəsi ilə həyata keçirilir. Məqalədə milli e-imza infrastrukturunun yeni texnoloji çağırışlar, mobillik imkanlarının artırılması, məhdud resusrlu qurğularda yüksək məhsuldarlığın təmin edilməsi, e-xidmətlərdən geniş istifadə üçün yüksək təhlükəsizlik tələbləri baxımından təkmilləşdirilməsi problemləri analiz edilir və aktual elmipraktiki məsələlər müəyyən edilir. Müəyyən edilən problemlərin həlli istiqamətində beynəlxalq təcrübə araşdırılmaqla milli infrastrukturun komponentlərinin təhlükəsizliyinin və inam zəncirnin qiymətləndirilməsi istiqamətində mərkəzlərinin işinin modelləşdirilməsi üçün elmi-tədqiqat istiqamətləri analiz edilmişdir. Məqalədə milli e-imza infrastrukturunun özünün təhlükəsizlik problemlərinin müəyyən edilməsi ilə mərkəzlərin xidmət sahələrində təhlükəszilik komponenti kimi səmərəsi müəyyən edilir.

312. Mahmudova R.Ş., Daşdəmirova K.Q. İnformasiya cəmiyyəti mühitində bəzi informasiya təhlükəsizliyi problemlərinin analizi // **İnformasiya Cəmiyyəti Problemləri, 2021,** № 2, s. 83-94.

Cəmiyyətdə informasiyanın, informasiya resurslarının və texnologiyalarının rolunun artması informasiya cəmiyyətində şəxsin, cəmiyyətin, dövlətin maraqlarının qorunması və informasiya təhlükəsizliyinin təmin olunması zəruriyyətini önə çıxarır. Tədqiqat işində informasiya cəmiyyəti mühitində şəxsin, cəmiyyətin və dövlətin maraqlarına təsir göstərə bilən təhdidlər analiz olunmuş, informasiya təhlükəsizliyinin əsas prinsipləri, onun təmin edilməsinin bəzi metodları tədqiq edilmişdir. İnformasiya təhlükəsizliyinin təmin edilməsi sahəsində xarici ölkələrin təcrübəsi araşdırılmış, Azərbaycanda informasiya təhlükəsizliyinin hüquqi təminatı sahəsində görülmüş işlər və aparılan elmi-nəzəri tədqiqatlar araşdırılmışdır.

313. Mahmudova R.Ş. Fərdin və cəmiyyətin informasiya təhlükəsizliyi mədəniyyətinin bəzi aspektləri haqqında // **İnformasiya Cəmiyyəti Problemləri, 2021,** № 1, s.56-67.
Məqalədə fərdin və cəmiyyətin informasiya təhlükəsizliyi mədəniyyətinin bəzi aspektləri araşdırılır. İnformasiya təhlükəsizliyi problemlərinə texnoloji və humanitar aspektdən yanaşmalar təhlil edilir. İnformasiya sistemlərində toplanan informasiyanın, o cümlədən sirr daşıyan məlumatların mühafizəsi, fərdi məlumatların qorunması kimi problemlərin həlli texnoloji üsul və vasitələrlə yanaşı insan faktorundan asılı olduğu üçün informasiya təhlükəsizliyi mədəniyyətinin öyrənilməsi olduqca aktualdır. Bu baxımdan fərdin və cəmiyyətin informasiya təhlükəsizliyi ilə bağlı müxtəlif

problemlər (informasiya bolluğunun yaratdığı problemlər, informasiya "çirklənməsi" problemləri, fərdi və kütləvi şüurun manipulyasiyası, kibercinayətlər, fərdi məlumatların qorunması, informasiya müharibələri, kiberxəstəliklər və s.) araşdırılır və bu problemlərin aradan qaldırılmasında informasiya təhlükəsizliyi mədəniyyətinin rolu əsaslandırılır. Müxtəlif yanaşmaların təhlili əsasında informasiya təhlükəsizliyi mədəniyyətinin mahiyyəti və tərkib hissələri analiz olunur. İnformasiya təhlükəsizliyi mədəniyyətinin texnoloji, informasiya-psixoloji və hüquqi-etik aspektləri araşdırılır və müəyyən təkliflər verilir. İşin yerinə yetirilməsində analiz və sintez, müqayisə, ümumiləşdirmə, sistemli yanaşma metodlarından istifadə edilmişdir. Məqalədə əldə edilən nəticələr informasiya təhlükəsizliyi problemlərini araşdıran tədqiqatçılar, informasiya təhlükəsizliyi fənnini tədris edən müəllimlər tərəfindən mənbə kimi istifadə oluna bilər.

314. Əhmədova X.V. Klasterləşdirmə metodlarının tətbiqi ilə sosial şəbəkələrdə saxta profillərin aşkarlanması // **İnformasiya Texnologiyaları Problemləri, 2021,** №1, s.83-94.

Sosial şəbəkələrin milyonlarla aktiv istifadəçiyə malik olması insanların gizli şəkildə idarə edilməsi (manipulyasiya), müxtəlif növ çağırışlar, insan və ya təşkilatların nüfuzdan salınması kimi zərərli məqsədlərin icrası üçün şərait yaradır. Bu zaman troll profillər, sibil hesablar, kuklalar, bot hesablar və

s. kimi qrup şəklində fəaliyyət göstərən saxta profillər geniş şəkildə istifadə edilir. Klassifikasiya alqoritmlərinin tətbiqi ilə saxta profillərin aşkarlanması zamanı verilənlərin sinif nişanlarına (ing. label) malik olmaları, çox sayda profilin tək-tək təsnif edilməsi zamanı sərf edilən vaxt və s. kimi problemlər ortaya çıxır. Bu məqalədə sosial şəbəkələrdə saxta profillərin qruplaşdırılması üçün k-means, Gaussian Mixture, aqlomerativ klasterləşdirmə, spektral klasterləşdirmə alqoritmləri istifadə edilmişdir. Klasterizasiya alqoritmləri saxta profillərin aşkarlanmasında klassifikasiya metodlarına nisbətən pis nəticə göstərdiyindən bu məqalədə saxta profillərin aşkarlanması üçün tətbiq edilmiş klasterizasiya metodlarının hansı verilənlər üzrə daha yaxşı nəticə verməsi məsələsinə baxılmışdır. Alqoritmlərin tətbiqi zamanı profiləsaslı verilənləri ehtiva edən əlyetər bazalardan istifadə edilmişdir. Klasterizasiya metodlarının nizamlanmış rand indeksi, homogenlik, dolğunluq və s. kimi qiymətləndirmə metrikalarının tətbiqi ilə məhsuldarlığının qiymətləndirilməsi zamanı əldə edilmiş nəticələrə əsasən, aqlomerativ klasterləşdirmə alqoritmi digər tətbiq edilmiş klasterizasiya alqoritmlərinə nisbətən daha yaxşı nəticə göstərmişdir.

315. İmamverdiyev Y.N. Sənaye idarəetmə sistemlərində kibertəhlükəsizlik problemlərinin analizi // **İnformasiya Texnologiyaları Problemləri, 2021,** № 2, s. 16-29.

Sənaye idarəetmə sistemləri (SİS) elektrik istehsalı və təchizatı, içməli su təchizatı, neft və neftkimya, nüvə enerjisi, nəqliyyat

sistemləri, dəmir yolu və metro sistemlərində idarəetmə və monitorinq üçün geniş istifadə olunurlar. Onlar bu kritik milli infrastrukturlarda əməliyyatların beyni və onurğa sütunudur. Kritik infrastrukturların işinin pozulması cəmiyyətə sürətlə və getdikcə kəskinləşən təsir göstərə bilər və bu təsiri kritik infrastrukturlar arasında yüksək dərəcədə qarşılıqlı asılılıq daha da ağırlaşdırır. 2009-cu ildə aşkarlanmış Stuxnet zərərli proqramı SİS kibertəhlükəsizliyinin reallığını və ciddiliyini göstərdi. Industry 4.0 konsepsiyasının geniş tətbiqi ilə əlaqədar SİS-lərin kibertəhlükəsizliyi xüsusi aktuallıq kəsb edir. Məqalədə SİS-lərin mahiyyəti və komponentləri barədə qısa məlumat verilir və onların kibertəhlükəsizliyinin müasir vəziyyətinin qısa analizi aparılır. SİSlərin kibertəhlükəsizliyinin qiymətləndirilməsi üzrə tədqiqatlar risklərin idarə edilməsi, zərərli proqram təminatının aşkarlanması və analizi metodları, kibertəhlükəsizliyin monitorinqi üçün honeynet texnologiyaları və test stendlərinin yaradılması istiqamətləri üzrə analiz edilir və hər bir istiqamət üzrə açıq tədqiqat problemləri göstərilir. Əsas tədqiqat metodları modelləşdirmə, müqayisəli və təsviri metodlar, analogiya, analiz və sintez metodlarıdır; əsas tədqiqat yanaşmaları sistemli, kompleks və situativ yanaşmadır. Alınmış nəticələrin ölkədə SİS-lərin kibertəhlükəsizliyi infrastrukturunun formalaşdırılması və inkişafında, SİS kibertəhlükəsizliyi sahəsində elmi tədqiqatların təkmilləşdirilməsi və milli informasiya təhlükəsizliyi üzrə

tədbirlər kompleksinin işlənməsində və praktiki reallaşdırılmasında faydalı olacağı gözlənilir.

316. Алгулиев Р.М., Махмудов Р.Ш. Особенности «черного рынка» персональных данных и создаваемые им проблемы // **Информационное общество, 2021**, №1, с. 49-55.

В статье исследуются сущность и особенности «черного рынка» персональных данных. Рассмотрены являющиеся предметом купли-продажи на «черном рынке» виды информации и услуг, технологии и их ценовая политика, а также цели, для которых используются персональные данные, приобретенные на «черном рынке». Кроме того, отмечены проблемы, связанные с незаконным приобретением и продажей персональных данных с точки зрения личных, корпоративных и национальных интересов.

317. Sukhostat L.V. An Intelligent Model based on Deep Transfer Learning for Detecting Anomalies in Cyber-Physical Systems // **Radio Electronics, Computer Science, Control. 2021,** vol. 3, pp. 124-132.

The problem of detecting anomalies from signals of cyber-physical systems based on spectrogram and scalogram images is considered. The object of the research is complex industrial equipment with heterogeneous sensory systems of different nature. The goal of the work is the development of a method for signal anomalies detection based on transfer learning with the

extreme gradient boosting algorithm. The developed approach is implemented in software and evaluated for the anomaly detection task in acoustic signals of cyber-physical systems on the MIMII dataset. Conclusions. The conducted experiments have confirmed the efficiency of the proposed approach and allow recommending it for practical use in diagnosing the state of industrial equipment. Prospects for further research may lie in the application of ensemble approaches based on transfer learning to various real datasets to improve the performance and fault-tolerance of cyber-physical systems.

318. Alguliyev R.M., Abdullayeva F.J., Ojagverdiyeva S.S. Log-File Analysis to Identify Internet-addiction in Children // **International Journal of Modern Education & Computer Science. 2021,** vol. 13, no. 5, pp. 23-31.

This article uses machine-learning techniques to detect Internet addiction (IA). Activities of children in the Internet environment is analyzed. The log-files of children and their IA problem are explored. To determine the degree of IA among children and adolescents an experiment is conducted on public dataset. The effectiveness of the methods is analyzed by various evaluation metrics and promising results are obtained. The results show better performance of Weighted SVM, compared to Bernoulli NB, Logistic Regression, MLPClassifier, SVM classifiers. Acquired results of the research provide kids information security. To evaluate a kids IA helps to identify their psychological conditions, and it creates a better situation

for parents, teachers, and other related people to communicate with children and teenagers better way.

319. Abdullayeva F.J., Ojagverdiyeva S.S. Multicriteria decision making using analytic hierarchy process for child protection from malicious content on the Internet // **International Journal of Computer Network and Information Security. 2021**, vol. 13, no. 3, pp. 52-61.

Modern children are active Internet users. However, in the context of information abundance, they have little knowledge of which information is useful and which is harmful. To make the Internet a safe place for children, various methods are used at the international and national levels, as well as by experts, and the ways to protect children from harmful information are sought. The article proposes an approach using a multi-criteria decision-making process to prevent children from encountering harmful content on the Internet and to make the Internet more secure environment for children. The article highlights the age characteristics of children as criteria. Harmless information, Training information, Entertainment information, News, and Harmful information are considered as alternatives. Here, a decision is made by comparing the alternatives according to the given criteria. According to the trials, harmful information is rated in the last position. There is no child protection issue on the Internet using the AHP method. This research is important to protect children from harmful information in the virtual space. In the protection of minors Internet users is a reliable

approach for educational institutions, parents and other subjects related to child safety.

320. Abdullayeva F.J. Advanced persistent threat attack detection method in cloud computing based on autoencoder and softmax regression algorithm // **Array, 2021**, vol. 10, pp. 1-11.

The paper proposes autoencoder based deep learning approach for APT (Advanced Persistent Threat) attack detection. The advantage of this model is that it achieves a high classification result by identifying complex relationships between features in a database. Additionally, the model simplifies the process of classifying large volumes of data by reducing the size of data in the encoder. Here, first of all, the autoencoder neural network was applied, and informative features were studied from the network traffic data in an unsupervised manner. After the informative feature study, softmax regression layer was added to the top layer of the constructed autoencoder network to classify APT attacks. In this study, a deep neural network model constructed by adding different layers was tested on a database open to scientific research and compared to existing methods; the proposed method gave superior results in detection of APT attacks. The average detection accuracy of the proposed APT detection framework was achieved of 98.32%.

321. Fərəcova A.C. Pandemiya dövründə beynəlxalq təcrübədə informasiya təhlükəsizliyi / **Ümummilli lider Heydər Əliyevin anadan olmasının 98-ci ildönümünə**

həsr olunmuş tələbə və gənc tədqiqatçıların II beynəlxalq elmi konfransı, Bakı, **25-28 aprel 2021,** s. 429-431.

Məqalədə pandemiya dövründə beynəlxalq təcrübədə informasiya təhlükəsizliyi araşdırılmışdır. Koronavirus epidemiyasının dünyada geniş şəkildə yayılması məlumatların daha çox rəqəmsal şəkildə ötürülməsinə səbəb olmuşdur. Bu məlumatların əldə edilməsi, emalı və istifadəsi fərdlərin icazəsi ilə olmadığı təqdirdə informasiya təhlükəsizliyinə şərait yaradacaqdır. Bir sıra ölkələrdə eyni zamanda pandemiya şəraiti ilə birgə informasiya təhlükəsizliyinə səbəb olacaq problemlərlə də mübarizə aparılmağa başlanmışdır. Pandemiya dövründə informasiya təhlükəsizliyinin təmin olunması sahəsində Hollandiya, İngiltərə, Fransa, Berlin və Belarusiya kimi ölkələr tərəfindən görülən işlər və qəbul edilmiş qanunlar araşdırılmışdır.

322. Vəlixanlı O.V. Proqram məhsullarına olan hücumların müdafiəsi üsullarının analizi / **Ümummilli lider Heydər Əliyevin anadan olmasının 98-ci ildönümünə həsr olunmuş tələbə və gənc tədqiqatçıların II beynəlxalq elmi konfransı**, Bakı, **25-28 aprel 2021**, s. 426-428.

Məlumdur ki, proqram məhsullarına olan tələbat sürətlə artmaqdadır. Bu isə öz növbəsində onları hədəf alan hücumların sayının artması ilə nəticələnir. Məqalədə proqram məhsullarının müdafiəsi üçün irəli sürülmüş metodların analizi aparılmışdır. Analiz zamanı həm proqram həm də

avadanlıq əsaslı müdafiə metodlarına baxılmışdır. Hər bir metod haqqında ümumi məlumat verilmişdir.

323. Bağırov E.O. Klasterizasiya üsullarının zərərli proqramların aşkarlanmasına tətbiqi / **Ümummilli lider Heydər Əliyevin anadan olmasının 98-ci ildönümünə həsr olunmuş tələbə və gənc tədqiqatçıların II beynəlxalq elmi konfransı**, Bakı, **25-28 aprel 2021**, s. 437-439.

Bu işdə kateqoriya tipli verilənlərdən ibarət olan zərərli proqramların aşkarlanması üçün supervizorsuz öyrənmə metodu olan klasterizasiya üsullarından k-modes alqoritminin tətbiqinə baxılmışdır.

324. Махмудова Р.Ш., Дашдамирова К.Г. Проблемы информационной безопасности в информационном обществе / **XI Международная научно-техническая конференция "Информационные технологии в промышленности, логистике и социальной сфере",** Минск, **26–27 мая 2021,** с. 101-105.

В исследовании анализируются угрозы, которые могут затронуть интересы личности, общества и государства в условиях информационного общества. Изучен опыт зарубежных стран в области информационной безопасности. Были проанализированы текущая ситуация в области информационной безопасности в Азербайджане и научно-теоретические основы проблем информационной безопасности.

325. Imamverdiyev Y.N., Abdullayeva F.J. Convolutional neural network for detecting application layer distributed denial of service attacks / **XVI Международная научно-техническая конференция «Оптико-электронные приборы и устройства в системах распознавания образов и обработки изображений» (Распознавание–2021),** Курск, **14-17 сентября 2021,** с. 22-25.

Distributed Denial of Service(DDoS) is one of the main threats to information security.Application layer DDoS attaks (Al-DDoS) can be organized against many different applications.

326. Abdullayeva F.J., Ojagverdiyeva S.S. Detection of vulgarities in Web-content based on Naive Bayes algorithm / **XVI Международная научно-техническая конференция «Оптико-электронные приборы и устройства в системах распознавания образов и обработки изображений» (Распознавание–2021), Курск, 14-17 сентября 2021,** с. 12-14.

Protecting children from harmful information on the Internet is one of the most pressing issues/ The article proposes an approach using machine learning methods to detect vulgar words? phrases and expressions.

327. Abdullayeva F.J., Ibrahimov R. Development of acoustic system for detection of drones based on ensembles of audio features / **XVI Международная научно-техническая конференция «Оптико-**

электронные приборы и устройства в системах распознавания образов и обработки изображений» (Распознавание–2021), Курск, Россия, **14-17 сентября 2021,** с. 14-16.

One of the methods of detecting drones is the analysis of audio signals. In this case, spectral features were extracted from sound files by analyzing audio data. The Simple Neural Network Model (Simple NN) and the Convolutional Neural Network Model (CNN) were built to classify the extracted audio features. Asa result of experiments on real data, the Simple Neural Network showed superior results and achieved 98% detection accuracy.

328. Abdullayeva F.J., Valikhanli O.V. A method of detecting GPS spoofing attacks on Unmanned Aerial Vehicles / **XVI Международная научно-техническая конференция «Оптико-электронные приборы и устройства в системах распознавания образов и обработки изображений» (Распознавание–2021), Курск,** Россия, **14-17 сентября 2021,** с. 16-18.

In this paper, the detection method of GIPS spoofing attacks on UAV (Unmanned Aerial Vehicles), based on CNN (Convolutional Neural Network) is proposed.

329. Alguliyev R.M., Aliguliyev R.M., Abdullayeva F.D. The Improved LSTM and CNN Models for DdoS Attacks Prediction in Social Media. **Chapter 23.** USA: IGI Global, **2022.** 19 p.

Automatic identification of conversations related to DDoS events in social networking logs helps the organizations act proactively through early detection of negative and positive sentiments in cyberspace. In this article, the authors describe the novel application of a deep learning method to the automatic identification of negative and positive sentiments in large volumes of social networking texts. The authors present classifiers based on Convolutional Neural Network (CNN) and Long Short-Term Memory (LSTM) to address this problem domain. The improved CNN and LSTM architecture outperform the classification techniques that are common in this domain including classic CNN and classic LSTM in terms of classification performance, which is measured by recall, precision, f-measure, train loss, train accuracy, test loss, and test accuracy. In order to predict the occurrence probability of the DDoS events the next day, the negative and positive sentiments in social networking texts are used. To verify the efficacy of the proposed method experiments is conducted on Twitter data.

330. Əliyev Ə.Q., Şahverdiyeva R.O. Postkonflikt zonalarda iqtisadi informasiya sistemlərinə potensial ziyanların və təhlükələrin qiymətləndirilməsinə konseptual yanaşma // **Azərbaycan Ali Texniki Məktəblərinin Xəbərləri, 2022,** № 2, cild 24, s. 235-242.

