ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ
МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РЕСПУБЛИКИ КАЗАХСТАН
MINISTRY OF SCIENCE AND HIGHER EDUCATION OF THE REPUBLIC OF KAZAKHSTAN

ХАЛЫҚАРАЛЫҚ УНИВЕРСИТЕТІ
МЕЖДУНАРОДНЫЙ УНИВЕРСИТЕТ
INTERNATIONAL UNIVERSITY

# ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ

# МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

# INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES

**2022 (3) 3**
*Маусым-қыркүйек*

**ISSN 2708–2032 (print)**
**ISSN 2708–2040 (online)**

---

**Халықаралық ақпараттық және коммуникациялық технологиялар журналы**
**ISSN 2708–2032 (print)**
**ISSN 2708–2040 (online)**
Меншіктенуші: «Халықаралық ақпараттық технологиялар университеті» АҚ (Алматы қ.).
Қазақстан Республикасы Ақпарат және әлеуметтік даму министрлігінің Ақпарат комитетінде – **20.02.2020** жылы берілген.
**№ KZ82VPY00020475** мерзімдік басылым тіркеуіне қойылу туралы куәлік.
Тақырыптық бағыты: ақпараттық технологиялар, әлеуметтік-экономикалық жүйелерді дамытудағы цифрлық технологиялар, ақпараттық қауіпсіздік және коммуникациялық технологияларға арналған.
Мерзімділігі: жылына 4 рет.
Тиражы: 100 дана
Редакцияның мекенжайы: 050040, Алматы қ-сы, Манас к-сі, 34/1, 709-кабинет, тел: +7 (727) 244-51-09).
E-mail: ijict@iitu.edu.kz Журнал сайты: https://journal.iitu.edu.kz

**Международный журнал информационных и коммуникационных технологий**
**ISSN 2708–2032 (print)**
**ISSN 2708–2040 (online)**
Собственник: АО «Международный университет информационных технологий» (г. Алматы).
Свидетельство о постановке на учет периодического печатного издания в Министерство информации и общественного развития Республики Казахстан **№ KZ82VPY00020475,** выданное от **20.02.2020 г.**
Тематическая направленность: информационные технологии, информационная безопасность и коммуникационные технологии, цифровые технологии в развитии социо-экономических систем**.**
Периодичность: 4 раза в год.
Тираж: 100 экземпляров.
Адрес редакции: 050040 г. Алматы, ул. Манаса 34/1, каб. 709, тел: +7 (727) 244-51-09).
E-mail: ijict@iitu.edu.kz Сайт журнала: https://journal.iitu.edu.kz

---

**«International Journal of Information and Communication Technologies»**
**ISSN 2708–2032 (print)**
**ISSN 2708–2040 (online)**
Owner: International Information Technology University JSC (Almaty).
The certificate of registration of a periodical printed publication in the Ministry of Information and Social Development of the Republic of Kazakhstan, Information Committee No. KZ82VPY00020475, issued on 20.02.2020.
Thematic focus: information technology, digital technologies in the development of socio-economic systems, information security and communication technologies
Periodicity: 4 times a year.
Circulation: 100 copies.
Editorial address: 050040. Manas st. 34/1, Almaty. +7 (727) 244-51-09). E-mail: ijict@iitu.edu.kz
Journal website: https://journal.iitu.edu.kz

**МАЗМҰНЫ**

**БАҒДАРЛАМАЛЫҚ ҚАМТАМАНЫ ӘЗІРЛЕУ ЖӘНЕ БІЛІМ ИНЖЕНЕРИЯСЫ**



**АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ЖЕЛІЛЕР ЖӘНЕ КИБЕРҚАУІПСІЗДІК**



**ЭКОНОМИКАДАҒЫ ЖӘНЕ МЕНЕДЖМЕНТТЕГІ ЦИФРЛЫҚ ТЕХНОЛОГИЯЛАР**



**БҰҚАРАЛЫҚ АҚПАРАТ ҚҰРАЛДАРЫНДАҒЫ ЦИФРЛЫҚ ТЕХНОЛОГИЯЛАР**

**СОДЕРЖАНИЕ**

## РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНЖЕНЕРИЯ ЗНАНИЙ



## ИНФОКОММУНИКАЦИОННЫЕ СЕТИ И КИБЕРБЕЗОПАСНОСТЬ



## ЦИФРОВЫЕ ТЕХНОЛОГИИ В ЭКОНОМИКЕ И МЕНЕДЖМЕНТЕ



## ЦИФРОВЫЕ ТЕХНОЛОГИИ В МАСС-МЕДИА

## CONTENTS

### SOFTWARE DEVELOPMENT AND KNOWLEDGE ENGINEERING



### INFORMATION AND COMMUNICATION NETWORKS AND CYBERSECURITY



### DIGITAL TECHNOLOGIES IN ECONOMICS AND MANAGEMENT



### DIGITAL TECHNOLOGIES IN THE MASS MEDIA

# АҚПАРАТТЫҚ КОММУНИКАЦИЯЛЫҚ ЖЕЛІЛЕР ЖӘНЕ КИБЕРҚАУІПСІЗДІК

# ИНФОКОММУНИКАЦИОННЫЕ СЕТИ И КИБЕРБЕЗОПАСНОСТЬ

# INFORMATION AND COMMUNICATION NETWORKS AND CYBERSECURITY

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Vol. 3. Is. 3. Number 11 (2022). Pp. 24–35
Journal homepage: https://journal.iitu.edu.kz
https://doi.org/*10.54309/IJICT.2022.11.3.003*
УДК 004.02:004.05:004.032.26