Məqalə Azərbaycanın erməni işğalından azad edilmiş postkonflikt zonalarında iqtisadiyyatın və regional

strukturların bərpasında rəqəmsal transformasiyanın iqtisadi informasiya sistemlərinə ola bilən potensial ziyanların və təhlükələrin qeyri-səlis metodlarla qiymətləndirilməsinin konseptual əsaslarına həsr olunmuşdur. Regional iqtisadiyyatın bərpasında və onların inkişafında 4.0 Sənaye inqilabının tətbiqləri və beynəlxalq təşkilatların tövsiyələri nəzərə alınmaqla innovativ mühitin formalaşdırılmasında müvafiq İKT və informasiya sistemlərinin vacibliyi müəyyənləşdirilmişdir. Postkonflikt zonaların iqtisadi informasiya sistemlərinə potensial təhlükələr və ziyanların spektri göstərilmişdir. İnformasiya sistemlərinin təhlükəsizliyinə təhdidlər nəticəsində ola bilən potensial ziyanların növləri verilmiş, potensial ziyanların kompleks qiymətləndirilməsinə bəzi elmi-metodoloji yanaşmalar qeyd olunmuşdur. İnformasiya sistemlərinə potensial təhlükə və ziyanların qeyri-səlis qiymətləndirilməsi üçün təkliflər verilmişdir. İnformasiya sistemlərinin potensial ziyanlarının ekspertlər tərəfindən alınmış yekun qeyri-səlis çoxluqlarının emalı prinsipləri qeyd olunmuşdur. Göstərilmişdir ki, postkonflikt zonalarda iqtisadi informasiya sistemlərinə ola bilən potensial ziyanların qiymətləndirilməsi məsələlərinin həllində müasir texnologiya və metodların tətbiqi ilə effektiv nəticələrə nail olmaq mümkündür.

331. Сухостат Л.В. Обзор некоторых решений безопасности современных АСУ ТП // **Телекоммуникации**, 2022, № 2, с. 14-23.

В данной статье исследуются вопросы безопасности автоматизированных систем управления технологическими процессами (АСУ ТП). Представлен обзор по следующим направлениям: разработка отказоустойчивых протоколов, обнаружение вредоносных программ, защита персональных данных и контроль доступа. Данная работа дает понимание уязвимостей и существующих решений кибербезопасности АСУ ТП и освещает будущие направления исследований.

332. Мехдиев Ш.А. Анализ некоторых проблем надежности киберфизических систем // **Информационные технологии. Проблемы и решения, 2022, №** 1, т. 18, с. 63-69.

В процессе эксплуатации киберфизические системы (КФС) подвержены воздействию широкого спектра факторов, влияющих на их техническое состояние и безаварийное функционирование. Эта парадигма потребовала решения некоторых технических и научных проблем для обеспечения высокой надежности, кибербезопасности и киберустойчивости различных по назначению КФС на производстве, транспорте, в энергетике, коммунальном хозяйстве, строительстве, здравоохранении или в умных городах. Применения КФС могут быть направлены на снижение потребления ресурсов и улучшение общей эффективности процессов путем настройки под индивидуальные потребности.

КФС в инфраструктуре умного города повышают общественную безопасность в целом, а внедрение интеллектуальной системы управления беспилотным транспортом предотвращает возникновение заторов и уменьшает риски аварий со смертельным исходом. Сохранение ресурсов в умных киберфизических зданиях достигается за счет лучшего управления энергоэффективностью зданий. В результате сокращаются потери электроэнергии, воды и тепла. В сельском хозяйстве за счет постоянного наблюдения за окружающей средой минимизируются влияния неблагоприятных факторов на результаты труда аграриев. Диагностические параметры, характеризующие состояния компонентов и модулей КФС, формируются на основе данных от измерительных датчиков. Общее количество датчиков для этих целей непрерывно растет.

333. Shikhaliyev R.H. A method for intelligent planning of computer networks monitoring // **Problems of Information Technology, 2022,** vol. 13, no. 1, pp. 42-48.

To ensure the efficiency of management, the security of computer networks (CN), as well as to ensure the required level of quality of service for network applications, accurate and up-to-date information on the state of the CN is required. This information can be obtained through continuous active monitoring of the quantitative characteristics of the CN. Thus, active monitoring becomes an important tool for ensuring the

efficiency of management and security of the CN. However, continuous active monitoring, especially of large networks, can lead to congestion of network channels, which can reduce the effectiveness of monitoring the CN. Consequently, with active monitoring of the CN, it is necessary to manage the use of resources (channel and computational) of the network and reduce the load on the network. To solve this problem, this paper proposes a method for intelligent planning of monitoring of the CN. Using machine learning algorithms, can be analyzed the state and performance of the CN and acquire knowledge that can be used to determine the most appropriate rules for monitoring the CN. Thus, it is necessary to find such monitoring rules that will ensure the effectiveness of monitoring the CN. The proposed method can reduce the impact of monitoring on network performance, and on the operation of network applications.

334. Abdullayeva F.D., Valikhanli O.V. Development of a method for detecting GPS spoofing attacks on unmanned aerial vehicles // **Problems of Information Technology, 2022,** vol. 13, no. 1, pp. 3-8.

As in other vehicles, unmanned aerial vehicles (UAV) mainly use GPS (Global Positioning System) for the provision of navigation. Non-execution of necessary measures on UAV, availability of the devices used in the process of attack may cause GPS spoofing attack on UAV. The quick detection of the attack plays an important role in obtaining safety precautions.

The use of artificial neural networks in the detection of such attacks is very convenient. Therefore, in the article new approach based on convolutional neural network (CNN) method is proposed in order to detect GPS spoofing attack. The new approach has been developed for two different types of UAVs. As a result of conducted experiments, high-accuracy detection of GPS spoofing attack has been provided.

335. Mahmudova R.Sh. Analysis of international experience in the formation of a culture of information security in society // **Problems of Information Technology, 2022,** vol. 13, no. 1, pp. 85-94.

The rapid development of information and communication technologies, the increase in sources of information, the electronization of many services in all areas, the emergence of new means of communication between people, the collection of personal data in various information systems and other realities create new opportunities for development. On the other hand, the use of information to manipulate peoples minds, to create chaos in society, actualizes the development of a culture of information security in society. The article analyzes the experience of developed countries in the formation of information security culture. As part of the documents, challenges and measures taken by international organizations such as the UN, the Organization for Economic Cooperation and Development, the experience of individual countries in raising the level of information security culture of

professionals, citizens and various groups, as well as educators, children and youth, was studied and summarized. The study used methods of systematization, generalization, comparative analysis. The results of the study may be useful to institutions responsible for ensuring information security in society.

336. Hajirahimova M.S. Experimental study of machine learning methods in anomaly detection // **Problems of Information Technology, 2022,** vol. 13, no. 1, pp. 9-21.

Recently, the widespread usage of computer networks has led to the increase of network threats and attacks. Existing security systems and devices are insufficient in the detection of intruders" attacks on network infrastructure, and they considered to be outdated for storing and analyzing large network traffic data in terms of size, speed, and diversity. Detection of anomalies in network traffic data is one of the most important issues in providing network security. In the paper, we investigate the possibility of using machine learning algorithms in the detection of anomalies – DoS attacks in computer network traffic data on the WEKA software platform. Ensemble model consisting of several unsupervised classification algorithms has been proposed to increase the efficiency of classification algorithms. The effectiveness of the proposed model was studied using the NSL-KDD database. The proposed approach showed a higher accuracy in the detection of anomalies compared to the results shown by the classification algorithms separately.

337. Alakbarov R.K., Hashimov M.A. Fog computing technology application in cyber-physical systems and analysis of cybersecurity problems // **Problems of Information Technology, 2022,** vol. 13, no. 2, pp. 23-29.

New requirements for modern technologies have become a driving force in the development of information technology. New distributed computing systems are required to handle a large data flow generated by the application of the Internet of Things (IoT) and to ensure their efficient processing. Although cloud computing is an effective technology for processing and storing data generated in a networked environment, it has complications with the real time transmission of large amounts of data due to the low bandwidth of network. To speed up the data processing, fog computing systems have been widely used in recent years. Fog counting systems are one of the proposed solutions for working with IoT devices. Because it can meet the computing needs of multiple devices connected to the network. In these systems, the data is processed at computing nodes located near the data generating devices, which reduces the bandwidth complications of the network channel. In this regard, this article considers the application of fog computing technology in cyber-physical systems. It analyzes the fog technology architecture and its advantages over cloud computing. Cyber security problems arising when using fog technology in cyber-physical systems are analyzed and

available protection methods partially solving them are highlighted.

338. Nabiyev B.R. Investigation of clustering and classification methods for ıntellectual analysis of log files // **Problems of Information Technology, 2022,** vol. 13, no. 2, pp. 48-60.

Today, the application of information technology in all areas of our lives has led to wider spread and popularity of cybercrime. In modern industrial control systems and cyber-physical systems, log files are very important in terms of detecting cyber incidents, identifying and preventing threats and anomalies. However, today, a large volume of log files generated in these systems greatly complicates the process of extracting useful information from them. This, in turn, highlights the need for intellectual analysis of log files. To this end, this article explores a number of clustering and classification methods and algorithms for the intellectual analysis of log files. Thus, K-means, CURE, EM, kNN, Naive Bayes and DT algorithms are selected out of these algorithms and their working principle is studied, explained, and the application of each algorithm on KDD CUP 99 data set is studied and compared.

339. Abdullayeva F.D. Neural Network Moldels for Detection of Unmanned Aerial Vehicles Based on Spectrogram Analysis // **Problems of Information Technology, 2022,** vol. 13, no. 2, pp. 16-23.

The widespread use of unmanned aerial vehicles (UAVs) in both the national and military fields has made them the focus of industrial organizations. However, the use of UAVs has seriously affected the violation of the confidentiality of personal data, posed a threat to states, national institutions, nuclear power plants, historical places. One way to reduce this threat is to detect harmful UAVs. The article develops machine learning and deep learning methods based on sound signal analysis to detect harmful UAVs. Features were extracted from the sound signals and their ensemble was created. The created new data was transmitted to the input of neural network models in the form of vectors and drones were detected. The effectiveness of the proposed approach has been tested on a database open to scientific research.

340. Alakbarova I.Y. International experience and approaches to the intellectual analysis of behavior in the e-government environment // **Problems of Information Society, 2022**, vol. 13, no. 2, pp. 64-72.

The role of the Internet in people's daily lives, the impact of social networks on the formation of public opinion, the spread of mobile communications, the collection of personal information in electronic information systems in the e-government environment made the problem of "behavior analysis" even more relevant. In order to improve the efficiency of the public administration process during the formation of the information society, one of the most important tasks to be

performed by the government organizations is the correct assessment and prediction of citizens' behavior and making the right decisions. The main goal of the intellectual analysis of behavior is to understand the logic of the activities of individuals and social groups. This article studies the international practice in intellectual analysis of behavior, examines the methods and algorithms used in this area, and identifies problems. Proposals are developed for the effective solution of questions on the intellectual analysis of behavior in the e-government environment. The approach we propose for intellectual analysis of behavior based on textual information consists of 4 levels: 1) primary processing, 2) document description, 3) classification of a set of documents into positive and negative classes, 4) determination of accuracy and completeness characteristics in classification. The use of semantic indicators for intellectual analysis of behavior can help conduct research with greater accuracy and effectively solve behavioral prediction problems.

341. Abdullayeva F.D. Distributed denial of service attack detection in E-government cloud via data clustering // **Array, 2022,** vol. 15, pp. 1-12.

One of the main essential security issues of cloud computing is the detection and prevention of network intrusions. The gaps in the network directly affect the security of the cloud as it is the foundation of it. Attacks in the cloud are launched either by compromised nodes of the network outside of the cloud or by

virtual machines (VMs) within the cloud network. So, monitoring both external and internal traffic of the cloud network is of great importance. In this paper, a machine learning method performing accurate clustering of network data to detect DDoS attacks has been proposed. The method uses a feature selection technique to increase the efficiency of data clustering. To provide the feature selection the PCA algorithm has been used. For the dataset formed on selected features, the DBSCAN (density-based spatial clustering of applications with noise), Agglomerative Clustering, and k-means algorithms are applied. In the experiment, the clustering results of the methods using fewer features were higher on all metrics than the clustering results of the methods using all the features. Compared to the standard algorithms, the PCA + DBSCAN, PCA + Agglomerative, and PCA + k-means algorithms obtained higher values on the Adjusted Rand Index metric and reached 0.8989, 0.9130, 0.9094 values, respectively. The effectiveness of the approach also was evaluated on the other clustering metrics and obtained high results. The proposed system can be installed in both internal and external cloud infrastructure. This allows, to detect attacks on the external cloud network, as well as on the internal physical network or in the virtual network between hypervisors.

342. Alguliyev R.M., Abdullayeva F.D., Ojagverdiyeva S.S. Image-based malicious Internet content filtering method

for child protection // **Journal of Information Security and Applications, 2022**, no. 65, pp. 1-10.

Children and teenagers are among Internet users and they encounter harmful data in the global network. Young users often become the potential victims of pornographic images. Avoiding pornographic images harmful to the child audience is an important research task in the field of detection, computer vision and multimedia. Malicious content can be prevented using various methods. Current paper presents a ChildNet model that filters harmful image content. The pixels of the digital images are used as a data source for recognition of nudity in the images. For each class, a multi-layer deep neural network architecture with five convolution blocks is developed to study the color patterns of undesirable image pixels. The developed neural network consists of 21 layers; the size of the filters is specified as (3 × 3). The filter's size is reduced to increase the accuracy of pixel recognition. The efficiency of the proposed method is tested on real datasets for evaluation purposes and the superior results are obtained from the proposed method in comparison with classical CNN.

343. Abdullayeva F.D. Convolutional Neural Network-Based Automatic Diagnostic System for AL-DDoS Attacks Detection // **International Journal of Cyber Warfare and Terrorism,** 2022, vol. 12, no. 1, pp. 1-15.

Distributed denial of service (DDoS) attacks are one of the main threats to information security. The purpose of DDoS

attacks at the network (IP) and transport (TCP) layers is to consume the network bandwidth and deny service to legitimate users of the target system. Application layer DDoS attacks (AL-DDoS) can be organized against many different applications. Many of these attackstarget HTTP, in which case their goal is to deplete the resources of web services. Various schemes have been proposed to detect DDoS attacks on network and transport layers. There are very few works being done to detect AL-DDoS attacks. The development of an intelligent system automatically detecting AL-DDoS attacks in advance is very necessary. In this paper to detect AL-DDoS attacks a deep learning model based on the convolutional neural network is proposed. To simulate the AL-DDoS attack detection process, while in testing of the model on CSE-CIC-IDS2018 DDoS and CSIC 2010 datasets, 0.9974 and 0.9059 accuracy values were obtained, respectively.

344. Aliyev A.G., Shahverdiyeva R.O. Scientific and methodological bases of complex assessment of threats and damage to information systems of the digital economy // **International Journal of Information Engineering and Electronic Business, 2022,** no.2, pp. 23-38.

The article examines the scientific and methodological basis of a comprehensive assessment of threats and damage to information systems of the digital economy. The information infrastructure and tasks of the digital economy have been

defined. Sources of information security in the digital economy sectors and their information security requirements have been studied. The results of the analysis of the situation in the countries of the world on the Global Cyber security Index are shown schematically. The graph of the dynamics of cybersecurity expenditures in the ICT segments is shown. Cases of information security violations in the digital economy and the processes of assessing the damage caused by them have been studied. Generalized criteria for assessing information damage in the digital economy have been proposed. Threats to information and communication systems and classification of damage are given. A structural scheme of the conceptual model of threats and damage to information systems and resources in the field of digital economy of Azerbaijan has been proposed. An expert description of the ways in which information threats are disseminated has been developed using a fuzzy approach. The main types of damage caused by threats to the security of information systems are given. The security aspects of the abundance and surplus of information in the digital economy are shown. The directions of increasing the level of security and confidence in the digital economy and the structures to ensure its security are given. The main directions of information security in the digital economy have been identified, the directions of ensuring its security and increasing its confidence have been identified. Some methodological approaches to integrated risk and damage assessment in the digital economy

have been explored. A scientific-methodological approach based on fuzzy methods has been proposed for the implementation of complex risk and damage assessment in the digital economy.

345. Dashdamirova K.G. Development of decision support system using OLAP-technologies for information security monitoring systems // **Проблемы программирования**, **2022,** no. 1, pp. 403-408.

The article highlighted the need for continuous monitoring of the computer networks (CN) for information security and analyzed the sources of data for information security monitoring (ISM). Methods of data collection from various sources have been investigated, and categories of ISM systems have been studied. The architectural-technological model of the system supporting decision-making based on OLAP (Online Analytical Processing) and data warehouse has been proposed for quick response to security-related incidents and detected incidents in ISM systems.

346. Abdullayeva F.D. Internet of Things-based healthcare system on patient demographic data in Health 4.0 // **CAAI Transactions on Intelligence Technology, 2022,** vol. 7, ıssue 4, pp. 644-657.

In this paper, a comprehensive analysis of machine learning approaches in the field of diagnosing COVID-19 has been conducted, and for the detection of chronic diseases in patients, to identify symptoms of COVID-19 virus infection in advance, and control the situation a healthcare system has been

proposed. The constructed system provides real-time monitoring of chronic diseases and COVID-19 virus infection in patients. The proposed system consists of five layers: IoT sensor layer, Data transmission layer, Fog layer, Cloud layer, the Application layer. The system architecture in the Fog layer uses machine learning and deep learning algorithms to diagnose patients" diseases, to generate and send diagnostic and emergency alerts to users. The classification module of the system"s Fog layer categorises the patient"s health status into healthy and unhealthy classes. In this module, to classify medical data the Decision Tree, Random Forest, SVM, Gradient Boosting, Logistic Regression algorithms are used. The COVID-19 dataset is used to test the effectiveness of the methods. The best results from the comparative analysis of the methods are obtained from the Decision Tree, Random Forest, and Gradient Boosting algorithms, which are recognised data points with high accuracy and on the accuracy metric reached 1.0, 0.99, 1.0 values, respectively. The classification of the other two SVM and Logistic Regression algorithms provided the worst results, and the accuracy score of both classifiers obtained a 0.89 value.

347. Aliyev A.G. Study of development trends and application risks of cryptocurrency and blockchain technologies in the digital environment // **Informatica Economica, 2022,** vol. 26, no. 3, pp. 37-49.

The paper is devoted to the study of the formation and development trends of cryptocurrency and blockchain technologies in the digital economic environment, as well as the risks and dangers of their application. According to the features of classification, the main features of virtual currencies have been explained. The risks and dangers that may arise with the regular use of cryptocurrency and blockchain technologies emerging in the digital environment were considered. The possibilities of applying cryptocurrency and blockchain technologies in economic structures and processes in the new economic environment have been explored. The security features of blockchain technology and the mechanism of operation of the cryptocurrency have been explained. The differences between cryptocurrency and traditional money have been explained, and the essence of different approaches to cryptocurrencies in the international arena has been analyzed. Statistical analysis of scientific publications on cryptocurrencies has been conducted. The capitalization dynamics of cryptocurrency are presented. The rating of cryptocurrencies is shown according to the level of capitalization. The dynamics of price changes in Bitcoin are given. The structural content of cryptocurrencies and blockchain technologies was explained, and their application in economic operations was studied. The risks and dangers of cryptocurrency in the digital environment were analyzed. The mechanism of their operation in business and financial

operations was explained. The dangers of the use of cryptocurrencies in the existing traditional financial system have been identified. The problems of legal regulation of cryptocurrencies in the world have been analyzed. In the 4.0 Industrial Platform in the Digital Environment, some recommendations have been given for preventing the risks and dangers of using cryptocurrency and blockchain technologies.

348. Kazimov T.H., Bayramova T.A. Development of a hybrid method for calculation of software complexity // **System Research & Information Technologies, 2022**, no. 2, pp. 32-44.

The use of code metrics allows software developers and project managers to evaluate various features of the software (to be built or already in existence), predict workload, determine software complexity and reliability, and quantify the quality of software systems being developed. Articles written in recent years have proposed various methods for solving this problem. However, there is still no very effective approach to measuring software complexity. This article provides a brief overview of existing software complexity metrics and proposes a new hybrid method for computing software complexity. The proposed hybrid method for evaluating software complexity combines the key features of the Halsted, Maccabe, and SLOC metrics and also allows for a more efficient assessment of complexity.

349. Aliyev A.G. Technologies ensuring the sustainability of information security of the İnformation of the digital economy and their perspective development directions // **Information Engineering and Electronic Business, 2022,** vol. 14, no. 5, pp. 1-14.

The article is devoted to the technologies to ensure the sustainability of information security in the formation of the digital economy and their prospects. It has been shown that the digital transformation of the economy and society is a priority for the advanced countries of the world. It was argued that the safe and sustainable formation of an intellectual society and economy based on new information, knowledge and technology is one of the main goals. The features of the transition from an industrial economy to a new ICT-based information economy were analyzed. The issues of digital transformation of real economic sectors were considered. It was noted that ensuring the development of the modern economy on the basis of digital technologies, the development of high-tech sectors is one of the main goals. Potential areas for digitization of the economy have been identified. The economic features of the main technologies that shape the digital economy have been studied. The stages of analysis of the secure development of the digital economy sectors have been developed. Many concepts of the digital economy are systematized and approaches to its features are explained. Forecast options for the impact of the digital economy on GDP in the countries of the world are given.

Mechanisms to ensure economic security, investment forecasts made by different countries to ensure economic cybersecurity are given. Research on the level of economic security and the main threats to the economy was analyzed. The main directions of security of the national economy and the main factors affecting the economic security of the country have been identified. Current approaches to economic security are summarized. The main types of economic security are given and a system of indicators is defined. The structural elements of the system of indicators for the analysis of economic security are proposed. System indicators have been developed to analyze the sustainability of economic security. Criteria for assessing the sustainability of regional economic security have been proposed. An analysis of the state of growth in the field of cyberattacks in different years and the main stages of the evolution of cybersecurity are described.

350. Aliyev A.G. Research of risks and threats of using cryptocurrency and blockchain technologies in the digital environment // **Информационные технологии. Проблемы и решения, 2022,** № 4(21), pp. 55-61.

The article is devoted to the study of the risks and dangers that may arise with the regular use of cryptocurrencies and blockchain technologies in the digital environment. The application of cryptocurrencies and blockchain technologies in economic structures and processes has been explored. The security features of blockchain technology and the working

mechanism of cryptocurrency are explained. The differences between cryptocurrency and traditional money are explained, and the existence of different approaches to cryptocurrencies in the international arena is shown. Cryptocurrency risks and threats were analyzed in the digital environment. The dangers of the use of cryptocurrencies in the existing traditional financial system have been identified. The problems of legal regulation of cryptocurrencies in the world have been analyzed. Recommendations on the risks and dangers of using cryptocurrencies and blockchain technologies in the digital environment in the 4.0 Industrial Platform were given.

351. Əliyev Ə.Q. Regional sosial-iqtisadi inkişafın keyfiyyətliliyinin təminində onun kiberdayanıqlılığının artırılması məsələləri / **Ümummilli Lider Heydər Əliyevin anadan olmasinin 99-cu ildönümünə həsr olunmuş "Regionlarin sosial-iqtisadi inkişafinin yeni keyfiyyət mərhələsinə yüksəlməsində rəqəmsal iqtisadiyyatin rolu"**, Lənkəran, **6 may 2022**, s. 17-19.

Təqdim olunan işdə regional sosial-iqtisadi inkişafın keyfiyyətliliyi aspektində kiberdayanıqlılığın artırılması məsələlərinə baxılmışdır. Sosial-iqtisadi inkişafa rəqəmsal iqtisadiyyatın təsiri təhlil olunaraq kiberdayanıqlığın zəruriliyi əsaslandırılmış, onun ölçülməsinə olan baxışlar araşdırılmışdır. Müvafiq sahədə meyarlar təklif edilmiş, kiberdayanıqlılığın artırılması üzrə bəzi tövsiyələr verilmişdir.

352. Fətəliyev T.X. Elm mühitində kritik infrastrukturların kiberdayanıqlığı / **"Vətən müharibəsi: 44 günlük zəfər səlnaməsi" respublika elmi-praktik konfransı,** Bakı, **2-3 noyabr 2022**, s. 138-141.

Sənaye 4.0 ideologiyasının təsiri altında elmin yeni keyfiyyətdə təkamülünü həyata keçirən Elm 4.0 çərçivəsində kritik infrastrukturların kiber dayanıqlığının tədqiqi aktual məsələ kimi qarşıya qoyulmuş və əsas nəticələr təqdim olunmuşdur.

353. Şıxəliyeva N.R. Tibbi sosial şəbəkələrdə fərdi məlumatların təhlükəsizliyi / **Ümummilli lider Heydər Əliyevin anadan olmasının 99-ci ildönümünə həsr olunmuş tələbə və gənc tədqiqatçıların III beynəlxalq elmi konfransı,** Bakı, **18-29 aprel 2022,** s. 207-209.

Məqalədə tibbi sosial şəbəkələrdə istifadəçilərin fərdi tibbi məlumatlarının təhlükəsizliyi ilə əlaqədar bir sıra problemlər göstərilmişdir. Pasiyentlər onları maraqlandıran problemlərin həlli üçün sosial mediaya müraciət edir, peşəkar saytlarda qeydiyyatdan keçirək məlumatlardan yararlanmağa çalışırlar. Qeydiyyatdan keçən pasiyentlər fərdi tibbi məlumatlarını qeyd etməli olurlar. Bu isə fərdi məlumatların konfidensiallıq siyasətinin zəif olduğu tibbi sosial mediada pasiyentlərin fərdi məlumatlarının konfidensiallığına xələl gətirə bilər.

354. Vəlixanlı O.V. Kibertəhlükəsizliyin təmin olunması üçün PUA naviqasiyasında istifadə olunan mövcud metodların analizi / **Ümummilli lider Heydər Əliyevin anadan olmasının 99-cu ildönümünə həsr olunmuş**

tələbə və gənc tədqiqatçıların III beynəlxalq elmi konfransları, Bakı, **18-29 aprel 2022,** s. 209-211.

Məqalədə Pilotsuz Uçuş Aparatlarının (PUA) avtonom naviqasiyasının təmin olunması üçün müxtəlif metodlara baxılmışdır. Bu metodlara GPS naviqasiya sistemi, visual odometriya (ing. visual odometry) və ətalət ölçü cihazından (ing. Inertial Measurement Unit, IMU) istifadə daxildir. Məqalədə qeyd edilən metodların hər biri haqqında ayrıca məlumat verilmişdir. Bundan əlavə metodların müsbət və mənfi cəhətləri də vurğulanmışdır. Sonda isə bu metodların birlikdə istifadə edilməsinə aid nümunə göstərilmişdir.

355. Abdullayeva F.C., Ocaqverdiyeva S.S. Qeyri-səlis məntiqi çıxarış əsasında uşaqların informasiyaya girişinin idarə edilməsi metodu / "**İnformasiya sistemləri və texnologiyalar: nailiyyətlər və perspektivlər" III beynəlxalq elmi konfransı**, Sumqayıt, **8-9 dekabr 2022**, s. 63-65.

Məruzə materialında Mamdani qeyri-səlis məntiqi çıxarış sistemindən istifadə etməklə uşaqların onlayn mühitdə qorunmasını həyata keçirən bir yanaşma verilir. Bu yanaşmada uşaqların bir neçə fərdi parametri (yaşı, ürək və göz xəstəliyi, psixoloji vəziyyəti) nəzərə alınmaqla onların rəqəmsal texnologiyalardan istifadəsi zamanı informasiyaya girişinə nəzarət edən və ekran vaxtının düzgün təyin edilməsini həyata keçirən sistem təklif edilir.

356. Bayramova T.A. Proqram təminatı xətalarının klassifikasiyası / "**İnformasiya sistemləri və texnologiyalar: nailiyyətlər və perspektivlər" III beynəlxalq elmi konfransı**, Sumqayıt, **8-9 dekabr 2022**, s. 256-258.

Proqram təminatında olan xətaların axtarılması və aradan qaldırılması üçün metodları nəzərdən Keçirməzdən əvvəl proqram təminatında ən çox rast gəlinən səhvləri, xətaların yaranma səbəblərini, ciddiliyini və aradan qaldırılma prioritetini araşdırmaq lazımdır.

357. Mahmudova R.Ş., Əbdülhüseynova X.M. Müasir dövrdə uşaq və yeniyetmələrin informasiya təhlükəsizliyi problemləri / **"Yeni dövrdə təhsil və tədqiqat fəaliyyəti: reallıqlar və çağırışlar" Beynəlxalq elmi konfransı,** Mingəçevir, **16-17 dekabr 2022**, s. 535-538.

Məqalədə elektron məkanda uşaq və yeniyetmələrin məruz qaldığı təhlükələr, onların qarşısının alınması məsələləri ilə bağlı beynəlxalq təcrübə analiz edilmişdir. Ölkəmizdə informasiya təhlükəsizliyinin təmin edilməsi, o cümlədən qanunvericilik bazasının formalaşdırılması və inkişaf etdirilməsi istiqamətində həyata keçirilmiş tədbirlər, qəbul edilmiş mühüm normativ-hüquqi sınədlər araşdırılmışdır. Uşaq və yeniyetmələrin informasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması üçün təkliflər verilmişdir.

358. Rzayeva N.A. Kiberfiziki sistemlərdə təhdidlər və onların təsnifatı **"Yeni dövrdə təhsil və tədqiqat fəaliyyəti: reallıqlar və çağırışlar" Beynəlxalq elmi konfransı**, Mingəçevir, **16-17 dekabr 2022**, s. 717-720.

Məruzədə kiber-fiziki sistemlər, informasiya təhlükəsizliyi və avtomatlaşdırılmış informasiya sistemlərinə təsir edəcək mümkün təhlükələrin təhlili təsnifatlaşdırılmışdır. Kiber-fiziki sistemlərdə informasiya təhlükəsizliyinin təsnifatı bir neçə kriteriya əsasında yerinə yetirilməsi qısa şəkildə şərh edilmişdir.

359. Набибекова Г.Ч. Применение технологии блокчейн в OLAP-системах / **XXI Международная научно-техническая конференция «Развитие информатизации и государственной системы научно-технической информации (РИНТИ-2022)»**, Минск, **17 ноября 2022**, с. 202-207.

Проведен анализ работ, посвященных различным подходам к применению технологии блокчейн для обеспечения информационной безопасности баз данных в OLAP-системах. Было предложено использовать частный блокчейн для защиты данных электронной демографической системы, функционирующей в среде электронного государства.

360. Дашдамирова К.Г. Система поддержки принятия решений в среде мониторинга информационной безопасности / **XXI Международная научно-**

техническая конференция «Развитие информатизации и государственной системы научно-технической информации (РИНТИ-2022)» Минск, **17 ноября 2022**, с. 95-99.

Предложена архитектурно-технологическая модель системы поддержки принятия решений на основе технологии OLAP (Online Analytical Processing) и хранилища данных с целью быстрого реагирования на инциденты, связанные с нарушениями безопасности в системах мониторинга информационной безопасности и оказания поддержки лицам, принимающим решения, а также совершенствования аналитической деятельности в данной области.

361. Дашдамирова К.Г. Киберсоциально технологические проблемы и перспективы сетевого общества в условиях Индустрии 4.0 / **4-ая Международная конференция "Современные сетевые технологии" (MoNeTec-2022**), Москва, **27-29 октября 2022,** с. 55-61.

В статье проанализирована эволюция развития сетевого общества. Исследовано влияние промышленных революций на формирование Общества 3.0 и Общества 4.0. Проанализированы новые возможности, которые Индустрия 4.0 привнесла в жизнь сетевого общества. Отмечено, что начался процесс создания Общества 5.0 – суперинтеллектуального общества. Проанализировано современное состояние цифровых технологий, влияющих

на технологическое и социальное развитие общества, исследованы интернетсоциотехнологические проблемы сетевого общества. Показано, что многие инновации, которые Индустрия 4.0 привносит в жизнь сетевого общества, усугубят многие проблемы. Даны рекомендации для устойчивого развития общества. Проанализированы работы, проделанные в Азербайджане, и основные направления научных исследований в рамках Индустрии 4.0.

362. Дашдамирова Ж.М. Криптовалюты, блокчейн технологии, роль и перспективы в цифровой экономике / **III Международная научная конференция «Информационные системы и технологии: достижения и перспективы»**, Сумгаит, **08-09 декабря 2022,** с. 202-204.

Статья основана на исследованиях криптовалюты, а также технологии блокчейн. Также рассмотрена сущность и применение криптовалюты как инновационного инструмента в современной цифровизированной экономике, необходимость внедрения в современную систему, доказано на законодательном уровне обязанность признания их правового статуса. Вследствие инновации современных технологий возникает необходимость в переменах способов хранения и передачи информации, а также её защите, в реформировании правового статуса новых технологий,

связанных с кибербезопасностью, в том числе инноваций в области цифрового права. Рассмотрены перспективы формирования криптовалюты как международной валюты. Популярность крипты в мире определена тем, что она не привязана ни к какой-либо стране или государственной структуре. Исследованы главные достоинства и недостатки криптовалюты.

363. Гашимов М.А. Вопросы кибербезопасности сервисов «умный город» / **3-я международная научно-практическая конференция «Облачные и распределенные вычислительные системы в электронном управлении» ОРВСЭУ-2022 в рамках Национального Суперкомпьютерного Форума,** Переславль-Залесский**, 29 ноября - 2 декабря 2022,** с. 176-181.

Одним из новых направлений, предложенных для решения различных проблем городов в последнее десятилетие, является концепция «Умный город» (УГ). Эта концепция использует современные технологии, применяет инновации и предлагает высокое качество жизни. «Умный город» анализирует ситуации, происходящие в районе, предлагает технологические решения для улучшения его развития и качества жизни горожан. В данной статье также представлена информация о преимуществах сервисов, которые охватывают среду «умного города» для граждан и государственных учреждений. С другой

стороны, хотя «умный город» рассматривается как перспективное решение для предоставления эффективных услуг гражданам с использованием информационно-коммуникационных технологий, он подвержен различным угрозам безопасности. Одной из важнейших проблем, связанных с широким распространением и реализацией концепции «Умный город», является ее кибербезопасность. С этой целью в статье проанализированы проблемы кибербезопасности, возникающие при использовании сервисов «умного города».

364. Мехдиев Ш.А., Фаталиев Т.Х. Кіберстійкість критичних інфраструктур науки / **V Міжнародна науково-практична конференція**, Кропивницький, **19–20 травня 2022**, с. 7-8.

Among the many problems that arise during the transformation of science under the influence of Industry 4.0 technologies, ensuring comprehensive security and cyber resilience is relevant, which is studied in the work. Problems on this issue are grouped and solutions are given.

365. Aliyev A.G. Formation and development tendencies of cryptocurrencies and blockchain technologies in the digital economy / **Глобальные проблемы модернизации национальной экономики. Материалы XI международной научно-практической конференции,** Москва, **18 мая 2022,** pp. 124-131.

The article is devoted to the study of the formation and development trends of cryptocurrency and blockchain technologies in the digital economy. It is shown that the study of the formation and development of cryptocurrencies and blockchain technologies as a result of the transformation of digital technologies is a topical issue. The essence and structural content of cryptocurrencies and blockchain technologies were explained, and their application in economic operations was studied. The mechanism of operation of blockchain technology and cryptocurrency in business and financial operations is explained. The differences between cryptocurrencies and traditional currencies have been compared. Recommendations were made on the use of cryptocurrency and blockchain technologies in the digital environment. It was noted that the use of such technologies in the digital environment can give new impetus to the future development of the modern economy.

366. Hashimov M.A. Personal Data Security Problems in Smart City Environment / **Cybersecurity for Critical Infrastructure Protection via Reflection of Industrial Control Systems, NATO Science for Peace and Security Series D: Information and Communication Security,** Amsterdam, **27-29 October 2022**, pp. 65-71.

The concept of smart city is considered as a promising solution to provide effective services to citizens through information and communication technologies. However, the data sensed

through various devices when using smart city services poses problems for the security of citizens personal data. To this end, the article analyzes the issues of personal data security in the smart city environment and presents suggestions to solve them to some extent.

367. Valikhanli O.V. Methods of Detecting Cyber-Attacks on Unmanned Aerial Vehicles: A Survey / **Cybersecurity for Critical Infrastructure Protection via Reflection of Industrial Control Systems, NATO Science for Peace and Security Series D: Information and Communication Security,** Amsterdam, **27-29 October 2022**, pp. 40-47.

This paper covers a wide range of issues related to the cyber security of unmanned aerial vehicles (UAVs). It highlights the most common attacks which target UAVs. Moreover, it examines and compares the methods for detecting these types of attacks. As a result of the comparison, the advantages and disadvantages of such methods are discussed.

368. Abdullayeva F.J., Ibrahimov R. Comparative Analysis of Methods for Detecting Unmanned Aerial Vehicles / **Cybersecurity for Critical Infrastructure Protection via Reflection of Industrial Control Systems, NATO Science for Peace and Security Series D: Information and Communication Security,** Amsterdam, **27-29 October 2022**, pp. 56-64.

The widespread use of UAVs in both the national and military spheres has made them the focus of industrial organizations. However, the use of drones has seriously affected the violation of the confidentiality of personal data, posed a threat to states, national institutions, nuclear power plants, historical sites. One of the methods to reduce this threat is to detect malicious drones. The paper analyzes the existing methods in the detection of harmful drones and proposes a new approach to their detection.

369. Alguliyev R.M., Mahmudov R.Sh. Formation of Cyber-Physical Systems in Azerbaijan and Some Topical Problems of Their Complex Security / **Cybersecurity for Critical Infrastructure Protection via Reflection of Industrial Control Systems, NATO Science for Peace and Security Series D: Information and Communication Security,** Amsterdam, **27-29 October 2022**, pp. 81-89.

The article examines the formation of cyber-physical systems in Azerbaijan and some topical problems of their complex security. Moreover, the article highlights the features and problems of digital transformation of state institutions effected by cyber-physical systems. It classifies the main pillars of cyber-physical systems (algorithmic security, resistance to denials, power supply security, artificial intelligence security, functional reliability, structural reliability, adaptability, human factor). The need to improve the network and

communication infrastructure is justified. The ways to develop the field of Soft Engineering for the regular operation of cyber-physical systems at the national level, to solve some issues related to chip supply, protection of personal data, existing legal problems, and certain personnel are shown. Correspondingly, the main research trends in the field of cyber-physical systems are identified.

370. Alakbarov R.K., Hashimov M.A. Security Issues of Cloud-Based SCADA Systems / **Cybersecurity for Critical Infrastructure Protection via Reflection of Industrial Control Systems, NATO Science for Peace and Security Series D: Information and Communication Security,** Amsterdam, **27-29 October 2022**, pp. 1-8.

    In order to solve the problem posed in the article, the characteristics of Industry 4.0 (Fourth Industrial Revolution) are considered. In addition, the possibility of threats to the data security of an electronic demographic (e-demographic) decision support system (DSS) from intruders in the context of Industry 4.0 is considered, due to the attack risks for them is very high. It is found out that the damage to these data will affect the decision-making in the field of demography, and, consequently, on the course of demographic processes in the region. Solution ways of arisen problems are indicated.

371. Abdullayeva F.J. Cybersecurity Issues of Some Class Unmanned Aerial Vehicle Systems: A Survey /

Cybersecurity for Critical Infrastructure Protection via Reflection of Industrial Control Systems, NATO Science for Peace and Security Series D: Information and Communication Security, Amsterdam, **27-29 October 2022**, pp. 31-39.

The application of Unmanned Aerial Vehicles in various areas created problems in the field of cybersecurity, privacy, safety. Gaps in the security system of UAVs allow them to be easily hijacked. The article analyses the security issues of UAVs, reviews their attacks scenarios, and proposes a fuzzy approach to the automatic selection of effective mechanisms to prevent identified attacks. The Drone Backbone Model has been developed to show the impact of attacks on UAVs at different levels. The Backbone Model allows a numerical assessment of the impact of the attack on the system.

372. Fataliyev T.X., Verdiyeva N.N. Science 4.0: Complex Security Problems and Solution Mechanisms / **Cybersecurity for Critical Infrastructure Protection via Reflection of Industrial Control Systems, NATO Science for Peace and Security Series D: Information and Communication Security,** Amsterdam, **27-29 October 2022,** pp. 151-152.

It is supposed to consider the conceptual issues of the reconstruction of science as a corporate environment of Science 4.0 based on the key technologies of Industry 4.0 – Internet of Things, Cyber-Physical Systems, Artificial Intelligence, Cloud

computing, Big Data analytics and other Smart solutions. eScience is considered to be the technological base of Science 4.0. Complex security problems and their solution mechanisms are investigated within Science 4.0.

373. Shikhaliyev R.H. Some Approaches to Intellectual Monitoring of Industrial Control Systems Cybersecurity / **Cybersecurity for Critical Infrastructure Protection via Reflection of Industrial Control Systems, NATO Science for Peace and Security Series D: Information and Communication Security,** Amsterdam, **27-29 October 2022,** pp. 168-169.

For the security of the modern industrial control systems (ICS) basic protective tools can be used. These tools can protect against common attacks and be sufficient for low-risk systems. The required security level of the ICS be ensured by constantly monitoring. With the increase of the monitoring data volume, increase the costs of ICS resources consumption, as well as the data analysis becomes more complicated. It is necessary to intellectualize the security monitoring of the ICS. The purpose of this article is to study the approaches to the intellectualization of monitoring the security of ICS

374. Ojagverdiyeva S.S. About a Comprehensive Approach to Ensuring the Children's Safety in Terms of Industry 4.0 / **Cybersecurity for Critical Infrastructure Protection via Reflection of Industrial Control Systems, NATO Science for Peace and Security Series D: Information**

and Communication Security, Amsterdam, **27-29 October 2022,** pp. 171 - 172.

This study provides information on the concept of the safety of children's data environment. It highlights the concept of Children 4.0, which offers a comprehensive approach to ensuring the safety of data included in databases (medical data safety, spatial data safety, etc.) through wearable devices. This approach is also very important in protecting children's personal data.