## OVERVIEW OF THE PRESENT STATE OF CYBER SECURITY

***O.D. Shapovalenko[1], D.I. Bedrii[2]****

**Shapovalenko Oleksandr —** postgraduate student, State University of Telecommunications
https://orcid.org/ORCID: 0000-0001-5937-6641;
**Bedrii Dmytro —** doctor of technical sciences, senior researcher, docent, deputy director for science, State Enterprise «Ukrainian Scientific Research Institute of Radio and Television», docent of the «Artificial Intelligence and Data Analysis» department, National University «Odesa Polytechnic»
https://orcid.org/ORCID: 0000-0002-5462-1588. E-mail: dimi7928@gmail.com.



**Abstract**. In today's conditions, information and communication security in society deserves more and more attention. This is due to the fact that information security incidents such as personal data theft, bank information leakage, ransomware, privacy violations, intellectual property theft, etc., have become common news in the daily life of not only enterprises, but any person. This study reviewed the current state of cybersecurity in information and communication technologies, in particular, computer networks. The challenges and threats in the field of cybersecurity, as well as the prerequisites and factors that form them, were also analyzed. This is especially true in connection with the growing role of cybersecurity in the processes of digital transformation of the state. One of the effective tools is the introduction of artificial intelligence technology in all spheres of life of the state and society. In modern conditions, the world is accelerating the introduction of technological solutions based on artificial intelligence in various areas of the economy, government and public relations. The practical use of artificial intelligence technology involves the processing of large amounts of data. Thus, we can talk about the relevance of further research on the introduction of artificial intelligence technology in the field of improving the security of computer networks.

**Keywords**: information technology, artificial intelligence, cyber defense, cybersecurity, information security

**For citation:** O.D. Shapovalenko, D.I. Bedrii. Overview of the present state of cyber security // INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES. 2022. Vol. 3. Is. 3. Number 11. Pp. 24–35 (In Russ.). DOI: *10.54309/IJICT.2022.11.3.003.*

# КИБЕРҚАУІПСІЗДІКТІҢ ҚАЗІРГІ ЖАҒДАЙЫНА ШОЛУ

***О.Д. Шаповаленко[1], Д.И. Бедрий[2]****

**Шаповаленко Александр Дмитриевич —** Мемлекеттік телекоммуникация университетінің аспиранты
https://orcid.org/ORCID: 0000-0001-5937-6641;
**Бедрий Дмитрий Иванович —** техника ғылымдарының докторы, аға ғылыми қызметкер, доцент, «Украинский научно-исследовательский институт радио и телевидения» мемлекеттік кәсіпорны директорының ғылыми жұмыстар жөніндегі орынбасары, «Одесская политехника» Ұлттық университетінің жасанды интеллект және деректерді талдау кафедрасының доценті
https://orcid.org/ORCID: 0000-0002-5462-1588. E-mail: dimi7928@gmail.com.



**Аннотация.** Қазіргі жағдайда қоғамдағы ақпараттық-коммуникациялық қауіпсіздік барған сайын назар аударуды қажет етеді. Себебі, жеке деректердің ұрлануы, банктік ақпараттың сыртқа шығуы, төлем бағдарламасы, жеке өмірге қол сұғылмаушылық, зияткерлік меншікті ұрлау және т.б. сияқты ақпараттық қауіпсіздік оқиғалары кәсіпорынның ғана емес, кез келген адамның күнделікті өмірінде жиі кездесетін жаңалыққа айналды. Бұл зерттеу ақпараттық-коммуникациялық технологиялардағы, атап айтқанда, компьютерлік желілердегі киберқауіпсіздіктің қазіргі жағдайына шолу жасайды. Сондай-ақ киберқауіпсіздік саласындағы сын-қатерлер, сондай-ақ оларды қалыптастыратын алғышарттар мен факторлар талданды. Бұл, әсіресе, мемлекеттің цифрлық трансформациясы үдерістерінде киберқауіпсіздік рөлінің өсуіне байланысты. Мемлекет пен қоғам өмірінің барлық саласына жасанды интеллект технологиясын енгізу тиімді құралдардың бірі болып табылады. Қазіргі жағдайда әлем экономиканың, мемлекеттік және қоғамдық қатынастардың әртүрлі салаларында жасанды интеллектке негізделген технологиялық шешімдерді енгізуді жеделдетуде. Жасанды интеллект технологиясын іс жүзінде қолдану деректердің үлкен көлемін өңдеуді қамтиды. Осылайша, компьютерлік желілердің қауіпсіздігін арттыру саласында жасанды интеллект технологиясын енгізу бойынша кейінгі зерттеулердің өзектілігі туралы айтуға болады.

**Түйін сөздер:** ақпараттық технологиялар, жасанды интеллект, киберқорғаныс, киберқауіпсіздік, ақпараттық қауіпсіздік

**Дәйексөз үшін:** О.Д. Шаповаленко, Д.И. Бедрий. Киберқауіпсіздіктің қазіргі

жағдайына шолу // ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ-КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ. 2022. Том. 3. Is. 3. Нөмірі 11. 24-35 бет (орыс тілінде). DOI: 10.54309/IJICT.2022.11.3.003.

# ОБЗОР СОВРЕМЕННОГО СОСТОЯНИЯ КИБЕРБЕЗОПАСНОСТИ

***О.Д. Шаповаленко[1], Д.И. Бедрий[2*]***

**Шаповаленко Александр Дмитриевич —** аспирант, Государственный университет телекоммуникаций, Киев, Украина
https://orcid.org/ORCID: 0000-0001-5937-6641;
**Бедрий Дмитрий Иванович —** д.т.н., старший исследователь, доцент, заместитель директора по научной работе, Государственное предприятие «Украинский научно-исследовательский институт радио и телевидения», доцент кафедры «Искусственный интеллект и анализ данных», Национальный университет «Одесская политехника», Одесса, Украина
https://orcid.org/ORCID: 0000-0002-5462-1588. E-mail: dimi7928@gmail.com.



**Аннотация.** В сегодняшних условиях все большего внимания заслуживает информационно-коммуникационная безопасность в обществе. Это связано с тем, что такие инциденты информационной безопасности, как: кража персональных данных, утечка банковской информации, программы-вымогатели, нарушение конфиденциальности, кража интеллектуальной собственности и др., стали обычными новостями в повседневной жизни не только предприятий, но любого человека. В данном исследовании был проведен обзор современного состояния кибербезопасности в информационно-коммуникационных технологиях, в частности и компьютерных сетях. Также были проанализированы вызовы и угрозы в сфере кибербезопасности, а также предпосылки и факторы их формирующие. Особенно это актуально в связи с ростом роли обеспечения кибербезопасности в процессах цифровой трансформации государства. Одним из эффективных инструментов является внедрение технологии искусственного интеллекта во всех сферах жизнедеятельности государства и общества. В современных условиях в мире происходит ускорение внедрения технологических решений, базирующихся на искусственном интеллекте в разных сферах экономики, управления государством и общественных отношений. Практическое использование технологии искусственного интеллекта предусматривает обработку больших массивов данных. Таким образом, можно говорить об актуальности дальнейших исследований внедрения технологии искусственного интеллекта в сфере повышения защищенности компьютерных сетей.

**Ключевые слова**: информационные технологии, искусственный интеллект, киберзащита, кибербезопасность, защита информации

**Для цитирования**: О.Д. Шаповаленко, Д.И. Бедрий. Обзор современного состояния кибербезопасности // МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ. 2022. Том. 3. Is. 3. Номер 11. Стр. 24–35 (на русском языке). DOI: 10.54309/IJICT.2022.11.3.003.

**Введение**

В сегодняшних условиях все большего внимания заслуживает информационно-коммуникационная безопасность в обществе. Это связано с тем, что такие инциденты информационной безопасности, как: кража персональных данных, утечка банковской информации, программы-вымогатели, нарушение конфиденциальности, кража интеллектуальной собственности и др., стали обычными новостями в повседневной жизни не только предприятий, но любого человека.

Внедрение во все сферы жизнедеятельности человека, общества и государства информационных технологий обусловило распространение больших массивов информации в вычислительных и информационных сетях на значительных территориях (https://zakon.rada.gov.ua/laws/show/1126-97-%D0%BF). В условиях отсутствия отечественных конкурентоспособных информационных технологий предоставляется преимущество техническим средствам обработки информации и средствам связи иностранного и совместного производства, которые в большинстве своем не обеспечивают защиту информации.

Коммуникационное оборудование иностранного производства, используемое на сетях связи, предусматривает дистанционный доступ к его аппаратным и программным средствам, в том числе и из-за рубежа, что создает условия для несанкционированного влияния на их функционирование и контроль за организацией связи и содержанием пересылаемых сообщений (Жилін, 2021).

В связи с этим, увеличилась потребность в решении задачи защиты информации, поскольку она является важнейшим стратегическим ресурсом, а также повышения защищенности компьютерных сетей.

Целью исследования является обзор современного состояния кибербезопасности в информационно-коммуникационных технологиях, в частности и компьютерных сетях.