375. Sukhostat L.V. Anomaly Detection in Industrial Control System Based on the Hierarchical Hidden Markov Model / **Cybersecurity for Critical Infrastructure Protection via Reflection of Industrial Control Systems, NATO Science for Peace and Security Series D: Information and Communication Security,** Amsterdam, **27-29 October 2022,** pp. 48 - 55.

An approach based on a hierarchical hidden Markov model for anomaly detection in industrial control systems is proposed. The signals of the system components are fed to the input of the proposed model. The hidden state is an independent probabilistic model, so each state is also a hidden Markov model. In the proposed model, the detection of anomalies according to the readings of the industrial control system sensors is combined with modeling at the event level. The model has several levels, and the event is modeled at the highest level. The approach is evaluated on a secure water treatment

dataset and compared with the results of the previous work, which showed that the proposed model is better in terms of recall and F-measure metrics and amounted to 0.9164 and 0.9563, respectively.

376. Bayramova T.A. Analysis of Modern Methods for Detecting Vulnerabilities in Software for Industrial Information Systems / **Cybersecurity for Critical Infrastructure Protection via Reflection of Industrial Control Systems, NATO Science for Peace and Security Series D: Information and Communication Security,** Amsterdam, **27-29 October 2022,** pp. 160-162.

    Errors and vulnerabilities in software are analyzed and problems of their detection are considered. Existing modern methods of vulnerability detection using artificial intelligence technologies are studied. In addition to detecting these cybersecurity vulnerabilities in a timely manner, it specifies the correct choice of software development technologies, methods and operating conditions to prevent them.

377. Mehdiyev Sh.A. On Monitoring the Technical Condition and Technological Safety of Functional Elements of the Cyber-Physical Infrastructure / **Cybersecurity for Critical Infrastructure Protection via Reflection of Industrial Control Systems, NATO Science for Peace and Security Series D: Information and Communication Security,** Amsterdam, **27-29 October 2022,** pp.18-26.

During operation, yber-physical systems (CPS) are constantly exposed to a wide range of factors that affect their technical condition in different ways. CPS combine a huge number of sensors and actuators to interact with each other and with the environment. The collection and processing of signals from sensors that measure the physical parameters of processes are carried out to identify anomalies and predict the state of the system to ensure its functional safety and optimal functioning. As the interaction in the CPS environment increases, physical systems become more vulnerable to threats. Understanding threats and their consequences, identifying the unique properties of CPS are key trends in ensuring their functional security. The degree of readiness of the CPS to perform the tasks and functions assigned to them essentially depends on the uninterrupted autonomous power supply of the installed sensors.

378. Aghayev F.T., Mammadova G.A., Zeynalova L.A., Malikova R.T. Problems and Methods of Information Security in Electronic Education / **Cybersecurity for Critical Infrastructure Protection via Reflection of Industrial Control Systems, NATO Science for Peace and Security Series D: Information and Communication Security,** Amsterdam, **27-29 October 2022,** pp. 146-147.

The popularity of e-education has been growing in recent years. Because of it, the problem of ensuring its security arises,

which must be carried out using security methods and internationally recognized standards. This article identifies various problems of personal data security in e-education and proposes solutions to ensure the protection of educational information.

379. Nabibayova G.Ch. Analysis and Research of the Impact of Industry 4.0: Challenges on Demographic Processes / **Cybersecurity for Critical Infrastructure Protection via Reflection of Industrial Control Systems, NATO Science for Peace and Security Series D: Information and Communication Security,** Amsterdam, **27-29 October 2022,** pp. 153-155.

In order to solve the problem posed in the article, the characteristics of Industry 4.0 (Fourth Industrial Revolution) are considered. In addition, the possibility of threats to the data security of an electronic demographic (e-demographic) decision support system (DSS) from intruders in the context of Industry 4.0 is considered, due to the attack risks for them is very high. It is found out that the damage to these data will affect the decision-making in the field of demography, and, consequently, on the course of demographic processes in the region. Solution ways of arisen problems are indicated.

380. Alakbarova I.Y. On One Approach for Detecting Social Relationships by Analyzing Video Images in E-Government / I.Y. Alakbarova // **Cybersecurity for Critical Infrastructure Protection via Reflection of**

Industrial Control Systems, NATO Science for Peace and Security Series D: Information and Communication Security, Amsterdam, **27-29 October 2022,** pp. 163 - 164.

In the modern world, video surveillance (CCTV) cameras are installed in all areas where it is important to strengthen security: in healthcare, education, sports and many other areas. The fact that the information collected from CCTV cameras is big data and most of it is not structured makes it relevant to use artificial intelligence and big data technologies in the analysis of this data. The purpose of this article is to develop an architectural diagram of an intelligent video surveillance system.

381. Mahmudova Sh.J. Development of an Intelligent Software System to Ensure Cyber Security Through Ontology **Cybersecurity for Critical Infrastructure Protection via Reflection of Industrial Control Systems, NATO Science for Peace and Security Series D: Information and Communication Security,** Amsterdam, **27-29 October 2022,** pp. 27 - 30.

This study reviews software security, etc. It studies the methods for the analysis of software security. The problems of software protection are identified. The risks for software projects, their management, determination and categories are studied. The article describes the ontology of cybersecurity based on standards. The main concepts related to cybersecurity

problem and their relationships are reviewed. It studies basic structure, concept, etc. of intelligent software system to ensure cybersecurity.

382. Dashdamirova K.G. Cyber Socio-Technological Problems of the Networked Society and Their Analysis / **Cybersecurity for Critical Infrastructure Protection via Reflection of Industrial Control Systems, NATO Science for Peace and Security Series D: Information and Communication Security,** Amsterdam, **27-29 October 2022,** pp. 156-157.

The article analyzes the history of the evolution of society and the internet socio-technological problems of the networked society are investigated.

383. Alakbarov O.R. Cyber Security Issues of Smart Devices in E-Health: A Review / **Cybersecurity for Critical Infrastructure Protection via Reflection of Industrial Control Systems, NATO Science for Peace and Security Series D: Information and Communication Security,** Amsterdam, **27-29 October 2022,** pp. 165-166.

The term e-health is generally used to refer to the application of information technology in the delivery of different types of healthcare services. The use of technology in healthcare not only makes life easier for people, but also raises a number security issues. The article discuses and providers solutions for the security of smart devices and patient information stored in cloud services. Also considered were the methods of further

enhancing the security of the electronic health system. Besides, the architecture and safety standards of smart hospitals have been researched.

384. Nabiyev B.R. Investigation of Computer Incidents for Cyber-Physical Infrastructures in Industrial Control Systems / **Cybersecurity for Critical Infrastructure Protection via Reflection of Industrial Control Systems, NATO Science for Peace and Security Series D: Information and Communication Security,** Amsterdam, **27-29 October 2022,** pp. 125-130.

Cyber-physical infrastructures in industrial control systems, including critical infrastructure and manufacturing, heavily on cyber-physical infrastructures and embedded devices. As industrial control systems become more complex and network-centric, physical infrastructure becomes increasingly dispersed and vulnerable. In rapid growth within the competitive technology, we have seen an expressive increase in information security vulnerabilities against such systems, ranging from simple hacking tools to new generation intelligent attacks. With the growing reliance on industrial control networks and, of course, the growing number of attacks, the lack of cyber-security monitoring and forensic analysis of security incidents. Cyber-forensic analysis of ICS/SCADA systems is unlike standard forensic analysis of enterprise computer systems, the cyber-forensic specialist often has to be an expert in cyber-physical infrastructures systems, networks, and devices to

determine where potential forensic evidence may be located. This paper discusses ICS/SCADA, typical attacks and vulnerabilities, problems with forensic analysis, and the development of forensic methodology/tools for such systems.

385. Alakbarov R.K. Cloudlet Selection Strategy According to the Types of Applications in Cloud Networks / **5th International Conference on Computing and Informatics (ICCI'2022),** Newcairo, **9-10 March 2022**, pp.200-203.

The selection of the most suitable cloudlet that allows running users applications rapidly in the cloud is still an urgent problem. For the elimination of resource shortages, power consumption, and delays in communication channels on mobile devices, the remote cloud servers are placed adjacent to devices. The delays on communication channels and power consumption on mobile devices are reduced through cloud-based mobile computing. In the paper we propose a strategy for selecting a cloudlet with high computing productivity, which provides a fast solution, considering the complexity degree of the application (file type). Also, in the paper, the solution of the task in a cloudlet close to the user, the downloading of the task to the cloudlet, the sending of the outcome to the user, and the minimization of network interruptions are presented.

386. Alakbarov R.K., Hashimov M.A. Fog Computing Application in Oil And Gas Industry and Analysis of Cybersecurity Problems / **Proceedings of the 8th**

International Conference on Control and Optimization with Industrial Application, Baku, **24-26 August 2022**, pp. 63-65.

The article discusses the application of fog computing technology in the oil and gas industry. Some of the features and advantages of fog computing technology over cloud technology are shown. Compared to cloud technology, fog is based on the computing power of distributed nodes in order to reduce the overall load of the data center. Since the nodes generating the data are distributed, centralized control over them becomes complicated. Currently, the Fog Platform is a cybercrime hotspot, primarily due to the lack of centralized management and poorly protected peripheral nodes Therefore, security issues in FC technology are more complicated. To this end, the article analyzes potential cybersecurity threats in the fog computing network and shows some countermeasures to protect against cyber attacks.

387. Fataliyev T.X., Mehdiyev Sh.A. Research of Cyber Resilience of Critical Infrastructures of Science Transformed Based on Industry 4.0 Applications / **Proceedings of the 8th International Conference on Control and Optimization with Industrial Application,** Baku, **24-26 August 2022**, pp. 162-164.

In modern times, the basic technologies of Industry 4.0 are widely used in various areas of the scientific community: in physical experiments, supercomputer calculations of theoretical

models, social research, genetic engineering, etc. In such a scientific environment, its science infrastructure has been formed based on the use of the Internet of Things (IoT), cyber-physical systems (CPS), artificial intelligence (AI), cloud solutions, big data analytics, and digital twins,smart cities, etc. The main purposeof this work is to study the problems and develop ways tosolve the cyber resilience of critical infrastructures of the scientific environment.

388. Alguliyev R.M., Sukhostat L.V. Anomaly Detection in Cyber-Physical Systems based on BiGRU-VAE / **16th IEEE International Conference on Application of Information and Communication Technologies (AICT 2022),** Washington, **12-14 October 2022**, pp. 1-5.

Various problems inevitably arise in cyber-physical systems, such as equipment failure, performance degradation, etc. Untimely detection of an abnormal state caused by a cyber-attack or a failure to operate devices in a cyber-physical system can lead to severe losses for the entire system. This paper proposes a method based on a deep bidirectional gated recurrent unit and variational autoencoder model to detect anomalies in a cyber-physical system. Experiments on a real dataset have shown the effectiveness of the proposed method in detecting anomalies in a cyber-physical system. Comparison with known methods showed the most accurate results according to the precision, recall, and F-measure metrics and amounted to 99.87%, 77.39%, and 87.20%, respectively.

389. Shikhaliyev R.H. Proactive Computer Network Monitoring based on Homogeneous LSTM Ensemble / **16th IEEE International Conference on Application of Information and Communication Technologies (AICT 2022),** Washington, **12-14 October 2022**, pp. 1-6.

Various problems inevitably arise in cyber-physical systems, such as equipment failure, performance degradation, etc. Untimely detection of an abnormal state caused by a cyber-attack or a failure to operate devices in a cyber-physical system can lead to severe losses for the entire system. This paper proposes a method based on a deep bidirectional gated recurrent unit and variational autoencoder model to detect anomalies in a cyber-physical system. Experiments on a real dataset have shown the effectiveness of the proposed method in detecting anomalies in a cyber-physical system. Comparison with known methods showed the most accurate results according to the precision, recall, and F-measure metrics and amounted to 99.87%, 77.39%, and 87.20%, respectively.

390. Dashdamirova K.G. Development of OLAP Based Decision Support System for Information Security Monitoring at National, Regional and Corporate Levels / **13th International Scientific and Practical Conference from Programming UkrPROGP'2022,** Kiyev, **11-12 October 2022**, pp. 354-363.

In the conditions where cyber threats are widespread and unavoidable, it is necessary to promptly detect cyber threats

and quickly react to possible incidents in order to ensure the information security of the national information environment. In the article, the need for continuous monitoring of computer networks to ensure information security is highlighted. The main components of the process of ensuring information security at the national, regional and corporate levels are studied. Sources of data for information security monitoring, methods of collecting data from various sources are investigated, categories of Information Security Monitoring Systems (ISMS) are studied. The carriers of social dangers are always people or social groups. The peculiarity of social threats is that they always threaten a large number of people, even if they are directed specifically against one person.

391. Hashimov M.A. Analysis of cyber security challenges in smart city environment / **18th International Conference on "Technical and Physical Problems of Electrical Engineering" (ICTPE-2022),** Istanbul, **30 October 2022,** pp. 83-86.

One of the new ways proposed to solve various urban problems during the last decade is the smart city concept. A smart city is presented as a concept that uses advanced technologies, applies innovations and offers a high quality of life. A smart city analyzes the situations happening in the city, offers technological solutions to improve the urban development and quality of life. The presented article provides information on the current state and further prospects of the smart city

concept. It highlights the benefits of the services covering the smart city environment for citizens and government institutions. The article also analyzes cyber security problems arising during the use of smart city services.

392. Mammadova M.H. Analysis of the Internet of Things capabilities inmonitoring the physiological state and location of personnel on an offshore oil. Tallinn: **Scientific Route,** Chapter 3**, 2023,** 32 p.

This chapter explores the opportunities of using the Internet of Things (IoT) to ensure the safety of personnel on offshore oil platform. To this end the IoT appli-cations and technologies are analyzed for the monitoring of the physiological state and location of personnel. The chapter presents the opportunities of using IoT with cloud technologies, Big Data technologies, and artificial intelligence for system de-velopment which enables to monitor and if necessary, to make appropriate decisions through systematic monitoring of the state of personnel based on expert assessment of deviation of real time parameters values from the norm. The practical tasks relat-ed to the application of IoT technology in various fields of healthcare are explored. IoT Services and IoT Applications used in e-health are analyzed and classified. The risks and challenges arising from the implementation of IoT solutions in healthcare and posing a threat to both the physical safety of patients and the confidentiality of their personal data are identified.

393. Набибекова Г.Ч. Обеспечение информационной безопасности распределенных электронных систем, содержащих OLAP, с помощью технологии блокчейн // **Информационные технологии, 2023,** № 5, том 29, с. 250-256.

В статье изложены свойства технологии блокчейн, в соответствии с которыми содержимое блоков блокчейна носит неизменный характер, а использование одноранговой сети P2P предполагает децентрализованное управление. Описана сущность и значение смарт-контрактов и полученных на их основании смарт-представлений, участвующих в процессе анализа данных и принятии решений. Рассмотрены работы, посвященные различным подходам к проблеме интеграции технологии блокчейн и хранилища данных. Для обеспечения всех трех ключевых аспектов информационной безопасности — целостности, доступности и конфиденциальности информации, что является важным как для государственных, так и для корпоративных структур, было предложено использовать не публичный блокчейн, а частный. Разработана модификация модели электронной системы поддержки принятия решений, содержащей блок OLAP, в которую включен частный блокчейн. Показано, что данную модель системы поддержки принятия решений (СППР) можно использовать в качестве электронной демографической

СППР, которая является инфраструктурой для решения государственных задач в этой сфере, поскольку многие характеристики данной модели соответствуют многоотраслевому характеру демографии.

394. Shikhaliyev R.H. Cybersecurity analysis of industrial control systems // **Problems of Information Society**, **2023,** vol. 14, no**.** 2, pp. 47-54.

The current frontiers in the description and simulation of advanced physical and biological Industrial control systems (ICS) used to control various critical industrial and social systems. ICS integrates modern computing, communication, and Internet technologies. The integration of these technologies makes ICS open to the outside world, which makes it vulnerable to various cyberattacks. ICS's cybersecurity is becoming one of the most important issues due to the significant damage caused by cyberattacks to organizations and society. This article analyzes the cybersecurity issues of ICS. In particular, an analysis of the main components and architectures of the ICS, security aspects of the ICS, vulnerabilities, and threats to the cybersecurity of the ICS, as well as measures and means to ensure the cybersecurity of the ICS, is carried out. The analysis will help to give some insight into the cybersecurity issues of ICS and identify various research objectives necessary to ensure the cybersecurity of ICS.

395. Alakbarova I.Y. Development of a model for the analysis of human behavior in a smart home environment // **Problems of Information Society, 2023,** vol. 14, no. 1, pp.75-84.

The article studies the approaches related to the analysis of human behavior in the smart home environment, the influence of cyber-physical systems on the behavior analysis, and the role in the formation and functionality of smart homes. It defines existing problems related to the security of smart homes, and proposes a new model for analyzing human behavior based on the sensed data. The model reveals the main features of each citizen's behavior and allows for a more in-depth study of the socio-political and economic processes taking place in the society.

396. Mahmudova R.Sh. Problems of evaluating the organization's information security culture // **Problems of Information Society, 2023,** vol. 14, no. 1, pp. 66-74.

Nowadays, digitization of all areas of human activity leads to an increase in the number of information security incidents in organizations. From this point of view, the problem of information security culture in organizations becomes very relevant in modern times. Obviously, the majority of incidents related to information security violations in organizations are associated to the human factor. To overcome this problem, the research in the field of the evaluation of information security culture is urgent. Measuring and evaluating information

security culture can enable an organization to identify its weaknesses in this area and take measures to eliminate them. This article examines various approaches to the concept of information security culture, and analyzes the affecting factors within the organization (management's attitude towards information security, information security policy, information security awareness and employee's behaviors). It also studies the documents adopted in the field of development and evaluation of information security culture in the European Union countries and the United States, and implemented projects. It analyzes proposed methods for measuring the information security culture in the organization using various methods. Moreover, the article reveals existing problems in this field and provides certain recommendations for their elimination. The methods of analysis and synthesis, comparison, generalization and systematic approach are used in this research.

397. Baghirov E.O. Malware detection based on opcode frequency // **Problems of Information Technology, 2023,** vol. 14, no. 1, pp. 3-7.

The amount of new malware has been continuously growing, and its threats are increasing rapidly. Developing new types of detection methods and thereby protecting computer systems from malicious programs has always been of interest to scientific researchers, individuals and organizations. In this work, several classification methods are applied on the dataset

which is prepared on the basis of opcodes obtained from known malicious and benign program samples. Dependency between opcodes higher than 70% of total are removed to achieve more relevant results. The other main factors affecting the results of the methods are evaluated. Results prove that Random Forest classifier can classify suspicious programs with higher accuracy than others.

398. Valikhanli O.V. Analysis of various techniques for ensuring autonomous navigation of unmanned aerial vehicles // **Problems of Information Technology, 2023,** vol. 14, no. 1, pp. 8-14.

Unmanned Aerial Vehicles (UAVs) have many advantages compared to other vehicle systems. UAVs are faster, cheaper, and more flexible. However, like many other systems UAVs also need navigation. But, it's not safe to use only one navigation system for various reasons. The recent increase in the number of cyberattacks is one of these reasons. Failure of the navigation system can cause the UAV to lose control. This, in turn, can lead to serious accidents. Therefore, this work analyzes various techniques to ensure the autonomous navigation of UAVs. Also, the advantages and disadvantages of each technique are discussed. Finally, the implementation of these techniques with Kalman filters (KF), deep learning, and machine learning is demonstrated and the results of various studies on this subject are also highlighted.

399. Alakbarov R.K. Security issues and solution mechanisms in cloud computing systems: a review // **Problems of Information Technology, 2023,** vol.14, no.2, pp. 12-22.

The recent rapid development of cloud technologies has encouraged its widespread use by individual mobile users, private organizations and public institutions. Mobile users and organizations deploy their data on cloud servers and use it. Connections to cloud servers are realized over the Internet, which makes data transmitted over the network vulnerable to various types of attacks. Although numerous security solutions have been proposed for data security in cloud computing systems, the security of provided services remains an actual problem for both cloud users and cloud service providers. The article provides a general survey of security and privacy issues in cloud computing systems, and reviews various types of attacks and possible threats, as well as protection methods and available solutions against such attacks, and proposes mechanisms.

400. Shikhaliyev R.H. Using machine learning methods for industrial control systems intrusion detection // **Problems of Information Technology, 2023,** vol.14, no.1, pp.37-48.

In recent decades, information technology has been integrated into industrial control systems (ICS). At the same time, there was a connection of the ICS to the Internet and a transition to

cloud computing. Consequently, new vulnerabilities and threats to sophisticated cyberattacks have emerged that create significant risks for the cybersecurity of ICS, and the old security model based on the isolation of ICS is no longer able to ensure their cybersecurity. This situation makes it very important to intellectualize the cybersecurity of ICS, for which machine learning (ML) methods are used. The use of ML methods will make it possible to detect cybersecurity problems of ICS at an early stage, as well as eliminate their consequences without real damage. This paper discusses the issues of ICS intrusion detection based on ML methods. The work can help in the choice of ML methods for solving anomaly detection problems of ICS.