**Основная часть**

Быстрые темпы развития в разных отраслях науки и техники привели к созданию компактных и высокоэффективных технических средств, при помощи которых можно легко подключаться не только к телекоммуникационному оборудованию и сетям связи, но и к компьютерным сетям, и к самим компьютерам. С целью добывания, пересылки и анализа любых данных, в частности персональных, банковских, корпоративных и пр. Для этого может использоваться аппаратура радио-, радиотехнической, оптико-электронной, радиотепловой, акустической, химической, магнитометрической, сейсмической и радиационной разведок [https://zakon.rada.gov.ua/laws/show/1126–97–%D0%BF, Жилін, 2021).

В работе (Трофименко, 2019) авторами выявлено, что в условиях стремительного роста кибератак важным является мониторинг современного состояния кибербезопасности Украины, определение основных проблем развертывания национальной системы киберзащиты и направлений их решения. При этом нужен как анализ уже реализованных мероприятий в сфере защиты компьютерных и телекоммуникационных сетей от кибератак, так и определение нужных для реализации мероприятий по созданию условий для безопасного функционирования

киберпространства. Проведенное исследование свидетельствует о существенных политических, экономических и социальных киберусилиях для усиления киберстойкости, прилагаемой государством с целью развития национальных возможностей по кибербезопасности. Авторы выяснили, что эффективное обеспечение киберзащиты требует комплексного решения и скоординированных действий на национальном, региональном и международном уровнях для предупреждения, подготовки, реагирования и возобновления инцидентов со стороны органов власти, частного сектора и гражданского общества. Также в исследовании определены политические, научно-технические, организационные и просветительские вопросы, решение которых является необходимым в рамках комплексного противостояния киберугрозам для опережающего реагирования на динамические изменения, происходящие в киберпространстве. Отмечена целесообразность прикладывания усилий для установления государственно-частного партнерства, разработка и внедрение механизма обмена информацией между государственными органами, частным сектором и гражданами в отношении угроз критической информационной инфраструктуре. Также указывается, что Украина должна активизировать свое участие в организации совместных международных проектов по наращиванию кибернетического потенциала с целью согласования действий и поиска новых путей в усилении кибербезопасности и защите критически важных информационных инфраструктур в ответ на новые тенденции в глобальном движении до цифровой экономики и информационного сообщества. Данное исследование может пригодиться в процессе разработки механизмов повышения защиты компьютерных сетей.

Авторами в работе (Потій, 2021) предложены концептуальные основы внедрения организационно-технической модели киберзащиты, а именно определены ее миссия, цель, назначение и главные цели, силы и средства киберзащиты. Авторы рассмотрели архитектуру организационно-технической модели киберзащиты, представляющей собой структурированную систему, состоящую из трех инфраструктур киберзащиты, в частности организационно-управляющей инфраструктуры киберзащиты, как совокупности субъектов обеспечения кибербезопасности, формирующих и/или реализующих государственную политику в сфере кибербезопасности; технологической инфраструктуры киберзащиты, как совокупности сил и средств киберзащиты, а также инфраструктуры, обеспечивающей функционирование сил киберзащиты, информационно-коммуникационных сетей и их ресурсов, используемых в интересах сил киберзащиты и базовой инфраструктуры киберзащиты, как совокупности объектов информационной инфраструктуры, коммуникационных и технологических систем предприятий, учреждений и организаций, граждан Украины и объединений граждан, других лиц, осуществляющих деятельность и/или предоставляют услуги, связанные с национальными информационными ресурсами, информационными электронными услугами, осуществлением электронных сделок, электронными коммуникациями, защитой информации и киберзащиты. Таким образом, внедрение организационно-технической

модели киберзащиты направлено на оперативное (кризисное) реагирования на кибератаки и киберинциденты, внедрения контрмер и минимизации уязвимости коммуникационных систем. Результаты этой работы могут лечь в основу моделей и методов повышения защищенности компьютерных сетей.

В работе (Жилін, 2021) отмечено, что в связи с развитием информационных технологий увеличилась потребность в защите информации. Также увеличивается уязвимость современного информационного общества к недостоверной информации, несвоевременному получению информации, промышленному шпионажу, компьютерной преступности и др. в этом случае скорость выявления угрозы, в контексте добычи системной информации о преступниках и возможных техник и инструментов реализации кибератак с целью их описания та оперативного реагирования на них является одной из актуальных задач. В частности, появляется задача в применении новых систем сбора информации о киберсобытии, реагирование на них, хранение и обмен этой информацией, а также на ее основе способов и средств поиска преступников при помощи комплексных систем, или платформ. Для решения задач такого типа авторами были проведены исследования перспективного направления Threat Intelligence как нового механизма получения знаний о кибератаках, проведен анализ индикаторов кибератак и инструментов их получения для определения его роли в задачах обеспечения киберзащиты. Авторы осуществили сравнение стандартов описания индикаторов компрометации и платформ их обработки. Разработана методика Threat Intelligence для задач оперативного выявления и блокировки киберугроз государственным информационным ресурсам, дающая возможность улучшить производительность работы аналитиков кибербезопасности и повышения защищенности ресурсов и информационных систем. Данное исследование можно использовать при разработке инструментов повышения защиты компьютерных сетей.

Еще одним направлением развития инструментов киберзащиты является применение искусственного интеллекта, который был рассмотрен авторами в работе (Ковтуненко, 2019), в частности были определены основные преимущества и проблемы его применения в системе управления предприятием. Были даны определения «искусственный интеллект» и показаны основные причины необходимости внедрения искусственного интеллекта в систему управления современного предприятия. Авторами выявлено, что одной из важнейших проблем этого внедрения является замена человеческого труда на автоматизированную работу машин, имеющая негативные последствия в условиях высокого уровня безработицы при отсутствии постоянного использования искусственного интеллекта. Также отмечено, что неотъемлемой частью внедрения новых систем компьютерного управления предприятием является четкое понимание последствий, которые оно вызывает. Использование искусственного интеллекта позволяет избежать человеческого фактора, в частности ошибок, связанных с невнимательностью, недостаточным уровнем квалификации, или негативным физическим или психологическим

состоянием. Поэтому в развитых странах мира проводится внедрение новых систем з компьютерным управлением предприятиями. Результаты этой работы пригодятся в процессе разработки механизмов повышения защищенности компьютерных сетей.

В работе (Шаповаленко, 2022) авторами отмечено, что в последнее время возник большой интерес к применению анализа данных для обнаружения вторжений в компьютерную сеть. В исследовании авторы рассмотрели методы интеллектуального анализа данных в системах обнаружения вторжений, а также типы необходимого опыта и инфраструктуры. В результате проведения экспериментальных исследований авторы предложили модель системы обнаружения вторжений на основе методов машинного обучения. Представленная модель может служить эффективным дополнением к стандартным IDS для улучшения системы безопасности сети.

Основные принципы реализации политики субъектами обеспечения кибербезопасности представлены на рис. 1 (*Урядовий кур'єр*, 2017).

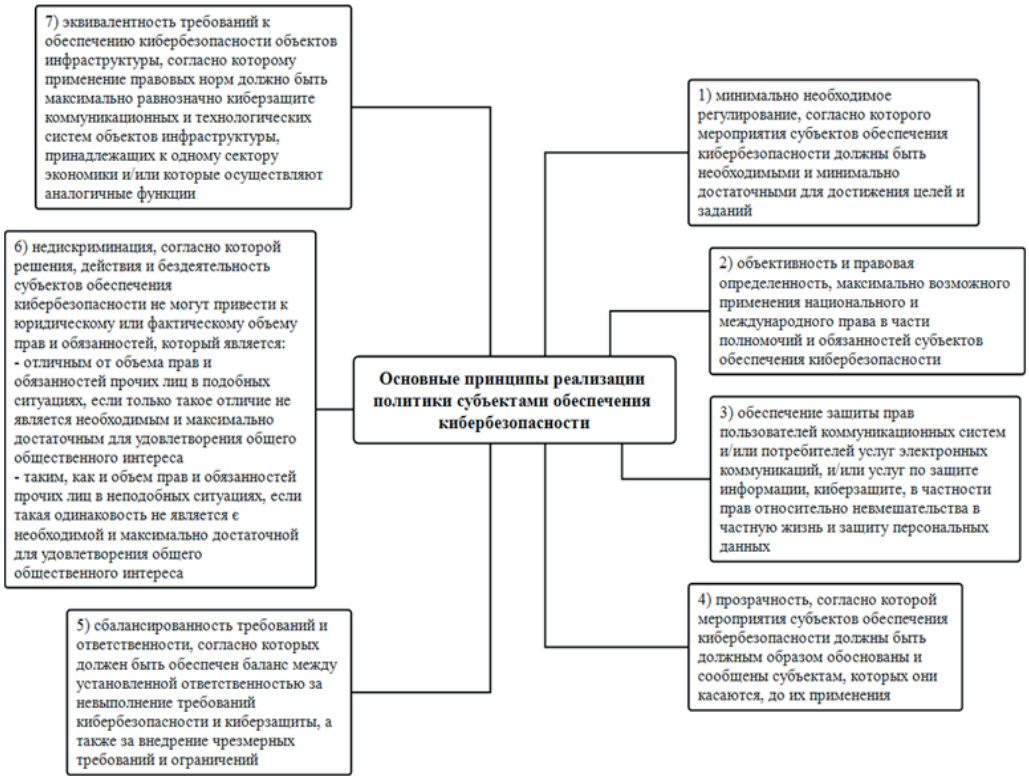


Рисунок 1. Основные принципы реализации политики субъектами обеспечения кибербезопасности

Указанные на рис. 1 принципы применяются без отдачи преимущества любому из них с учетом обеспечения защиты жизненно важных интересов человека

и гражданина, общества и государства, национальных интересов страны в киберпространстве.

Вызовы и угрозы в сфере кибербезопасности представлены в табл. 1 ("Про Стратегію кібербезпеки України": Указ Президента України від 26.08.2021 № 447/2021).