401. Shikhaliyev R.H., Sukhostat L.V. Proactive computer network monitoring based on homogeneous deep neural ensemble // **Results in Control and Optimization, 2023**, vol. 11, pp. 1-11.

Computer networks are getting more complex these days. A computer network failure can result in the loss of important data, disruption of network services and applications, and economic loss and threaten national security. Therefore, it is crucial to detect failures on time and diagnose their root cause, which is possible with the help of proactive computer network monitoring Proactive computer network monitoring requires effective anomaly detection methods. The paper proposes a conceptual model of a system for proactive computer network

anomaly detection. To achieve high prediction accuracy, we propose to use a homogeneous ensemble, which consists of a base learning algorithm. An ensemble of deep neural networks based on base learning three-layered LSTM models was created using the bagging algorithm. We use the CICIDS2017 dataset to evaluate the proposed approach. Experimental results show that our method effectively improves the accuracy of anomaly prediction in computer networks.

402. Mahmudova Sh.J. Development of a method for processing log files using clustering // **Soft Computing, 2023,** no. 27, pp. 1617–1628 .

A log file is a document that keeps track of all events that occur on a website or server. Many log files are very large, so they can be regularly written over outdated content, or entire collections of log files with names, including a date, for example, can be created. In the event of technical problems, site inaccessibility, virus infection, hacker attacks and Distributed Denial of Service (DDoS) attacks, the resource administrator can use the information in log to find the cause, which makes it easier and faster to eliminate unwanted incidents. The paper analyzes the definition, types, location, use and examples of log files. Data are transferred to the MySQL database using the Squid.db database. Clustering is performed using a database. The study highlights clustering, analyzes metrics, and determines the proximity of clusters and objects in clusters in Euclidean space. Experiments are conducted and the results are

satisfactory. For example, data are transferred to the MySQL database using the Squid.db database. Since the Squid proxy server is a cache proxy server, it stores resources, and the work is done quickly on the next request. Data are clustered using a compiled table of databases transferred to MySQL via Squid proxy. In this case, unnecessary entries are deleted from the table, which significantly speeds up data processing. The application of clustering method in problem solving is fast and simple. For the problem stated, the degree of closeness of clusters and objects in clusters in Euclidean space is determined. Experiments are conducted using obtained results.

403. Alguliyev R.M., Aliguliyev R.M., Alakbarov R.K. Constrained k-means algorithm for resource allocation in mobile cloudlets // **Kybernetika**, **2023,** vol. 59, no. 1, pp.88-109.

The article proposes a clustering-based model for the optimal allocation of cloud resources among cloudlets. The proposed model takes into account user activity, usage frequency of cloud resources, the physical distance between users and cloud resources, as well as the storage capacity of cloudlets for optimal allocation of cloud resources in cloudlets. The proposed model was formalized as a constrained k-means method and an algorithm was developed to solve it. The MATLAB 2022a toolkit was used to evaluate the efficiency of the proposed algorithm. The obtained results revealed that the algorithm is promising.

404. Shikhaliyev R.H. Conceptual model of intelligent monitoring system for computer networks // **Problems of Information Technology, 2023,** vol. 14, no**.** 1, pp. 23-28.

The size and complexity of computer networks (CNs) are constantly increasing, which requires the intellectualization of network monitoring. Undoubtedly, intellectualization will increase the effectiveness of monitoring the CNs. To ensure the intellectualization of the CNs monitoring, it is necessary to use machine learning (ML) methods. The use of ML methods enables to create an intelligent monitoring system. This article proposes a conceptual model of a system for CNs intelligent monitoring. The model is based on the analysis of log files using ML methods. The proposed model will make it possible to monitor the CNs in a targeted manner, which can increase the efficiency of network monitoring and management in terms of the use of network resources.

405. Bayramova T.A. Software defect prediction using the machine learning methods // **Problems of Information Technology, 2023,** vol. 14, no**.** 2, pp. 23-31.

Reliability of software systems is one of the main indicators of quality. Defects occurring when developing software systems have a direct effect on reliability. Precise prediction of defects in software systems helps software engineers to ensure the reliability of software systems and to properly allocate resources for the trial process. The development of an ensemble method by combining several classification methods occupies

one of the main places in research conducted in the field of error prediction in software modules. This paper proposes a method based on the application of ensemble training for defect detection. Here, a database obtained from PROMISE and GITHUB software engineering registry is used to detect defects. Experiments are conducted using Weka software. The prediction efficiency is evaluated based on F-measure and ROCarea. As a result of experiments, the defect detection accuracy of the proposed method is proven to be higher than that of individual machine learning methods.

406. Abdullayeva F.D. Cyber resilience and cyber security issues of intelligent cloud computing systems // **Results in Control and Optimization, 2023,** vol. 12, pp. 1-16.

It is necessary to provide the cyber security of cloud computing according to the components that constitute its structure. The first step in advancing the cyber security of this technology is to accurately identify its threats. In this paper, a new cyber security reference model of the cloud system, which consists of components making up separate layers of cloud computing is proposed. Available reference models of cloud computing security do not describe the virtualization and service layers and the important components for providing the cyber security of cloud computing in detail, do not consider the social media IoT sensor layer, which collects the text data typed by attackers to carry out cyber attacks on the cloud infrastructure, and the cyber resilience issues of the cloud computing at all In

addition, this paper studies the cyber security issues of cloud computing service models, and constructs an attack model to provide security of cloud systems. It gives an interpretation of standards and legislative acts on the cyber security of cloud computing. According to security aspects, clarification of the cyber security and cyber resilience concepts of cloud systems is provided. The cyber resilience architecture of intelligent cloud systems is developed. The advantage of developed cyber resilience model over available one is that, it determines the information security and cyber security aspects of cloud computing and combines them to form the cyber resilience aspects of cloud systems.

407. Alguliyev R.M., Imamverdiyev Y.N., Sukhostat L.V. Automatic facies detection based on oilfield core images // **Petroleum Science and Technology, 2023**, vol. 41, issue 17, pp. 1641-1664.

This paper proposes a machine learning method for automatically detecting and identifying facies from digital images of the oil well core. The method is based on artificial neural networks, specifically, pre-trained deep convolutional neural networks, improved using histogram of oriented gradients and local binary pattern methods. AlexNet, Inception, MobileNet, Xception, and DenseNet extract features from images. An algorithm based on the behavior of fireflies selects the most informative features. The k-nearest neighbors, support vector machines, and random forest methods are

considered as classifiers. The proposed approach uses a model that has been trained and tested on a core rock samples dataset of > 23,000 images related to four facies as coal, sandstone, siltstone, and shale. The experimental results show that the proposed HOG + LBP + DenseNet model combined with a random forest is better than support vector machines and k-nearest neighbors methods regarding facies recognition from core photographs and the precision (95.5%), recall (96.46%), and F-measure (95.98%) metrics. © 2022 Taylor & Francis Group, LLC.

408. Alakbarov R.K. Model of optimal placement of cloudlets in a wireless metropolitan area network // **Информационные технологии**, **2023,** no. 4, vol. 29, pp. 182–188.

Cloud computing has recently emerged as a new paradigm for processing and storing large amounts of data. The rapid increase in the number of mobile phones and IoT devices benefiting from cloud computing services reduces the Internet bandwidth, resulting in delays in delivering data processed on remote cloud servers to the user. Mobile devices use edge computing systems (cloudlet, fog computing, etc.) to overcome resource shortages, power consumption and delays in communication channels. Edge computing systems place processing devices (cloudlets) close to users. The closer the cloudlets to mobile devices, the lower the processing time and energy consumption of the mobile device, and the higher the

bandwidth of communication channels. Thus, cloudlet-based mobile computing clouds are widely used to reduce the latency in the Internet communication channels and energy consumption on mobile devices. This article identifies the most popular places for cloud servers in metropolitan mobile networks and discusses the optimal placement of a limited number of cloudlets in those places.

409. Alguliyev R.M., Alakbarov R.K. Integer programming models for task scheduling and resource allocation in mobile cloud computing // **I.J. Computer Network and Information Security, 2023,** vol. 15, no. 5, pp. 13-26.

In traditional mobile cloud computing, user tasks are uploaded and processed on a cloud server over the Internet. Due to the recent rapid increase in the number of mobile users connected to the network, due to overload of the Internet communication channels, there are significant delays in the delivery of data processed on cloud servers to the user. Furthermore, it complicates the optimal scheduling of the tasks of many users on cloud servers and the delivery of results. Scheduling is an approach used to reduce the tasks execution time by ensuring a balanced distribution of user tasks on cloud servers. The goal of scheduling is to ensure selection of appropriate resources to handle tasks quickly, taking into account user requirements. Whereas the goal of cloud service providers is to provide users with the required resources through performing effective scheduling so that both the user and the service provider can

benefit. The article proposes a scheduling model to reduce processing time, network latency, and power consumption of mobile devices through optimal task placement in the cloudlet network in a mobile cloud computing environment.

410. Mahmudova Sh.J. Development of an Algorithm Using the Vikor Method to Increase Software Reliability // **Springer Series in Reliability Engineering, in: Vijay Kumar & Hoang Pham (ed.), Predictive Analytics in System Reliability, 2023,** pp. 229-246.

Software efficiency indicators play a key role in its optimization. Various ways are available to ensure software optimization. One of the key indicators of software is its reliability. Software reliability refers to the program features to perform certain functions and they are kept within certain limits under specified conditions. Software reliability is determined by its non-denial and recoverability. Software reliability is considered an important quality factor. The article uses the VIKOR (VIsekriterijumska optimizacija i KOmpromisno Resenje) method for the development of an algorithm to increase software reliability. The VIKOR method is used for different areas. Some sources provide information on the application of the VIKOR method. It refers to a multi-criteria decision method or multi-criteria decision analysis method. The alternatives here are ranked and the one closest to the ideal so-called compromise is determined. As a result of the author"s research, six important criteria for software reliability

are identified and alternatives are used. The fuzzy VIKOR method is used for multi-criteria evaluation of software. The work done is considered to be novel, and the advantage is that the selected criteria have not yet been used for this type of task, this positively changes its efficiency. The experiments perform positive results.

411. Aliyev A.G. Conceptual approach to problems of security and cyber resilience issues of information infrastructure of regional and national economies // **Информационное общество, 2023**, no. 1, pp. 88-100.
The article is devoted to the conceptual study of the security and cyber resilience of the information infrastructure of regional-national economic systems, which is currently considered relevant. The directions of ensuring information security are interpreted and the problems of its sustainable development and resilience are studied. Internal threats for ensuring national and economic security are identified. The methods of ensuring information security are studied. Various purposeful elements and actors of the digital environment are identified. Relevant recommendations are made for reliable provision and improvement of information infrastructure security and cyber resilience of regional-national economies on the 4.0 Industrial platform and in the conditions of the digital economy.

412. Mahmudova R.Sh. Cyber-physical Systems: Security Problems and Issues of Personnel Information Security

Culture // **Education and Management Engineering, 2023,** vol. 13, no. 2, pp. 18-26.

Cyber-physical systems CFS have already become an integral part of our lives. Starting from the energy sector, production and transport, to healthcare, trade, and financial spheres, these systems have been widely applied everywhere. The realization of threats to the information security of such systems can cause very serious disasters, human casualties, financial loss, as well as damage the image of the companies that use these systems. From this point of view, it is very important to investigate the issues of ensuring information security of KFS. Security problems of cyber-physical systems are analyzed. At the same time, the role and importance of the human factor in ensuring the information security of cyber-physical systems are explained. The difficulties faced by enterprises in informing employees about information security and forming a culture of information security in them are analyzed. Appropriate training methods are explained and recommendations are given to develop employees necessary knowledge and skills related to information security.

413. Alakbarov R.K., Hashimov M.A. Application problems of cloud-based SCADA systems in the oil and gas industry // **SOCAR Proceedings, 2023**, no. 4, pp. 149-155.

SCADA (Supervisory Control and Data Acquisition) systems play an important role in the oil and gas industry providing real-time monitoring, control and data acquisition of critical

infrastructure. Unlike traditional SCADA systems based on local hardware and software, cloud-based SCADA systems take advantage of cloud computing technologies for real-time data collection and management. Cloud-based SCADA systems offer many advantages due to their scalability, flexibility and cost-effectiveness. To take advantage of these advantages, it is required to solve a number of problems related to the application of cloud-based SCADA systems in the oil and gas industry. One of the most important application challenges is the cybersecurity issues arising in cloud-based SCADA systems, which are a significant concern due to the critical nature of the infrastructure they control. Thus, the systems face various vulnerabilities and threats that can destroy the data integrity and the systems availability. This article outlines the current cyber-attacks that can compromise the security of cloud-based SCADA systems. Threats and vulnerabilities in using cloud-based SCADA systems are analyzed, and suggestions are made that partially help to solve them. Some security mechanisms are recommended to ensure the security of cloud-based SCADA systems. These mechanisms will help increase the reliability and security of cloud-based SCADA system operations in the oil and gas industry.

414. Rzayeva N.A. Süni intellektlə bağlı təhdidlərin təhlili / **Ümummilli Lider Heydər Əliyevin anadan olmasının 100 illiyinə həsr olunmuş "Süni intellekt və onun**

tətbiq sahələri" Respublika elmi konfransı, Sumqayıt, **07-08 dekbar 2023**, s. 74-76.

Süni intellekt mürəkkəb, çoxşaxəli və sənayelərarası sahədir. Süni intellekt, şübhəsiz ki, insan fəaliyyətinin bütün sahələrinə nüfuz etmiş və dövrümüzün əsas texnoloji nailiyyətlərindən birinə çevrilmişdir. Süni intellekt maşın öyrənməsi, neyron şəbəkələri, təbii dillərin işlənməsi və robototexnika kimi əsas prinsiplərə əsaslanır. Süni intellekt sahəsində əsas problem kibertəhlükəsizlik və necə işlədiyini təhlil etməkdir. Bu məqalədə biz süni intellektdən təkcə düşünmə, planlaşdırma, öyrənmə və məlumatların emalı texnologiyası kimi deyil, həm də obyektləri manipulyasiya etmək bacarığından danışacağıq.

415. Şıxəliyev R.H., Abdullayeva F.C. Kibertəhlükəsizlik problemlərinin həllində NLP effektiv vasitə kimi / **Ümummilli lider Heydər Əliyevin 100 illik yubileyinə və Beynəlxalq Ana dili gününə həsr olunmuş "Azərbaycan dilinin İKT problemləri, İKT-nin Azərbaycan dili problemləri" respublika elmi-praktiki konfransı,** Bakı, **21-22 fevral 2023**, s. 50-54.

Məqalədə NLP-nin kibertəhlükəsizlikdə tətbiq sahələri araşdırılıb, əsas tədqiqat istiqamətləri müəyyən edilib. Sosial media mənbələrində hücumçular tərəfindən yazılmış mətn tipli kibertəhdid xarakterli informasiyasının klassifikasiyası üçün NLP-yə əsaslanan yanaşma təklif edilib. Təklif olunan metod əvvəlcə kontentdə kibertəhdidlərlə bağlı sentimental izləri analiz edir, sonra isə proqnozlaşdırır. Yanaşma təşkilatların

təhdidlərin prioritetləşdirilməsi, təhdidlərin avtomatik modelləşdirilməsi kimi proaktiv qərarlar qəbul etməsinə imkan yarada bilər.

416. Bayramova T.A. Proqram sistemlərinin təhlükəsizlk problemləri haqqında / **Dövlət Təhlükəsizliyi Xidmətinin Heydər Əliyev adına Akademiyası Ulu Öndər irsinin daşıyıcısıdır. Respublika elmi-praktiki konfransı,** Bakı, **01-02 dekabr 2023**, s. 743-748.

Məqalədə kibercinayətkarların hədəfləri və kiberhücumların növləri təhlil edilmiş və son illərdə ən çox ziyan vuran kibercinayətkar qruplar haqda məlumat verilmişdir. Proqram təminatının boşluqları klassifikasiya etmək və qiymətləndirmək üçün müxtəlif təşkilatlar tərəfindən yaradılmış sistemlər göstərilmişdir. Proqram təminatında olan xətaların və boşluqların aradan qaldırılması üçün proqram kodunu analiz metodları haqda məlumat verilmidir.

417. Ocaqverdiyeva S.S. Uşaqların informasiya təhlükəsizliyinin təmin edilməsində Təhlükəsiz İnternet Mərkəzlərinin rolu / **Dövlət Təhlükəsizliyi Xidmətinin Heydər Əliyev adına Akademiyası Ulu Öndər irsinin daşıyıcısıdır. Respublika elmi-praktiki konfransı,** Bakı, **01-02 dekabr 2023**, s. 767-772.

Kiberməkanda uşaqların informasiya təhlükəsizliyinin təmin olunması məsələsi müasir dövrün aktual məsələlərindəndir. İnternet bu gün uşaq və yeniyetmələrin həyatının ayrılmaz hissəsinə çevrilmişdir, onlar mobil texnologiyaların və digər

rəqəmsal qurğuların aktiv istifadəçisidir. Onlar çox vaxt kiberzorakılığa, kibertəqibə və digər təhlükələrə məruz qalır və ya fərdi məlumatlarını paylaşmaqla özlərini kibercinayətkarların qurbanına çevirirlər. İnternetdən gələn təhdidlərdən, zərərli məlumatlardan uşaqların mühafizəsi üçün həm milli, həm də beynəlxalq səviyyədə müxtəlif siyasətlər və strategiyalar işlənir.Məqalədə uşaqların virtual məkanda qarşılaşdığı risklər şərh edilmiş, onların təhlükələrdən qorunmasında rəqəmsal savadlılığın rolu təhlil edilmiş və təhlükəsiz internetlə əlaqəli müyyən təcrübələr araşdırılmışdır. Kiberməkanda uşaqları mövcud təhlükələrdən qorumaq üçün Təhlükəsiz İnternet Mərkəzlərinin əhəmiyyəti qeyd edilmişdir.

418. Əliyev Ə.Q. İqtisadi proseslərdə hesabatlılığın və şəffaflığın təminində kiberdayanıqlılıq məsələləri / "**Dayanıqlı inkişaf. Hesabatlılıq. Şəffaflıq" beynəlxalq elmi-praktik konfrans,** Bakı, **15-16 sentyabr 2023**, s. 216-223.

Məqalə iqtisadi proseslərdə hesabatlılığın və şəffaflığın təminində kiberdayanıqlılıq məsələlərinə həsr olunmuşdur. İqtisadi idarəetmədə hesabatlılığın və şəffaflığın səviyyəsini yüksəltmək üçün milli iqtisadiyyatın kiberdayanıqlılığının artırılması ilə bağlı problemlər tədqiq olunmuşdur. İqtisadiyyatın inkişafında şəffaqlıq və hesabatlılığın funksional vəzifələri və təsirləri şərh olunmuşdur. İqtisadi inkişaf kontekstində şəffaflıq və hesabatlılığın bəzi əsas funksiyaları və prinsipləri sxematik olaraq verilmişdir. İqtisadi və informasiya

sistemlərinin dayanıqlılığının təmin edilməsi mexanizmləri işlənilmişdir. Hesabatlılığın və şəffaflığın təmininda kiberdayanıqlılıq məsələləri araşdırılmışdır. Kiber davamlılıq və dayanıqlılığın həm milli, həm də regional iqtisadiyyatda əhəmiyyəti qeyd olunmuşdur. Hesabatlılığa və şəffaflığa təsir edən məlumatın təhlükəsizliyi və məxfiliyi, kiber fırıldaqçılıq və maliyyə cinayətləri, təchizat zəncirinin təhlükəsizliyi, hadisələrə reaksiya və biznesin dayanıqlılığı, reqlamentlərə uyğunluq və hesabatlılıq, maraqlı tərəflərlə kommunikasiya və təhsil sisteminin qurulması, kiber sığorta kimi kiberdayanıqlılıq problemləri analiz olunmuşdur. Sənaye 4.0 platformasında iqtisadi proseslərdə hesabatlılığın və şəffaflığın təmininda kiberdayanıqlılıq məsələlərinin işlənilməsi üzrə müvafiq tövsiyələr verilmişdir.

419. Vəlixanlı O.V. Pilotsuz uçuş aparatının yerüstü idarəetmə stansiyasında olan zərərli proqramların aşkarlanması üçün dərin təlim üsulunun işlənməsi / **Ümumilli Lider Heydər Əliyevin 100 illik yubileyinə həsr olunmuş "Azərbaycan təhlükəsizlik orqanlarının fəxri rəhbəri" Respublika elmi-praktiki konfransı**, Bakı, **5 may 2023**, s. 481-484.