Таблица 1 – Вызовы и угрозы в сфере кибербезопасности

| Кибербезопасность | Вызовы и угрозы |
|---|---|
| 1 | 2 |
| Вызовы | 1) активное использование киберсредств в международной конкуренции |
| | 2) соревновательный характер развития средств кибербезопасности в условиях быстро прогрессирующих изменений информационно-коммуникационных технологий, в частности облачных и квантовых вычислений, 5G-сетей, больших объемов данных, Интернета вещей, искусственного интеллекта, др. |
| | 3) милитаризация киберпространства и развитие кибероружия, дающего скрытно проводить кибератаки для поддержки боевых действий и разведывательно-подрывной деятельности в киберпространстве |
| | 4) влияние пандемии COVID-19 на экономическую деятельность и социальное поведение, приведшее к стремительной трансформации и организации значительного сегмента общественных отношений в дистанционном режиме с широким применением и электронных сервисов и информационно-коммуникационных систем |
| | 5) внедрение новых технологий, цифровых услуг и механизмов электронного взаимодействия граждан с государством, которое осуществляется бессистемно в части мероприятий по кибербезопасности и без надлежащей оценки рисков |
| Угрозы | 6) гибридная агрессия в киберпространстве. Страна-агрессор неумолимо наращивает арсенал кибероружия наступательного назначения, применение которого может вызвать непоправимые, необратимые разрушительные последствия. Кибератаки направлены в первую очередь на информационно-коммуникационные системы органов власти и объекты информационной инфраструктуры с целью выведения их из строя (кибердиверсия), получения скрытого доступа и контроля, осуществления разведывательной и разведывательно-подрывной деятельности. Также кибератаки активно используются для проведения специальных информационных операций з целью манипулятивного влияния на население |
| | 7) киберпреступность, наносящая вред информационным ресурсам, общественным процессам, лично гражданам, снижает доверие общества к информационным технологиям и приводит к значительным материальным потерям. Также киберпространство используется для совершения преступлений против национальной безопасности страны, а также криминальных правонарушений, связанных с легализацией доходов, полученных незаконным путем, торговлей людьми, незаконным обращением с оружием, боевыми принадлежностями и взрывчатыми веществами, незаконным обращением наркотических средств, психотропных веществ, их аналогов или прекурсоров и прочих предметов и веществ, угрожающих жизни и здоровью людей |

| | |
|---|---|
| | 8) организованные и спонсируемые другими странами кибератаки, связанные с хищением в политических, экономических или военных целях конфиденциальной информации (кибершпионаж) и осуществлением разведывательно-подрывной деятельности. Особенностями таких кибератак является их продолжительность, сложность и скрытый характер, усложняющие их предупреждение, выявление и нейтрализацию |
| | 9) использование террористическими организациями киберпространства для совершения актов кибертерроризма, финансовой и прочей поддержки террористической деятельности |

Учитывая вызовы и угрозы в сфере киберпространстве, представленные в табл. 2, критично растет роль кибербезопасности в процессах цифровой трансформации государства.

Предпосылки и факторы, формирующие обозначенные угрозы:

- высокая технологическая зависимость от иностранных производителей продукции информационно-коммуникационных технологий, отсутствие системы оценки соответствия такой продукции требованиям безопасности, повышающей степень уязвимости информационной инфраструктуры от незадекларированных функций, и сужает возможности противодействия киберугрозам;
- несовершенство нормативно-правовой базы в сфере кибербезопасности, а также ее устаревание в сфере защиты информации, медленная имплементация положений европейского законодательства, недостаточное регулирование цифровой составляющей расследования уголовных правонарушений, а также низкий уровень правовой ответственности за нарушение требований законодательства в этой сфере;
- отсутствие у большей части органов власти и субъектов хозяйствования необходимого кадрового обеспечения и надлежащего контроля за киберзащитой, осуществление финансирования работ по киберзащите по остаточному принципу;
- отсутствие системы независимого аудита информационной безопасности и механизмов раскрытия информации об уязвимости в условиях динамической цифровизации всех сфер государственного управления и жизнедеятельности государства;
- несоответствие современным требованиям уровня подготовки и повышения квалификации специалистов по вопросам кибербезопасности и киберзащиты, в частности неэффективные механизмы их стимулирования к работе в государственном секторе;
- незавершенность мероприятий по внедрению организационно-технической модели киберзащиты, отвечающей современным угрозам, вызовам в киберпространстве и глобальным тенденциям развития индустрии кибербезопасности;
- отсутствие системы повышения цифровой грамотности граждан и культуры безопасного поведения в киберпространстве, низкий уровень информирования общество о киберугрозах и киберзащите;
- отсутствие действующей системы информационно-аналитического обеспечения кибербезопасности;

- недостаточная защищенность от кибератак информационных ресурсов и объектов информационной инфраструктуры;

- несоответствие требованиям законодательства состояние защиты информационно-коммуникационных систем государственных органов и субъектов хозяйствования, в которых обрабатывается значительная часть информации с ограниченным доступом.

Учитывая вызовы и угрозы в сфере кибербезопасности, а также предпосылки и факторы их формирующие, можно прийти к выводу, что есть необходимость обеспечения обработки больших массивов информации. Это связано с ростом информатизации общества и государства, что в свою очередь требует повышения уровня защищенности компьютерных сетей. Достаточно эффективным инструментом в этом случае выступает технология искусственного интеллекта во всех сферах жизнедеятельности государства и общества.

Искусственный интеллект — это наука и технология, способная воссоздать процессы мышления человеческого мозга и направить их на создание и обработку различных программ, а также интеллектуальных машин, способных полностью заменить и упростить человеческую работу (Кизим, 2012; https://www.everest.ua/ai-platform/analytics/shtuchnik-intelekt-efektivna-ta-odnochasno-nebezpechna-tehnologiya-chi-usvidomljujut-suspilstvo-ta-biznes-riziki-ta-perevagi-ai).

Искусственный интеллект — организованная совокупность информационных технологий, с применением которой можно выполнять сложные комплексные задания путем использования системы научных методов исследования и алгоритмов обработки информации, полученной или созданной во время работы, а также создавать и использовать собственные базы знаний, модели принятия решений, алгоритмы работы с информацией и определять способы достижения поставленных заданий (Розпорядження Кабінету Міністрів України; Концепція від 02.12.2020 № 1556).

Основным заданием в сфере кибербезопасности при внедрении технологии искусственного интеллекта является защита коммуникационных, информационных и технологических систем, информационных технологий, прежде всего тех, которые используются поставщиками услуг и являются важными для непрерывности функционирования государства, общества и безопасности граждан.

Применение технологии искусственного интеллекта в обеспечении информационной безопасности является одним из факторов, способствующий обеспечению национальных интересов. В частности, мониторинг социальных сетей и интернет-ресурсов, электронных медиа с использованием технологий искусственного интеллекта дает возможность выявлять системные тренды и проблематику, действовать на опережение, анализировать целевую аудиторию.

Таким образом, широкое использование технологии искусственного интеллекта дает возможность стандартизовать представление и распространение информации о современных знаниях с возможностью их дальнейшей реализации

в зависимости от конкретных требований участников сферы информационно-коммуникационных технологий.

**Заключение**

В результате исследования был проведен обзор современного состояния кибербезопасности в информационно-коммуникационных технологиях, в частности и компьютерных сетях. Также были проанализированы вызовы и угрозы в сфере кибербезопасности, а также предпосылки и факторы их формирующие. Особенно это актуально в связи с ростом роли обеспечения кибербезопасности в процессах цифровой трансформации государства.

Одним из эффективных инструментов является внедрение технологии искусственного интеллекта во всех сферах жизнедеятельности государства и общества. В современных условиях в мире происходит ускорение внедрения технологических решений, базирующихся на искусственном интеллекте в разных сферах экономики, управления государством и общественных отношений. Практическое использование технологии искусственного интеллекта предусматривает обработку больших массивов данных. Таким образом, можно говорить об актуальности дальнейших исследований внедрения технологии искусственного интеллекта в сфере повышения защищенности компьютерных сетей.

**ЛИТЕРАТУРЫ**

Жилін А., Ніколаєнко Б., Бакалинський О. (2021). Підвищення захищеності державних інформаційних ресурсів за рахунок застосування платформи Threat Intelligence. *Захист інформації*. — 2021. — Том 23. — № 3. — С. 136–146. DOI: 10.18372/2410-7840.23.16401.

Ковтуненко Ю.В. (2019). Застосування штучного інтелекту у системі управління підприємством: проблеми та переваги. *Економічний журнал Одеського політехнічного університету*. — 2019. — № 2(8). — С. 93–99. DOI: 10.5281/zenodo.4171114.

Потій О., Семенченко А., Дубов Д., Бакалинський О., Мялковський Д. (2021). Концептуальні засади впровадження організаційно-технічної моделі кіберзахисту України. *Захист інформації*. — 2021. — Том 23. — №1. — С. 47-59. DOI: 10.18372/2410-7840.23.15434.

Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. *Урядовий кур'єр*, —№ 215, — 2017.

Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" : Указ Президента України від 26.08.2021 № 447/2021. *Урядовий кур'єр*. — 28.08.2021. — № 165.

Кизим М.О. (2012). Перспективи розвитку інформаційно-комунікаційних технологій і штучного інтелекту в економіках країн світу та України : монографія / Кизим М.О., Матюшенко І.Ю., Шостак І.В. – Х. : — ВД «Інжек». — 2012. — 492 с.

Про схвалення Концепції розвитку штучного інтелекту в Україні : Розпорядження Кабінету Міністрів України; Концепція від 02.12.2020 № 1556-р. *Урядовий кур'єр*. 18.12.2020. — № 247.

Про затвердження Концепції технічного захисту інформації в Україні : Постанова Кабінету Міністрів України від 08.10.1997 № 1126. 1997. [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/1126-97-%D0%BF. (дата звернення: 16.06.2022).