Məqalədə pilotsuz uçuş aparatlarının (PUA) yerüstü idarəetmə stansiyalarında (YİS) olan zərərli proqramların aşkarlanması üçün hibrid model təklif olunmuşdur. Təklif olunmuş hibrid model əsas iki hissədən ibarətdir. Birinci hissə şəkillərdən əlamətlərin çıxarılması funksiyasını daşıyır. İkinci

hissə isə çıxarılmış bu xüsusiyyətlərin əsasında zərərli proqramların təsnif olunmasını təmin edir. Aparılmış tədqiqatların nəticəsi olaraq təklif olunmuş hibrid model 10 müxtəlif zərərli proqram növünü yüksək dəqiqliklə aşkar etməyə nail olmuşdur.

420. Ağayev F.T., Ələsgərova E.R., Bahadurzadə N.İ. Bulud texnologiyası əsasında elektron təhsil sisteminin təhlükəsizlik problemləri / **Dövlət Təhlükəsizliyi Xidmətinin Heydər Əliyev adına Akademiyası Ulu Öndər irsinin daşıyıcısıdır. Respublika elmi-praktiki konfransı,** Bakı, **01-02 dekabr 2023**, s. 664-670.

Onlayn təhsil sistemlərinin istifadəsi həm tədrisi, həm də öyrənməni təkmilləşdirdi. Tədqiqatçılar, tələbələr arasında elektron təhsilin qəbulu və ona təsir edən bir sıra amilləri araşdırsalar da, qəbul edilən təhlükəsizliyin rolu hələ araşdırılmayıb. e- Learning-də kibertəhlükəsizlik məsələsi daha az araşdırıldığından, bu məqalə bulud əsaslı e-Learning sistemləri ilə bağlı kibertəhlükəsizlik məsələlərinin idarə edilməsinə yönələcək yanaşmaları göstərmək məqsədi daşıyır. Təklif olunan metodologiya məlumatların mövcudluğunu və təcavüzkarlardan qorumaq üçün həll yollarını təmin edir. Bu tədqiqat bulud əsaslı e-Təhsillə bağlı təhlükəsizlik tədbirləri şəklində həll təklif etmək üçün bulud xidmətinin çatdırılması modelində müxtəlif təhlükəsizlik problemlərini müəyyən edir. Müxtəlif tədqiqatçılar tərəfindən təklif olunan elektron təhsilin xidmət göstərilməsi modellərində müxtəlif hücum növləri

müzakirə olunur. Elektron öyrənmə modellərinin bu araşdırması istifadəçiləri internet vasitəsilə buluddakı məlumatlarına təhlükəsiz şəkildə daxil olmağa təşviq edir.

421. Əhmədov E.Y. Elektron ticarətdə fırıldaqçılığın aşkarlanması üçün İsolation Forest, Local Outlier Factor və One Class SVM təlimsiz öyrənmə alqoritmlərinin müqayisəli analizi / **Dövlət Təhlükəsizliyi Xidmətinin Heydər Əliyev adına Akademiyası Ulu Öndər irsinin daşıyıcısıdır. Respublika elmi-praktiki konfransı,** Bakı, **01-02 dekabr 2023**, s. 698-700.

Məqalədə maşın təliminin nəzarət olunmayan alqoritmlərinin Phyton mühitində tətbiqi ilə e-ticarətdə fırıldaqçılığın aşkarlanması məsələsinə baxılır. İsolation forest, local Outlier factor və One Class SVM alqoritmlərinin üstünlükləri tədqiq edilmiş və eksperimentlər həyata keçirilmişdir. Eksperimentin nəticələrinin müqayisəli analizi üçün müxtəlif göstəricilər üzrə qiymətləndirilməsi aparılmışdır.

422. Набиев Б.Р., Дашдамирова К.Г. Интеллектуальный анализ киберугроз: проблемы и перспективы / **XVII Международная научно-техническая конференция "Оптико-электронные приборы и устройства в системах распознавания образов и обработки изображений" (Распознавание–2023),** Курск, **12-15 сентября 2023**, с. 166-168.

В области обработки изображений все более распространенным становится использование

беспроводных вычислительных кластеров. Использование беспроводного вычислительного кластера в обработке изображений дает несколько преимуществ, таких как повышенная скорость и повышенная точность.

423. Саидова М.Т., Гасанова Р.Ш., Аскеров Ф.Ш. Анализ методов идентификации фейковых журналов / **XVII Международная научно-техническая конференция "Оптико-электронные приборы и устройства в системах распознавания образов и обработки изображений" (Распознавание – 2023),** Курск, **12-15 сентября 2023**, с. 204-206.

Перечислены ключевые моменты, на которые исследователь должен обратить внимание при выборе журнала для публикации своего научного результата. Представлены обобщенные критерии для выявления фейковых журналов в академическом сообществе.

424. Дашдамирова К.Г. Анализ принятых международных и национальных стандартов в области мониторинга информационной безопасности / **XXII Международная научно-техническая конференция «Развитие информатизации и государственной системы научно-технической информации» РИНТИ-2023**, Минск, **16 ноября 2023**, с. 112-116.

Исследован международный опыт в области мониторинга информационной безопасности, проанализированы

международные и национальные стандарты, принятые во всем мире и Азербайджане.

425. Абдуллаева С.Р. Сравнительный анализ подходов к мониторингу и оценке интернет-медиа / **XXII Международная научно-техническая конференция «Развитие информатизации и государственной системы научно-технической информации» РИНТИ-2023**, Минск, **16 ноября 2023**, с. 98-102.

Проанализированы возможности средств и автоматизированных систем мониторинга, используемых для оценки онлайн-медиаресурсов. Исследованы конструктивные подходы к мониторингу ресурсов интернет-медиа. Рассмотрены существующие методы и средства мониторинга медиа, а также концептуальные модели системного анализа информации на интернет-ресурсах.

426. Алгулиев Р.М., Сухостат Л.В., Алыгулиев Р.М. Оценка критичности киберфизических систем на основе графа атак / **XVII Международная научно-техническая конференция "Оптико-электронные приборы и устройства в системах распознавания образов и обработки изображений" (Распознавание–2023),** Курск, **12-15 сентября 2023**, с. 52-54.

В работе предлагается метод определения критических устройств киберфизических систем с применением байесовского графа атак.

427. Baghirov E.O. Analyzing the performance of behavioral-based malware detection approaches under real-world conditions / **XVII Международная научно-техническая конференция "Оптико-электронные приборы и устройства в системах распознавания образов и обработки изображений" (Распознавание–2023),** Курск, **12-15 сентября 2023**, pp. 15-17.

As cyber-attackers have improved the complexity of malware and anti-detection methods, the effectiveness of traditional malware detection techniques has decreased. Behavioral-based malware detection is a promising approach for detecting new and unknown malware threats that lack a signature. This research aims to analyze the performance of behavioral-based malware detection approaches under realworld conditions. The results of the study provide insights into the strengths and limitations of behavioral-based malware detection approaches and identify areas for improvement.

428. Shikhaliyev R.H. Computer networks security monitoring model based on Deep Learning / **XVII Международная научно-техническая конференция "Оптико-электронные приборы и устройства в системах распознавания образов и обработки**

изображений" (Распознавание–2023), Курск, **12-15 сентября 2023**, pp. 34-36.

This article presents a computer network security monitoring model based on a deep learning model. Convolutional Neural Networks and Long Short-Term Memory models are used, which allow classifying network security data and detecting CN anomalies.

429. Valikhanli O.V. Detection of dos attacks in unmanned aerial vehicle networks / **XVII Международная научно-техническая конференция "Оптико-электронные приборы и устройства в системах распознавания образов и обработки изображений" (Распознавание–2023),** Курск, **12-15 сентября 2023**, pp. 39-41.

In this paper, a hybrid model is proposed to detect cyberattacks in unmanned aerial vehicle networks. The proposed model achieved 99.07% of accuracy.

430. Mahmudova Sh.J. The role of biometric networks in recognition of person / **XVII Международная научно-техническая конференция "Оптико-электронные приборы и устройства в системах распознавания образов и обработки изображений" (Распознавание–2023),** Курск, **12-15 сентября 2023**, pp.22-23.

In this article, propose about biometric network, the essence of the problem and identification. The advantages of biometric

technology are shown to address the issues facing the authorities of law enforcement system.

431. Alizada D.I. Possibilities of using hybrid cloud in intelligent electronic libraries / **XVII Международная научно-техническая конференция "Оптико-электронные приборы и устройства в системах распознавания образов и обработки изображений" (Распознавание–2023),** Курск, **12-15 сентября 2023**, pp. 13-15.

One of the important advantages of cloud computing is the ability to store and share knowledge through electronic libraries. The proposed library model provides for the use of hybrid clouds.

432. Mammadova M.H., Ahmadova A.A. General architecture of digital twins in medical field / **XVII Международная научно-техническая конференция "Оптико-электронные приборы и устройства в системах распознавания образов и обработки изображений" (Распознавание–2023),** Курск, **12-15 сентября 2023**, pp. 24-25.

The article examines the technology of digital twins and their possibilities. It shows the application and effects of DT in the field of health care. The article proposes a generalized architecture of health digital twins formed by physical and virtual objects with uninterrupted data sharing between them.

433. Alguliyev R.M., Abdullayeva F.D., Ojagverdiyeva S.S. Child Access Control Based on Age and Personality Traits / **The 6th International Conference on Computer Science, Engineering and Education Applications, ICCSEEA2023**, Warsaw, **19 August 2023**, pp. 289-298.

Exposure to harmful information on the Internet and constant use of digital devices (computer, phone, tablet, etc.) harm children's psychology and health. The use of methods that control access to the Internet and filter web content considered harmful to children is an effective means of solving this problem. The article proposes a method to control access to the Internet, taking into account several personality traits of the user-child (age, eye diseases, heart diseases, neurological and psychological conditions, etc.) using Mamdani-based fuzzy logic inference system. The values of the input parameters of this system are described by five linguistic parameters, which are "very low", "low", "medium", "high" and "very high" and with a triangular membership function. This approach is focused on the individual user and the main advantage is that parameters are used in vector form. This research is significant for the use of parents, guardians and those responsible for children.

434. Alakbarov R.K., Hashimov M.A. Development of security mechanisms in cloud-based SCADA systems / **5th International Conference on Problems of**

Cybernetics and Informatics, Baku, **28-30 August 2023**, pp. 1-4.

Moving SCADA (Supervisory Control and Data Acquisition) applications used to monitor critical infrastructure to the cloud can reduce costs, rise scalability and make it more beneficial for organizations (users) in terms of technical support. While cost reduction and efficiency gains are key to business, security is one of the most important issues. The article analyzes the threats and vulnerabilities that can interfere with the security of cloud SCADA systems. Several cybersecurity mechanisms have been developed to secure cloud SCADA systems.

435. Baghirov E.O. Evaluating the performance of different machine learning algorithms for Android malware detection / **5th International Conference on Problems of Cybernetics and Informatics,** Baku, **28-30 August 2023,** pp. 1-4.

With the increasing prevalence of Android malware, it has become essential to develop effective malware detection techniques. This study aims to evaluate the performance of various machine learning algorithms for Android malware detection. Several machine learning algorithms were evaluated using a dataset of Android applications, including both benign and malicious apps. The performance of each algorithm was measured in terms of accuracy, precision, recall, and F1-score. The results showed that the LightGBM algorithm had the highest accuracy, precision, and F1-score. These findings can

help to inform the development of effective Android malware detection systems.

436. Hashimov M.A. Cyber security issues of critical infrastructures in a smart city environment / **The 19th International Conference on Technical and Physical Problems of Engineering,** Istanbul, **31 October 2023,** pp.85-88.

The idea of smart city has emerged as a means to solve urban problems and expand the quality of life of citizens. Smart city services use advanced technologies to efficiently manage resources, improve public services and support sustainable development. However, the integration of information and communication technologies (ICT) into critical infrastructures, such as transportation, energy, and water systems, poses significant cybersecurity challenges. In this regard, this article analyzes the cyber security problems occurred during the use of critical infrastructures in this sphere. Some suggestions are made to slightly solve the mentioned problems.

437. Alakbarov R.K., Alakbarov O.R. Mobil Cloud Computing: Problems and Solution Way / **The 19th International Conference on Technical and Physical Problems of Engineering,** Istanbul, **31 October 2023,** pp.89-92.

The article analyzes the problems arising in the use of cloud-based mobile cloud computing and their solutions. Besides, this article studies the problems related to different parts of mobile

cloud computing. It identifies the criteria hindering the effective use of cloudlet-based mobile cloud computing (MCC) services in wireless urban networks. A strategy for solving these problems is developed. To implement the proposed strategy, it is recommended to use cloudlets with a hierarchical structure in mobile cloud computing systems.

438. Alakbarova I.Y. Assessment of Society Based on the Analysis of the Behavior of Citizens on the Platform of Electronic Demography / **5th International Conference on Problems of Cybernetics and Informatics**, Baku, **28-30 August 2023**, pp. 1-3.

Due to the fact that documents collected in various registries (medical certificates, court documents, fines, tax payments, etc.) as well as demographic indicators create big data, it is impossible today to determine human behavior by conventional statistical or empirical methods. The proposed approach to assessing the behavior of citizens on the e-demography platform consists of five steps: a collection of documents, data pre-processing, description of the data, clustering of documents, and assessment of the behavior of citizens by conducting sentiment analysis. Such an approach can be critical in studying society, identifying social and economic problems, and ensuring transparency of relations between citizens and authorities in the e-government environment.

439. Alguliyev R.M., Nabiyev B.R., Dashdamirova K.G. CTI challenges and perspectives as a comprehensive

approach to cyber resilience / **The 5th International Conference on Problems of Cybernetics and Informatics,** Baku, **28-30 August 2023**, pp. 1-5.

The significant growth in the number, variety, and sophistication of cyber threats in recent years makes traditional approaches ineffective against new generation cyber threats. More effective mechanisms against cyber threats and attacks require intelligent analysis of the threats themselves. Cyber Threat Intelligence (CTI) is a new approach based on artificial intelligence technologies aimed at collecting, analyzing and resolving current and potential attacks that threaten the security of an organization or its assets. This thesis explores CTI technologies and considers problems and advantages in this area.

440. Aliguliyev R.M. Performance Evaluation of Algorithms for Anomaly Detection Using Apache Spark / **The 5th International Conference on Problems of Cybernetics and Informatics,** Baku, **28-30 August 2023,** pp. 1-3.

Detecting outliers gain increasing attention as they have various application fields like fraud detection, medical analysis, intrusion detection and so on. There have been established different techniques and methods such as distance-based, density-based, statistical-based, ensemble-based, learning-based methods and this process is still ongoing to find out the more effective algorithms as some of them give the desired result on a certain data set but not effective for the different data set and

vise versa. This paper compares the experimental result of the most popular methods on the publicly available datasets using Apache Spark and helps the researchers to shape the future of investigation in regarding to the calculation of outliers.

441. Mahmudova Sh.J. Development of a method for increasing the reliability of distributed software systems on cloud systems platform / **VIII İnternational Scientific Conference "Development of science in the XXI century"**, Dortmund, **14-15 September 2023,** pp. 96-102.

Cloud computing allows users to store and manage data efficiently. This research aims to develop a method for creating of distributed software systems on the platform of cloud systems and improving their reliability. The use of cloud computing in the construction of the software system can reduce expenses, minimize the cost of data storage, etc. The modern development of the world economy is accompanied by the wide application of information systems, among which cloud technologies have a special place. For this, cloud computing, their features and services are investigated, related works and the most common cloud computing models and cloud databases are studied. Digital twin technologies, their types, etc. are studied to increase the software system performance in cloud computing, forecasting, onitoring, and to reduce production time. Reliability criteria for software systems in cloud computing are selected. The calculations

based on the obtained scientific results perform promising results.

442. Mammadova M.H., Jabrayilova Z.G. Decision Making in an Intelligent Health Management System of the Ship Crew in Maritime Transport / **2nd International Conference on Problems of Logistics, Management and Operation in the East-West Transport Corridor (PLMO 2023),** Baku, **24-26 May 2023**, pp. 24-26.

This paper proposes a methodological approach for the decision making in a distributed intelligent health management system for ship crew in maritime transport. The decision-making methodology is based on the concept of a person-centered approach to managing the health and safety of ship personnel, which implies the inclusion of employees as the main component in the control loop. Develops a functional model of the health management system for workers employed on ship and implements it through three phased operations that is monitoring and assessing the health indicators of each employee and making decisions. These interacting operations combine the levels of a distributed intelligent health management system. It presents appropriate approaches to the implementation of decision support processes and describes one of the possible methods for evaluating the generated data and making decisions using fuzzy pattern recognition. The models of a fuzzy ideal image and fuzzy real images of the health status of an employee are developed and an algorithm is described for

assessing the deviation of generated medical parameters from the norm. The paper also compiles the rules to form the knowledge bases of a distributed intelligent system for remote continuous monitoring. It is assumed that embedding this base into the intelligent system architecture will objectively assess the trends in the health status of the members of ship crew and make informed decisions to eliminate certain problems.

443. Baghirov E.O. Leveraging Machine Learning for Accurate Malware Traffic Detection / **International Conference on Intelligent Systems and New Applications (ICISNA'23),** Liverpul, **28-30 April 2023**, pp. 25-26.

This paper proposes a novel approach to accurately detect malware traffic using machine learning techniques. The increasing prevalence of malware and its sophisticated nature has made it difficult to identify and prevent attacks. In this work, we applied various machine learning algorithms to detect malware traffic by analyzing network traffic patterns. Our proposed method outperforms existing solutions and achieves high accuracy in detecting both known and unknown malware samples. The results demonstrate the effectiveness of machine learning in improving the accuracy of malware detection, and highlight the potential of this approach in enhancing cybersecurity measures.

444. Baghirov E.O. Machıne Learnıng-based Androıd Malware Detectıon: A Robust and Accurate Approach /

Dedicated to the 100th Anniversary of National Leader of Azerbaijan, Haydar Aliyev VII International Scientific Conference of Young Researchers, Bakı, **28-29 April 2023,** pp. 1128-1131.

The proliferation of smartphones and the widespread adoption of the Android operating system have made mobile devices the new frontier for cybercrime. Malware authors are increasingly targeting Android devices due to their popularity and vulnerability. Machine learning algorithms have shown promise in detecting malware on Android devices. This research paper investigates the use of machine learning for Android malware detection. The proposed approach leverages machine learning algorithms to learn and classify Android malware. Experimental results demonstrate the efficacy of the proposed approach in detecting Android malware with high accuracy.

445. Mustafa A.M. Analysis of Sources of Personal Data Formation in Cyber-Physical Social Systems / **IEEE 17th International Conference on Application of Information and Communication Technologies (AICT),** Baku, **18-20 October 2023,** pp. 150-153.

The recent rapid development of the interaction of individuals with cyber-physical social systems has necessitated the exploration of the security and privacy principles during the collection, storage, processing, and use of personal data in cyber-physical social systems (CPSS). Based on the above, this

study analyzes and classifies the sources of personal data formation in CPSS. This study plays an important role in future research to ensure personal data security in CPSS.

446. Ojagverdiyeva S.S. Development Children 4.0 concept for information security of school-age children based on wearable technology // **Problems of Information Society. 2024,** vol. 15, no. 2, pp. 61-70.

Modern children are growing up with the influence of technology, and their use of wearable devices shows a noticeable increase in their technological skills and a rapidly evolving digital landscape. One of the advantages of sensor technologies is that these smart objects have the ability to transmit information in time, provide availability and communicate in real time. Portable devices enable parents to get real-time information about school-age children's behavior, education, location and physical activities, and in short, to track and monitor their children's behavior. However, as the volume of data obtained through sensors increases, it becomes difficult for parents to analyze this data and requires protection mechanisms using intelligent technologies. Since the information collected in the database through portable devices is sensitive and informative, individuals or companies are interested in using this information for various purposes. The Children 4.0 concept proposed in this study is a comprehensive approach to ensuring the security of information collected in databases (medical information, location information, etc.)

through a portable item (bracelet). This approach is offered to ensure the information security of school-age children based on mobile technology while protecting children's personal information.

447. Alguliyev R.M., Aliguliyev R.M., Sukhostat L.V. Radon transform based malware classification in cyber-physical system using deep learning // **Results in Control and Optimization. 2024,** issue 100382, vol. 14, pp. 1-14.

The development of cyber-physical systems entails the growth and diversity of malware, which increases the scale of cybersecurity threats. Attackers use malicious software to compromise various components of cyber-physical systems. Existing technologies make it possible to reduce the risk of malware infection using vulnerability and intrusion scanners, network analyzers, and other tools. However, there is no perfect protection against the increasingly sophisticated types of malware. The goal of this research is to solve this problem by combining different visual representations of malware and detection models based on transfer learning. This method considers two pre-trained deep neural network models (AlexNet and MobileNet) that are capable of differentiating various malware families using grayscale images. Radon transform is applied to the resulting grayscale malware images to improve the classification accuracy of the new malware binaries. The proposed model is evaluated using three datasets (Microsoft Malware Classification, IoT_Malware and MalNet-

Image datasets). The results show the superiority of the proposed model based on transfer learning over other methods in terms of the efficiency of classifying malware families aimed at infecting cyber-physical systems.