Штучний інтелект — ефективна та одночасно небезпечна технологія. Чи усвідомлюють суспільство та бізнес ризики та переваги AI? — [Електронний ресурс]. – Режим доступу: https://www.everest.ua/ai-platform/analytics/shtuchnik-intelekt-efektivna-ta-odnochasno-nebezpechna-tehnologiya-chi-usvidomljujut-suspilstvo-ta-biznes-riziki-ta-perevagi-ai/.

Трофименко О., Прокоп Ю., Логінова Н., Задерейко О. (2019). Кібербезпека України:

аналіз сучасного стану. *Захист інформації*. — 2019. — Том 21. — № 3. — С. 150–157. DOI: 10.18372/24107840/21/13951.

Шаповаленко О.Д., Кліменкова Н.А. (2022). Застосування інтелектуального аналізу даних для виявлення мережевого вторгнення. *Інформаційні технології в освіті, науці і техніці (ІТОНТ-2022).* Тези доповідей VI Міжнародної науково-практичної конференції 23–25 червня 2022 року. Черкаси, — 2022. — С. 79–80.

**REFERENCES**

Artificial intelligence is an efficient and dangerous technology. Are society and business aware of the risks and benefits of AI? Available at: https://www.everest.ua/ai-platform/analytics/shtuchnik-intelekt-efektivna-ta-odnochasno-nebezpechna-tehnologiya-chi-usvidomljujut-suspilstvo-ta-biznes-riziki-ta-perevagi-ai/ [in Ukrainian].

Human Activity Recognition Using Tools of Convolutional Neural Networks: A State of the Art Review, Data Sets, Challenges and Future Prospects. 2022. [Electronic resource] URL: https://arxiv.org/abs/2202.03274. (accessed: 20.06.2022).

Zhilin A., Nikolayenko B., Bakalynskyi O. (2021). Increasing the security of state information resources due to the use of the Threat Intelligence platform. *Protection of information*. — 2021. — Volume 23. — No. 3. — Pp. 136–146. DOI: 10.18372/2410-7840.23.16401. [in Ukrainian].

Potii O., Semenchenko A., Dubov D., Bakalinskyi O., Myalkovskyi D. (2021). Conceptual principles of implementation of organizational and technical model of cyber protection of Ukraine. *Protection of information*. — 2021. — Volume 23. — No. 1. — Pp. 47–59. DOI: 10.18372/2410-7840.23.15434. [in Ukrainian].

Kovtunenko Yu.V. (2019). Application of artificial intelligence in enterprise management system: problems and advantages. *Economic journal Odessa polytechnic university*. — 2019. — No. 2(8). — Pp. 93–99. DOI: 10.5281/zenodo.4171114. [in Ukrainian].

Kyzym M.O., Matiushenko I.Yu. & Shostak I.V. (2012). Prospects for the development of information and communication technologies and artificial intelligence in the economies of the countries of the world and Ukraine. KHARKIV: Inzhek, — 2012. [in Ukrainian].

Shapovalenko O.D., Klimenkova N.A. (2022). Application of intelligent data analysis to detect network intrusion. Information technologies in education, science and technology (ITONT-2022). Abstracts of reports of the VI International Scientific and Practical Conference on June 23–25, — 2022. — Cherkasy, 2022. — Pp. 79–80. [in Ukrainian].

On the main principles of ensuring cyber security of Ukraine: Law of Ukraine dated October 5, — 2017. — No. 2163-VIII. Government Courier, No. 215, 2017. [in Ukrainian].

On the decision of the National Security and Defense Council of Ukraine dated May 14, 2021 "On the Cybersecurity Strategy of Ukraine": Decree of the President of Ukraine dated August 26. — 2021. — No. 447/2021. Government courier. 08/28/2021. No. 165. [in Ukrainian].

On the approval of the Concept of the development of artificial intelligence in Ukraine: Order of the Cabinet of Ministers of Ukraine; Concept No. 1556 dated 02.12.2020. Government courier. — 18.12.2020. — No. 247. [in Ukrainian]. DOI: 10.54309/IJICT.2023.11.3.004

Trofymenko O., Prokop Yu., Loginova N., Zadereyko O. (2019). Cybersecurity of Ukraine: analysis of the current state. *Protection of information*. — 2019. — Volume 21. — No. 3. — Pp. 150–157. DOI: 10.18372/24107840/21/13951. [in Ukrainian].

# ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ

# МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

# INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES

Правила оформления статьи для публикации в журнале на сайте:
https://journal.iitu.edu.kz
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Собственник: АО «Международный университет информационных технологий» (Казахстан, Алматы)



Подписано в печать 15.09.2022.
Формат 60x881/8. Бумага офсетная. Печать - ризограф.7,0 п.л. Тираж 100
050040 г. Алматы, ул. Манаса 34/1, каб. 709, тел: +7 (727) 244-51-09.

Издание Международного университета информационных технологий
Издательский центр КБТУ, Алматы, ул. Толе би, 59