448. Mehdiyev S.A., Hashimov M.A. Analysis of Threats and Cybersecurity in the Oil and Gas Sector within the Context of Critical Infrastructure // **International Journal of Information Technology and Computer Science. 2024,** vol. 16, no. 1, pp. 43-53.

This article explores the multifaceted challenges inherent in ensuring the cybersecurity of critical infrastructures, i.e., a linchpin of modern society and the economy, spanning pivotal sectors such as energy, transportation, and finance. In the era of accelerating digitalization and escalating dependence on information technology, safeguarding these infrastructures against evolving cyber threats becomes not just crucial but imperative. The examination unfolds by dissecting the vulnerabilities that plague critical infrastructures, probing into the diverse spectrum of threats they confront in the contemporary cybersecurity landscape. Moreover, the article meticulously outlines innovative security strategies designed to fortify these vital systems against malicious intrusions. A distinctive aspect of this work is the nuanced case study presented within the oil and gas sector, strategically chosen to illustrate the vulnerability of critical infrastructures to cyber threats. By examining this sector in detail, the article aims to

shed light on industry-specific challenges and potential solutions, thereby enhancing our understanding of cybersecurity dynamics within critical infrastructures. This article contributes a comprehensive analysis of the challenges faced by critical infrastructures in the face of cyber threats, offering contemporary security strategies and leveraging a focused case study to deepen insights into the nuanced vulnerabilities within the oil and gas sector.

449. Mehdiyev Sh.A., Hashimov M.A. Analysis of Threats and Cybersecurity in the Oil and Gas Sector within the Context of Critical Infrastructure // **International Journal of Information Technology and Computer Science. 2024,** vol. 16, no. 1, pp. 43-53.

This article explores the multifaceted challenges inherent in ensuring the cybersecurity of critical infrastructures, i.e., a linchpin of modern society and the economy, spanning pivotal sectors such as energy, transportation, and finance. In the era of accelerating digitalization and escalating dependence on information technology, safeguarding these infrastructures against evolving cyber threats becomes not just crucial but imperative. The examination unfolds by dissecting the vulnerabilities that plague critical infrastructures, probing into the diverse spectrum of threats they confront in the contemporary cybersecurity landscape. Moreover, the article meticulously outlines innovative security strategies designed to fortify these vital systems against malicious intrusions. A

distinctive aspect of this work is the nuanced case study presented within the oil and gas sector, strategically chosen to illustrate the vulnerability of critical infrastructures to cyber threats. By examining this sector in detail, the article aims to shed light on industry-specific challenges and potential solutions, thereby enhancing our understanding of cybersecurity dynamics within critical infrastructures. This article contributes a comprehensive analysis of the challenges faced by critical infrastructures in the face of cyber threats, offering contemporary security strategies and leveraging a focused case study to deepen insights into the nuanced vulnerabilities within the oil and gas sector.

450. Shikhaliyev R.H. Cybersecurity risks management of industrial control systems: A review // **Problems of Information Technology. 2024**, vol. 15, no. 1, pp. 37-43.
Industrial control systems (ICS) form the basis of critical infrastructures, managing complex processes in various sectors of industry, energy, etc. With the increasing frequency and complexity of cyber threats, effective management of ICS cybersecurity risks is critical. This paper is devoted to the analysis of approaches used in the field of cybersecurity risk management of automated process control systems. The study examines the cybersecurity risks of ICS and the role of international standards in managing cybersecurity risks. The results of the analysis carried out in this paper can serve as

information for the development of new reliable cybersecurity risk management systems for ICS.

451. Abdullayeva F.D., Suleymanzade S.N. Cyber security attack recognition on cloud computing networks based on graph convolutional neural network and graphsage models // **Results in Control and Optimization. 2024,** no.15, pp. 1-10.

In this paper, the modeling of the network attacks of cloud computing through Graph Neural Networks is considered. Based on structural features and relationships between neighboring nodes and the edges of the cloud ecosystem a cyberattack detection method is proposed. A simulation dataset is created on the CSE-CIC-IDS2018 dataset to train and test the proposed graph neural network based models. In a comparative analysis of the suggested method with the existing one superior results are obtained from the model constructed on the GraphSAGE algorithm. Thus in the recognition of dataset samples, the model obtained a value of 0.97739 according to the accuracy metric. The values obtained by the algorithm on precision, recall, and F1-score metrics were also higher compared to the Graph Convolutional Neural Network model.

452. Alakbarov R.K., Hashimov M.A. Application of Artificial Intelligence Technologies in Security of Cyber-Physical Systems // **International Journal of Computer**

Science & Information Technology. 2024, vol. 16, no. 4, pp. 37-51.

Cybersecurity questions of cyber-physical systems (CPS) have become ever more vital in recent times. Advances in technology and digitization have posed new weaknesses in CPS and cyber attackers take advantage of it. Viruses, malware, and sophisticated forms of cyberattacks have become a dangerous reality for critical infrastructure CPS. Lately, artificial intelligence (AI) technology has been extensively applied in the struggle against cyber threats in CPS. AI may improve system security by providing tools to quickly detect cyberthreats and automatically resolve them. Digitization of critical infrastructures (energy distribution networks, smart systems, oil and gas industry, water infrastructure, etc.) has increased their efficient management and at the same time, the number of cyber attackers on sensors, actuators, network and control equipment has also increased. Cyber security of critical objects can be ensured through AI. This article explores the theoretical foundations, application fields, and AI conceptual models. It analyzes the benefits and shortcomings of applying AI technologies to the security of the abovementioned systems. Mechanisms for detecting cyber threats in cyber-physical systems with the help of AI and predicting and preventing security threats are proposed.

453. Mahmudova R.Sh. Smart socio-technological infrastructures: cyber security risks and the human factor

// **Problems of Information Society. 2024,** vol. 15, no. 2, pp. 49-60.

Smart socio-technological infrastructure is a new approach to the design and creation of complex systems, based on the integration of technological and social elements. Currently, smart sociotechnological infrastructures are applied in all spheres of life, from business and industry to healthcare and medical facilities. The implementation of these infrastructures creates new opportunities for the development of various fields. However, it causes a number of problems. The reasons for new information security problems arising from the characteristics of smart sociotechnological infrastructures may include the increase in the number of devices (the number of devices interacting with each other increases, which expands the potential attack plane), the complexity of integration (the integration of social and technological components leads to the creation of new vulnerabilities), data heterogeneity (where the processing and storage of various types of information, including confidential information, make them an attractive target for cybercriminals), the dynamism of the environment (smart socio-technological infrastructures are constantly evolving and adapting, which makes it difficult to ensure their security). This article examines information security problems of smart socio-technological infrastructures. New threats arising from the introduction of these infrastructures are classified. The development of information security culture is

justified as one of the main factors of combating these threats, and recommendations are given on the principles and methods of its formation.

454. Valikhanli O.V. UAV networks DoS attacks detection using artificial intelligence based on weighted machine learning // **Results in Control and Optimization**. **2024**, 100457, vol. 16, pp. 1-8.

While Unmanned Aerial Vehicles (UAVs) have found applications across numerous industries, they still remain vulnerable to various cybersecurity challenges. Different types of cyberattacks target UAVs. Early detection of these cyberattacks is considered the most important step in ensuring the cybersecurity of UAVs. In this article, an artificial intelligence method based on machine learning was developed for detecting different types of Denial of Service (DoS) attacks targeting the UAV network. Initially in this work, feature selection methods are implemented to select the most important features. Then, machine learning methods are used to classify attacks. According to the conducted experiments, the proposed method outperformed others with an accuracy of 99.51 % and a prediction time of 0.1 s. Additionally, a novel dataset is used in this work, which offers several advantages. The dataset was created within a real-world environment rather than a simulated one. Furthermore, the data were collected within a 5G network.

455. Imamverdiyev Y.N., Sukhostat L.V. COVID-19: cybersecurity issues in times of pandemic // **Electronic Government. 2024**, vol. 20, no. 5, pp. 569-590.

COVID-19 is one of the worst threats to the global community in this century. Society is facing a massive number of cyberattacks during this period. Cybersecurity is an issue for individuals and organisations, given the growing number of people using the internet. The purpose of this survey is to identify key cybersecurity problems and solutions during a pandemic, observed in the healthcare sector, education, and critical infrastructures. Cybersecurity issues during COVID-19 are analysed and aspects of personal data security are discussed. We studied the most prominent cyberattacks during the pandemic and found that they were related to phishing, ransomware, malware, and hacking. Measures to combat infodemics and the role of social media are explored. The evolution of infodemic risk from 2020 to 2022 is analysed. This research is expected to be very useful for improving cybersecurity systems in the context of heightened demands during COVID-19 and in the post-pandemic period.

456. Alguliyev R.M., Shikhaliyev R.H. Network cybersecurity incidents multiclassification based on deep learning // **Problems of Information Technology**. **2024**, vol. 15, no. 2, pp.16-23.

The rapid increase in network traffic and the growing complexity of cyberattacks have rendered traditional

cybersecurity monitoring methods insufficient for effectively detecting and classifying network incidents. To overcome these limitations, we present a deep learning-based approach that utilizes a hybrid architecture, combining Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) models, for the multi-classification of cybersecurity incidents. Our model is trained on the CICIDS2017 dataset, which encompasses a wide range of attack types. The hybrid CNN-LSTM model achieved a classification accuracy of 96.76% and an error rate of 9.34%, showcasing its ability to accurately detect and classify various cybersecurity threats. This approach offers a robust solution for enhancing the detection and classification of network cybersecurity incidents

457. Abdullayeva F.D., Valikhanli O.V. A survey on UAVs security issues: attack modeling, security aspects, countermeasures, open issues // **Control and Cybernetics**. **2024**, vol. 52, no. 4, pp. 405-439.

The Unmanned Aerial Vehicles (UAVs) are being ac tively used in various fields including agriculture, surveillance, sci entific research, and delivery. Despite their widespread use, UAVs face significant cybersecurity challenges due to their vulnerabilities as cyber-physical systems. UAVs are vulnerable to cyberattacks, which target cyber or physical elements, the interface between them, wireless connections, or a combination of several components. Given the complexity of securing these systems, this paper provides a com prehensive survey of the

current state of UAV cybersecurity. More over, different cybersecurity issues of UAVs are analyzed, various features, and functions of UAVs are considered. UAV attack clas sification scheme is constructed and attacks on various components are accounted for. Also, countermeasures against cyberattacks that target UAVs are discussed. Finally, UAV cyber security datasets for research purposes are indicated, and the remaining open issues in this field are identified.

458. Elshan Baghirov. A Comprehensive Framework for Real-Time Malware Detection and Monitoring in Production // **International Journal on Information Technologies & Security. 2024**, vol. 16, no. 4, pp. 85-94.

This paper proposes a comprehensive framework for real-time malware detection and monitoring tailored to operational systems. Leveraging advanced machine learning algorithms, our framework integrates continuous monitoring mechanisms to ensure timely detection and response to emerging threats. The framework emphasizes regular assessment of model performance using metrics such as the Population Stability Index (PSI), ensuring models remain effective and adaptive to evolving malware patterns. By deploying models within the production environment, the framework enables regular evaluation and adaptation, enhancing the robustness and reliability of the detection system. Our results demonstrate the framework's efficacy in providing a scalable and efficient solution for real-time malware detection and monitoring,

contributing to improved cybersecurity posture in dynamic and high-risk environments.

459. Alguliyev R.M., Mahmudov R.Sh. About Some Socio-economic Problems and Risks of Artificial Intelligence // **International Journal of Science, Technology and Society. 2024**, vol. 12, no. 5, pp. 140-150.

Article analyses some socio-economic risks related to application of artificial intelligence (AI) in several fields of activity. Also, existing gaps in legal regulation of activities related to artificial intelligence are investigated. Article clarifies issues related todetermining the division of liability for certain legal consequences resulting from artificial intelligence activity. Also, norms andprinciples to be adhered to in order to protect personal data during application of AI are demonstrated. As one of the concernsamong people regarding artificial intelligence, article notes the importance of provision of transparence and accountability of thistechnology. Simultaneously, article interprets problems arising from relations of artificial intelligence and intellectual property, as well as recognition of property rights for intellectual products created via AI. Also, macro and micro-level impact of artificialintelligence on economy is analyzed. Attention is paid to issues such as productivity, competition, changes in the nature of thelabor market, the increase in unemployment, and the deepening of social and digital inequality as a result of the application of thistechnology. Moreover, advantages and risks

of human-robot collaboration are evaluated. Article demonstrates the biggest threatsof artificial intelligence – creation of fake content, misinformation and hence, creation of significant problems. Preventionmethods of those threats are interpreted on technological and legal planes. Also, risks of application of artificial intelligence incritical fields such as military and health are characterized.

460. Alguliyev R.M., Aliguliyev R.M., Sukhostat L.V. Method for quantitative risk assessment of cyber-physical systems based on vulnerability analysis // **Kybernetika,** vol. 60, no. 6, **2024**, pp. 779-796.

Cyber-physical system protection against cyber-attacks is a serious problem that requires methods for assessing the cyber security risks. This paper proposes a quantitative metric to evaluate the risks of cyber-physical systems using the fuzzy Sugeno integral. The simulated attack graph, consisting of vulnerable system components, allows for obtaining various parameters for assessing the risks of attack paths characterizing the elements in the cyber and physical environment and are combined into a single quantitative assessment. Experiments are performed on a threat model using the example of a cyber-physical system for wind energy generation. The model integrates a cyber-physical network's topology and vulnerabilities, proving the proposed method's effectiveness in ensuring cyber resilience.

461. Mahmudova Sh. Development of a conceptual model for ensuring cyber-resilience of software systems // **Open Access Library Journal**. **2024**, vol. 11, no. 7, pp. 1-9.

Cyber-resilience of software systems is the ability to prevent, resist, and recover from adverse incidents using IT resources. Infrastructure can be extended through cyber-resilience. In this case, the problems can be solved in a short time. In this study, some methods of ensuring the cyber-resistance of the software system are explored. The role, type, and characteristics of cyber-resilience for the software system are also examined in the work. Ways to implement Cyber-resilience measures for cyber security and information technology are analyzed. The paper also outlines the ways to enhance cyber-resi- lience through smart threat operations. Cyber security possibilities and the ways to solve the problems encountered are highlighted. A new model is developed to ensure the cyber-resilience of the software system used.

462. Imamverdiyev Y.N., Baghirov E.O. Evasion techniques in malware detection: challenges and countermeasures // **Problems of Information Technology**. **2024**, vol. 15, no. 2, pp. 9-15.

In the ever-evolving digital landscape, the escalating sophistication of malware poses a substantial threat, necessitating continual advancements in detection methods. This paper addresses the pervasive challenge of evasion techniques employed by malware to circumvent standard

security measures. Focused on understanding the intricate methods employed by malware developers, our study explores the dynamic nature of this cyber threat. As malicious actors continually refine their approaches, a nuanced understanding of evasion tactics becomes paramount for developing effective countermeasures. The research emphasizes the need for robust defense mechanisms capable of adapting to the constantly changing cyber threat landscape. By unraveling the complexities of evasion techniques, this paper contributes valuable insights to the development of proactive and resilient cybersecurity measures. Through an exploration of specific evasion tactics, we aim to inform and empower cybersecurity professionals, facilitating the creation of strategies capable of effectively mitigating the risks posed by these dynamic digital threats.

463. Rzayeva N.A. Pilotsuz uçuş aparatlarının istifadəsində məxfilik risklərinin təhlili / "**Fevral məruzələri 2024: Aviakosmik məsələlərin həllində gənclərin yaradıcı potensialı" IX Beynəlxalq elmi-praktiki gənclər konfransı.** Bakı, **8-10 fevral 2024,** s. 118-120.

İnformasiya-kommunikasiya texnologiyalarının inkişafı həyatımızı zənginləşdirdi, eyni zamanda, informasiya təhlükəsizliyi sahəsində yeni çağırışlar da gətirdi. Daim inkişaf edən rəqəmsal mühit kontekstində dronlar texnologiya inkişafının ayrılmaz hissəsinə çevrilib. Lakin onların geniş istifadəsinə görə məxfilik problemləri özlüyündə problem

yaratmağa başlayır. Məqalə dronların təhlükəsizlik problemlərinin öyrənilməsinə həsr olunub və onların istifadəsi nəticəsində yaranan fərdi məlumatların təhlükəsizliyi problemlərini aydınlaşdırmağa kömək edir. Mövzunun aktuallığı əsaslandırılmışdır. Bundan başqa, fərdi məlumatların təhlükəsizliyindən bəhs edilir. Dronlarda məxfilik riskləri və onların yaranmasının mümkün səbəbləri təhlil olunur. Eyni zamanda, geniş spektrli problemləri əhatə edən fərdi məlumatlardan sui-istifadə riskləri araşdırılmışdır. Həmçinin məqalənin məqsədi dronlardan istifadə zamanı yarana biləcək fərdi məlumatlara qarşı təhlükələri qısaca təhlil etməkdir.

464. Rzayeva N.A. Kompüter şəbəkələrində kibertəhlükəsizlik məsələlərinin təhlili / **"İdarəetmədə və təhsildə informasiya kommunikasiya texnologiyaları" I respublika elmi konfransı.** Naxçıvan, **17-18 sentyabr 2024,** s.99-101.

Kibertəhlükəsizlik və ya kompüter təhlükəsizliyi kompüterlərin, mobil cihazların, elektron sistemlərin, xidmətlərin, şəbəkələrin və məlumatların kibercinayətkarların hücumlarından qorunması təcrübələri və metodlar toplusudur. Şəbəkələrin inkişafının başlanğıcında təhlükəsizlik aktual deyildi, bu, internetdə kiçik bir istifadəçi dairəsinin olması ilə əlaqədar idi. Bu gün kompüter şəbəkələrinin və internetin həyatın bütün sahələrini əhatə etməsi ilə əlaqədar olaraq kibertəhlükəsizliyin rolu daha da aktuallaşır. Kibertəhlükəsizliyə müxtəlif sahələrdə

və müxtəlif istiqamətlərdə, məsələn, biznes sferasında, mobil texnologiyalarda rast gəlmək olar.

465. Rzayeva N.A. Kibertəhlükəsizlikdə süni intellektin tətbiqləri / "**Süni intellekt: nəzəriyyədən praktikaya**" **beynəlxalq elmi konfrans.** Naxçıvan, **17-18 sentyabr 2024,** s. 344-348

Süni intellekt mürəkkəb, çoxşaxəli və sektorlararası bir sahədir. Süni intellekt, şübhəsiz ki, insan fəaliyyətinin bütün sahələrinə nüfuz edərək, dövrümüzün əsas texnoloji nailiyyətlərindən birinə çevrilmişdir. Süni intellekt maşın öyrənməsi, neyron şəbəkələri, təbii dillərin işlənməsi və robototexnika kimi əsas prinsiplərə əsaslanır. Əsas problem süni intellektin kibertəhlükəsizlik sahəsində necə işlədiyini təhlil etməkdir. Bu məqalədə biz süni intellektin təkcə düşünmə, planlaşdırma, öyrənmə və məlumatların emalı texnologiyası kimi deyil, həm də obyektləri manipulyasiya etmək bacarığından bəhs edəcəyik.

466. Valixanlı O.V. Pilotsuz uçuş aparatlarının naviqasiya sisteminə edilən GPS əngəlləmə kiberhücumunun aşkarlanması metodu / **Azərbaycan xalqının ümummilli lideri Heydər Əliyevin anadan olmasının 101-ci ildönümünə həsr olunmuş Tələbə və Gənc Tədqiqatçıların V Beynəlxalq elmi konfransları,** Bakı, **23 aprel - 1 may 2024**, s. 440-442.

Pilotsuz uçuş aparatlarının (PUA) naviqasiya sistemini hədəf alan bir neçə kiberhücum növü mövcuddur. Bunlardan biri də GPS əngəlləməsi kiberhücumudur. Məqalədə PUA-ların

naviqasiya sistemini hədəf alan GPS əngəlləməsi kiberhücumunun aşkarlanması üçün hibrid yanaşma təklif olunmuşdur. Hibrid yanaşmada iki müxtəlif tip məlumat növündən istifadə edilmişdir. Yeni yanaşmanın səmərəliyini yoxlamaq üçün müxtəlif eksperimentlər aparılmışdır.

467. Рзаева Н.А., Вердиева Н.Н. Анализ проблем защиты персональных данных в киберфизических системах / **XXIII Международная научно-техническая конференция "Развитие информатизации и государственной системы научно-технической информации" (РИНТИ-2024).** Минск, **21 ноября 2024,** с. 90-95.

Представлен анализ существующих проблем защиты персональных данных в киберфизических системах (КФС). Рассмотрены технологии и типы угроз, которым они подвергаются. Описаны некоторые решения данной области исследований. Определены направления исследований в области защиты конфиденциальности, которые могут помочь исследователям разработать новые подходы к защите от угроз в КФС.

468. Nabiyev B.R., Dashdamirova K.G. About the technological and cyber security aspects of ensuring the heterogeneous usage policy of the Internet environment / **2nd International Conference on Information Technologies and Their Applications (ITTA 2024).** Baku**, 23-24 April 2024**, pp. 1-12.

The internet has numerous profoundly infiltrated facets of human endeavor, evolving into a pivotal substitute for traditional ways of information acquisition and dissemination. This phenomenon enables the swift propagation of information, transcending geographical and temporal barriers through advanced information and communication technologies. As global communications gravitate towards cyberspace, social interactions increasingly occur within this digital realm. Individuals united by common ideologies or interests shift from physical reality to virtual communities, thereby shaping distinct virtual societies. Despite the internet's extensive reach and integration into diverse domains, access to all online resources is not universal. The vast array of internet resources, serving varied purposes, has resulted in a layered and segmented cyberspace, comprising various closed or private virtual networks accessible only by specific groups. This stratification, coupled with the utilization of different network layers for illicit activities, has precipitated several global challenges encompassing economic, political, and cybersecurity dimensions. Consequently, entities such as nation-states, corporations, groups, and individuals have erected virtual barriers and borders within the internet, establishing different usage policies. This paper highlights the cybersecurity implications of implementing heterogeneous usage policies in the internet environment. It also identifies and analyzes the

interconnection points among different internet layers, offering insights into their structural and functional dynamics.

469. Mahmudova Sh.J. Analysis of existing approaches to increase cyber resilience / **XVII International Scientific and Practical Conference "Challenges and problems of modern science",** London, **September 5-6, 2024**, pp. 92-95.

This work studies cyber security, its problems, measures, and operations. It also analyzes cyber risks and cyber resilience framework to increase cyber resilience. A cyber resilience framework is a comprehensive set of structured guidelines and practices designed to strengthen anorganization's ability to effectively with-stand and recover from cyber threats. The difference between a cyber resilience framework and a cybersecurity strategy lies in their scope and specificity. While a cybersecurity strategy describes a general approach to protecting digital assets, a cyber resilience framework examines the finer details of the activities and processes necessary to ensure resilience. A strong cyber resilience framework offers many benefits to organizations. A strong cyber resilience framework promises many benefits to companies. The cyber resilience framework rec-ommends 10 powerful propositions and examines their merits. A cyber resilience strategy prepares to proac-tively deal with threats, mitigate potential damage and ensure smooth business continuity.

470. Mahmudova Sh.J. Analysis of international experience on ensuring cyber resilience in software systems / **XI International Scientific and Practical Conference "Theoretical and practical perspectives of modern science"**. Stockholm, **August 27-28 2024,** pp. 91-94.

Cyber resilience in software systems is the ability to prevent, resist, and recover from various malicious events that occur when using information technology (IT) resources. Computing capabilities, artificial intelligence, digital security systems, connected devices, national defense systems, smart equipment and advanced communication networks such as 5G, 6G, the Internet of Smart Things (IoST) are tools of Industry 4.0. To ensure cyber resilience, multiple cyber vulnerabilities must be identified and addressed in the country's most critical economic and national security infrastructures. In addition, obviously, it is important to have professionals with the necessary skills, training and experience to solve these problems.

471. Alakbarov R.K., Hashimov M.A. The Role of Artificial Intelligence in Cyber resilience of Cyberphysical Systems / **Proceedings of the 9th International Conference on Control and Optimization with Industrial Applications (COIA-2024).** Istanbul, **27-29 August 2024,** pp. 721-725.

Lately, artificial intelligence (AI) technology has been extensively applied in the struggle against cyber threats in CPS. AI may improve system security by providing tools to

quickly detect cyberthreats and automatically resolve them. Digitization of critical infrastructures (energy distribution networks, smart systems, oil and gas industry, water infrastructure, etc.) has increased their efficient management and at the same time, the number of cyber attackers on sensors, actuators, networkand control equipment has also increased. Cyber security of critical objects can be ensured through AI. This article explores the role of AI in enhancing the cyber resilience of CPS. The article analyzes the advantages and disadvantages of using AI technologies in the security of Cyber-Physical systems. Mechanisms for detecting cyber threats in cyber-physical systems with the help of AI, predicting and preventing security threats have been proposed.

472. Ocaqverdiyeva S.S. Yaşıl transformasiya şəraitində uşaq təhlükəsizliyi // **Yaşıl və rəqəmsal transformasiyalar: qarşılıqlı təsirləri, pozitiv və neqativ aspektləri. Məqalələr toplusu. 2025**, s. 56-61.

Məqalədə yaşıl transformasiyaların rəqəmsal sənayeyə inteqrasiyası və bunun uşaqların onlayn təhlükəsizliyi və sağlamlığına potensial təsiri araşdırılır. Yaşıl transformasiyalar ilk növbədə ekoloji davamlılığı hədəfləsə də, məxfiliyi, məlumat təhlükəsizliyini və yaş qrupuna uyğun rəqəmsal platformalar tətbiq etməklə uşaqların onlayn təhlükəsizliyinin təmini kimi faydalar da təqdim edir. Digər tərəfdən uşaqların rəqəmsal cihazlardan həddindən artıq istifadəsinin mənfi nəticələri, o cümlədən təbiətlə əlaqənin

azalması, elektron tullantılar və elektromaqnit şüalanma kimi zərərli ətraf mühit amillərinə potensial məruz qalma halları araşdırılır. Rəqəmsal əsrdə uşaqlara ekoloji cəhətdən şüurlu və sağlam həyat tərzi üçün məsələlərin həllində İKT proqramları vasitəsilə yaşıl transformasiyaları mənimsətmək və 30 ekran vaxtının düzgün idarə edilməsi kimi həllər müzakirə olunur. Yaşıl transformasiya mühitində uşaqların təhlükəsizliyinin təmin edilməsi üçün təklif və tövsiyələr verilmişdir.

473. Mahmudova R.Ş. Ağıllı şəhərlər və yaşıl texnologiyalar kontekstində informasiya təhlükəsizliyi mədəniyyətinin inkişaf etdirilməsi məsələləri // **Yaşıl və rəqəmsal transformasiyalar: qarşılıqlı təsirləri, pozitiv və neqativ aspektləri.** Məqalələr toplusu. **2025,** s. 89-92.

Bu məqalədə ağıllı şəhər konsepsiyasının aktuallığı və onun müasir cəmiyyət üçün vacibliyi ətraflı təhlil olunur. Ağıllı şəhərlərin əsas məqsədi, resursların səmərəli istifadəsini təmin etmək, ekoloji təsirləri minimuma endirmək və vətəndaşların həyat keyfiyyətini artırmaqdır. Bu baxımdan bir sıra müasir texnologiyalardan istifadə olunur ki, onlardan biri də yaşıl texnologiyalardır. Ağıllı şəhərlər müasir texnologiyaların geniş tətbiqi ilə idarə olunur, lakin bu, təhlükəsizlik risklərini də artırır. Belə ki, bu şəhərlərdə məlumatların toplanması və saxlanması prosesi, IoT (İnternet of Things) cihazlarının geniş tətbiqi və infrastrukturlarda mövcud olan boşluqlar kibertəhlükələrə səbəb ola bilər. Məqalədə insan səhvlərinin

kibertəhlükəsizlik risklərini artırdığı vurğulanır və bu riskləri azaltmaq üçün tövsiyələr verilir.

474. Alguliyev R.M., Aliguliyev R.M., Sukhostat L.V. An approach for assessing the functional vulnerabilities criticality of CPS components // **Cyber Security and Applications. 2025,** no. 3, pp. 1-7.

Timely identification of critical security flaws in a cyber-physical system makes identifying risks and potential threats possible. To address this issue, threat models are created to better understand potential vulnerabilities that must be considered to ensure system reliability. Selecting the optimal solution for assessing the functional vulnerabilities criticality of cyber-physical system components is a complex process since all vulnerabilities must be identified, classified, and quantified according to a unified approach as part of the cybersecurity process. An effective tool for cyber-physical systems analysis is the Bayesian attack graph. Each path in the graph represents a sequence of attacks that an attacker can use to achieve a specific goal, such as gaining access to sensitive data or controlling a system. This paper proposes a quantitative method for assessing the vulnerability criticality of cyber-physical system components based on the Promethee II multi-criteria decision-making method. It allows ranking and identification of the system"s most vulnerable components. The proposed approach is evaluated using a threat model and three scenarios of cyberattacks on a cyber-physical system. Comparison with

TOPSIS, VIKOR, and ELECTRE methods proves the effectiveness of the proposed approach. The proposed approach can help technical specialists make more reasoned decisions when ranking critical vulnerabilities of cyber-physical system components to provide security measures and prevent cyberattacks.

475. Baghirov E.O. A comprehensive investigation into robust malware detection with explainable AI // **Cyber Security and Applications. 2025,** vol. 3, pp. 1-11.

In today's digital world, malware poses a serious threat to security and privacy by stealing sensitive data and disrupting computer systems. Traditional signature-based detection methods have become inefficient and time-consuming. However, data-driven AI techniques, particularly machine learning (ML) and deep learning (DL), have shown effectiveness in detecting malware by analyzing behavioral characteristics. Despite their promising performance, the black-box nature of these models requires improved explainability to facilitate their adoption in real-world applications. This can complicate the ability of cybersecurity experts to evaluate the model's reliability. In this work, Explainable Artificial Intelligence (XAI) is employed to comprehend and evaluate the decisions made by machine learning models in the detection of malware on Android devices. To evaluate malware detection, experiments were conducted using CICMalDroid dataset by applying ML models like Logistic Regression and several tree

algorithms. An overall 94% F1-score was achieved, and interpretable explanations for model decisions were provided, highlighting more critical features that contributed to accurate classifications. It was found that employing XAI techniques can provide valuable insights for malware analysis researchers, enhancing their understanding of the operations of the ML model, rather than solely focusing on improving accuracy.

476. Alguliyev R.M., Shikhaliev R.H. Computer Networks Cybersecurity Monitoring Based on Deep Learning Model // **Security and Privacy. January - February 2025**, vol. 8, iss. 1, e459, 18 p.

Effective cybersecurity monitoring is essential for safeguarding computer networks against evolving threats. However, the increasing scale, complexity, and data volume of modern networks pose significant challenges to traditional monitoring methods. To address these challenges, this article proposes a deep learning-based approach for computer network cybersecurity monitoring. Leveraging the MnasNet-LSTM model, network traffic data is classified into distinct categories, including normal traffic and cyberattacks. The model is trained using the CICIDS2017 dataset, yielding promising results with a classification accuracy of approximately 97.05% and a minimal error rate of 8.46%.

477. Alguliyev R.M., Abdullayeva F.J., Ojagverdiyeva S.S. Fuzzy expert system for access control of children to the

internet // **International Journal of Reasoning-based Intelligent Systems. 2025**, vol. 16, no. 6, pp. 455-462.

As children's use of the internet increases, serious online safety issues arise. As a result, it is observed that the damage to their psychology and health is increasing. Along with harmful content from web pages, the negative impact of constant use of digital devices leaves deep marks on children's health and psychology. In order to overcome these problems and prevent harm, there is a need to implement programs that control access to the internet, filter harmful content on web pages, constantly monitor children's behaviour, make assessments and make accurate decisions. The article proposes a method of internet access control using a fuzzy logic inference system. This method is focused on the individual user and is done by imposing restrictions on their use of technologies (computers, phones, tablets, etc.). Screen time is determined for the use of technology, taking into account the age of the user, health and psychological diseases.

478. Baghirov E.O., Imamverdiyev Y.N., Chukwu I.J. Detecting Obfuscated Malware Infections on Windows Using Ensemble Learning Techniques // **Informatics and Automation. 2025,** no. 1, vol. 24**,** pp. 99-124.

In the internet and smart devices era, malware detection has become crucial for system security. Obfuscated malware poses significant risks to various platforms, including computers, mobile devices, and IoT devices, by evading advanced security

solutions. Traditional heuristic-based and signature-based methods often fail against these threats. Therefore, a cost-effective detection system was proposed using memory dump analysis and ensemble learning techniques. Utilizing the CIC-MalMem-2022 dataset, the effectiveness of decision trees, gradient-boosted trees, logistic Regression, random forest, and LightGBM in identifying obfuscated malware was evaluated. The study demonstrated the superiority of ensemble learning techniques in enhancing detection accuracy and robustness. Additionally, SHAP (SHapley Additive exPlanations) and LIME (Local Interpretable Model-agnostic Explanations) were employed to elucidate model predictions, improving transparency and trustworthiness. The analysis revealed vital features significantly impacting malware detection, such as process services, active services, file handles, registry keys, and callback functions. These insights are crucial for refining detection strategies and enhancing model performance. The findings contribute to cybersecurity efforts by comprehensively assessing machine learning algorithms for obfuscated malware detection through memory analysis. This paper offers valuable insights for future research and advancements in malware detection, paving the way for more robust and effective cybersecurity solutions in the face of evolving and sophisticated malware threats.

479. Bayramova T.A. Development of a conceptual model for ensuring fault tolerance of software systems //

Problems of Information Technology. 2025, no. 1, vol.16, pp. 35-46.

Digital transformation is a comprehensive process of integrating information technology into all areas of human activity. Almost all aspects of our lives, from personal communications to global economic processes, are increasingly integrated with digital technologies. Banking, manufacturing, healthcare, education, and transportation are all increasingly using software to improve efficiency, optimize processes, and provide new services. Modern applications are becoming increasingly complex, consisting of many interconnected components. This increases the likelihood of errors and failures. The relevance of research in the field of software reliability is steadily growing.This article is devoted to the study of the differences and relationships between information and software systems, as well as an in-depth analysis of the key concepts of software reliability and fault tolerance. The main approaches and strategies for ensuring fault tolerance are considered, including redundancy, backup, monitoring, duplication, load balancing, microservices, backup, prediction and detection of errors, as well as their practical application. The aim of the study is to define the principles and methods of self-healing software and to analyze the risks associated with automatic response to failures. To solve the problem of ensuring fault tolerance in dynamic and complex software systems, a

conceptual model for designing reliable, self-learning and self-adaptive systems is proposed.

480. Zalova S.M. Cybersecurity issues in journalism based on artificial intelligence technologies // **Problems of Information Society. 2025,** no. 1, vol. 16, pp. 94-101.

Although the use of artificial intelligence in journalism creates innovations and opportunities, this process leads to complications in a number of cybersecurity issues. One of the main problems is the risk of disinformation and manipulation. Although artificial intelligence algorithms automatically process information, it is possible for these algorithms to make decisions based on incorrect information, which can result in the dissemination of biased or false news. At the same time, the database used in artificial intelligence programming can affect its objectivity and impartiality. The use of data collected by artificial intelligence and sources without verification can lead to the dissemination of untrustworthy and inaccurate news. This article examines cybersecurity issues arising from the application of artificial intelligence technologies in journalism. Artificial intelligence technologies are currently widely used at all stages of news production. It highlights the current situation regarding artificial intelligence technologies and the application of these technologies to journalism, as well as the problems encountered in this field. This article examines the problems arising from the application of artificial intelligence technologies. "Deepfake" technologies, their negative aspects,

and the problems they may cause are studied. Proposals are made for solving cybersecurity issues and a conceptual model is developed.

481. Valikhanli O.V. Detection of malware in ground control stations of unmanned aerialvehicles based on image processing // **International Journal of Information and Computer Security. 2025,** no. 1-2, vol. 26, pp. 147-158.
Recently, unmanned aerial vehicles (UAVs) have become very popular due to their wide range of applications. UAVs are quite popular because they are more affordable and simpler to use compared to other vehicular systems. However, as with other cyber physical systems UAVs and their ground control stations (GCSs) may also be targeted by attackers. In this work, greyscale images are analysed to detect malwares in GCSs. The proposed hybrid model is based on ResNet-50 and support vector machine (SVM). ResNet-50 is used to extract necessary features from images. Subsequently, SVM is used to classify malware based on extracted features. Moreover, other hybrid models are also tested in this work to compare final results. As a result, proposed model achieved 98.62% accuracy.

482. Valikhanli O.V., Abdullayeva F.D. Securing UAV Flight Data Using Lightweight Cryptography and Image Steganography // **International Journal of Advanced Computer Science and Applications (IJACSA). 2025,** vol. 16, no. 5, pp. 278-289.

The popularity of Unmanned Aerial Vehicles (UAVs) in various fields has been rising recently. UAV technology is being invested in by numerous industries in order to cut expenses and increase efficiency. Therefore, UAVs are predicted to become much more important in the future. As UAVs become more popular, the risk of cyberattacks on them is also growing. One type of cyberattack involves the exposure of important flight data. This, in turn, can lead to serious problems. To address this problem, a new method based on lightweight cryptography and steganography is proposed in this work. The proposed method ensures multilayer protection of important UAV flight data. This is achieved by two layers of encryption using a polyalphabetic substitution cipher and ChaCha20-Poly1305 authenticated encryption, as well as randomized least significant bit (LSB) steganography. Most importantly, through this work, a balance is kept between security and performance. Additionally, all experiments are carried out on real devices, making the proposed method more practical. The proposed method is evaluated using MSE, PSNR, and SSIM metrics. Even with a capacity of 8000 bytes, it achieves an MSE of 0.04, a PSNR of 62, and an SSIM of 0.9998. It is then compared to existing methods. The results show better practical use, stronger security, and higher overall performance.

483. Abdullayeva F.D., Valikhanli O.V. Multimodal deep neural network for UAV GPS jammingattack detection // **Cyber Security and Applications. 2025,** vol. 3, pp. 1-9.

Despite the progress in Unmanned Aerial Vehicles, various issues remain related to their cybersecurity. One of these issues is GPS jamming attacks. GPS jamming attacks can cause UAVs to lose control and crash. These crashes may result in injuries or fatalities. In this paper, we propose a novel multimodal UAV GPS jamming attack detection framework capable of recognizing attacks from visual and tabular data using deep convolutional neural networks and a multi-layer perceptron, respectively. The proposed multimodal model is capable of not only detecting the presence of jamming attacks but also identifying five different types of such attacks. As a result of the experiments conducted, high results were obtained compared to the existing methods. Thus, MLP was able to detect GPS jamming attacks with 96.25 % accuracy, CNN with 94.66 % accuracy, and the proposed multimodal deep learning (MLP+CNN) with 99 % accuracy.

484. Alakbarov R.K., Hashimov M.A. The role of artificial intelligence in ensuring the cybersecurity of SCADA systems // **International Journal of Artificial Intelligence and Applications. 2025,** no. 3, vol. 16, pp. 1-10.

One of the vital systems for the management of industrial infrastructure is SCADA (Supervisory Control and Data

Acquisition). They are extensively applied in different industrial processes, particularly or energy, water, and transportation networks. These systems are principally efficient and unfailing when united with Artificial Intelligence (AI) technologies. The application of AI technologies in traditional SCADA systems creates many new opportunities. These technologies provide more accurate monitoring of processes, more effective control, increased security, and optimization of operations. But, due to their integration with modern Information Technologies and the Internet, these systems are more and more unprotected from cyber threats. Outdated security procedures are often unsatisfactory against these attacks. AI has emerged as a promising solution to enhance SCADA cybersecurity through anomaly detection, automated threat response, and predictive risk assessment. This article explores the applications of AI-driven cybersecurity in SCADA systems, highlighting the benefits and future research directions. Integrating artificial intelligence into SCADA security is crucial to ensuring resilience, reliability, and protection against both known and emerging cyber threats.

485. Mehdiyev Ş.A. Enhancing the resilience of cyber-physical systems through energy-efficient communication in wireless sensor networks / **Journal of High-Frequency Communication Technologies. 2025,** no. 1, pp. 238-257.

This paper explores the multifaceted challenges of fault tolerance seen in cyber-physical systems (CPS), with particular emphasis on the critical role of wireless sensor networks (WSNs) in the collection and transmission of data essential for CPS operations. Special attention is given to the examination of the energy efficiency of WSNs and their influence on the overall fault tolerance of CPS. The study highlights the enhancement of node performance from energy efficient solutions and uptime with simultaneous introduction of new vulnerabilities to cyberattacks that compromise the resilience and security of WSNs. Key attack vectors, such as energy depletion and control packet manipulation, are identified and analyzed. The paper underscores the importance of establishing trust relationships between nodes and advocates for comprehensive protection strategies encompassing preventive, operational, and post incident measures. It emphasizes the "defense in depth" approach and discusses the concept of cyber immunity as a promising strategy for strengthening WSN cybersecurity. Future research directions include integration of artificial intelligence, leveraging of blockchain technologies, exploration of quantum computing applications, and development of proactive measures for mitigation of emerging cyber threats.

Redaktor: Mədinə Səidova

Texniki redaktorlar: Anar Səmidov

Könül Vəliyeva

Korrektor: Kəmalə Muradova

Kompüter tərtibatı: Nərgiz Abdullayeva

Xatirə Həbibova