АВТОРЫ СТАТЬИ

ВОРОНКОВА ВАЛЕНТИНА
НИКИТЕНКО ВИТАЛИНА
РЕГИНА АНДРЮКАЙТЕНЕ
РОМАН ОЛЕКСЕНКО
НАТАЛЬЯ КАПИТАНЕНКО

КИБЕРПРЕСТУПНОСТЬ

КАК НОВЕЙШЕЕ ЯВЛЕНИЕ ИНФОРМАЦИОННО-КОММУНИКАЦИОННОГО ОБЩЕСТВА И ПУТИ ЕЕ ПРЕДУПРЕЖДЕНИЯ

Доктор философских наук, профессор, Академик академии наук высшего образования Украины, заведующая кафедрой менеджмента организаций и управления проектами, Инженерный учебно-научный институт Запорожского национального университета (Запорожье, Украина) / Doctor of Philosophy (D.Sc.), Professor, Academician of the Academy of Higher Education of Ukraine, Head of the Department of Management of Organizations and Project Management, Engineering educational and scientific Institute of Zaporizhzhia National University (Zaporizhzhia, Ukraine)

- *E-mail: valentinavoronkova236@gmail.com*
- *ORCID: http://orcid.org/ 0000-0002-0719-1546*
- *Инженерный учебно-научный институт, Запорожский национальный университет, пр.Соборный, 226, 69006 Запорожье, Украина*
- *Engineering educational and scientific Institute of Zaporizhzhia*
- *National University, 226 Soborny Avenue, 69006 Zaporizhzhia, Ukraine*

D.Sc. Валентина Воронкова

НИКИТЕНКО ВИТАЛИНА / NIKITENKO VITALINA

кандидат философских наук, доцент, доцент кафедры менеджмента организаций и управления проектами, Инженерный учебно-научный институт Запорожского национального университета (Запорожье, Украина) / PhD in Philosophy, Associate Professor, Associate Professor of the Department of Management of Organizations and Project Management, Engineering educational and scientific Institute of Zaporizhzhia National University (Zaporizhzhia, Ukraine)

E-mail: vitalina2006@ukr.net
ORCID: https://orcid.org/0000-0001-9588-7836
Инженерный учебно-научный институт, Запорожский национальный университет, пр.Соборный, 226, 69006 Запорожье, Украина
Engineering educational and scientific Institute of Zaporizhzhia
National University, 226 Soborny Avenue, 69006 Zaporizhzhia, Ukraine

КАПИТАНЕНКО НАТАЛЬЯ / KAPITANENKO NATALIIA

кандидат юридических наук, доцент, доцент кафедры менеджмента организаций и управления проектами, Инженерный учебно-научный институт Запорожского национального университета (Запорожье, Украина) / PhD in Law, Associate Professor, Associate Professor of the Department of Management of Organizations and Project Management, Engineering educational and scientific Institute of Zaporizhzhia National University (Zaporizhzhia, Ukraine)

E-mail: kapitanenko.np @gmail.com
ORCID: https://orcid.org/0000-0002-1475-5784
Инженерный учебно-научный институт, Запорожский национальный университет, пр.Соборный, 226, 69006 Запорожье, Украина
Engineering educational and scientific Institute of Zaporizhzhia
National University, 226 Soborny Avenue, 69006 Zaporizhzhia, Ukraine

РЕГИНА АНДРЮКАЙТЕНЕ / ANDRIUKAITIENE, REGINA

доктор PhD социальных наук (менеджмент), доцент, зав. кафедрой бизнеса и экономики, Мариямпольский университет прикладных наук (Маряямполь, Литва), лектор Литовского университета спорта (Каунас, Литва) / Doctor PhD of social sciences, Head of the Department of Business and Economics, Associate Professor, Marijampole University of Applied Sciences (Marijampole, Lithuania), lect. of Lithuanian Sports University (Kaunas, Lithuania)

E-mail: regina.andriukaitiene@gmail.com
ORCID: https://orcid.org/0000-0002-0691-7333
Мариямпольский университет прикладных наук, ул. П. Армино 92, LT-68125, Маряямполе, Литва
Marijampole University of Applied Sciences, str. P. Armino 92, LT-68125, Marijampole, Lithuania

ОЛЕКСЕНКО РОМАН / OLEKSENKO ROMAN

доктор философских наук, профессор, профессор кафедры публичного управления и права, Таврический государственный агротехнологический университет имени Дмитрия Моторного (Мелитополь, Украина) / Doctor of Philosophy, Professor, Professor of Department Public Administration and Law, Dmytro Motornyi Tavria state agrotechnological University (Melitopol, Ukraine)

E-mail: roman.xdsl@ukr.net
ORCID: https://orcid.org/ 0000-0002-2171-514X
Таврический государственный агротехнологический университет имени Дмитрия Моторного, пр. Хмельницкого 18, 72312 Мелитополь Украина Запорожская область
Dmytro Motornyi Tavria State Agrotechnological University, Hetmanskaya str., 18, 72312 Melitopol, Ukraine Zaporizhzhia region

АННОТАЦИЯ

В статье представлен анализ киберпреступности как новейшего явления информационного общества, вызванного технологическим прорывом Четвертой промышленной революции, принёсшей риски и вызовы всему человечеству. Цель исследования – теоретический анализ достаточно сложного и опасного феномена киберпреступности, появление которого вызвано динамическим процессом преступного использования прорывных технологий в корыстных целях преступников с целью обогащения и незаконного использования.

Киберпреступники постоянно обновляют технические приемы и средства, чтобы применять самые последние технологии в своей незаконной деятельности. Сегодня преступники создают свои тайные радиотелекоммуникационные системы мобильной связи во всех странах и демонстрируют самый высокий уровень технической подготовки с целью их усовершенствования и, при этом, опережают защитников правопорядка. Сегодня киберпреступники упражняются во взломах стомиллионных счетов и в этом деле они продвинулись далеко вперед. Поэтому сегодня необходимо осознать угрожающие масштабы как организованной киберпреступности, так и террористических организаций, перед которыми правительства оказались неподвластными, так как они оборачиваются против людей. Борьба с киберпреступностью в информационном пространстве выступает как объект исследования.

Предмет исследования – пути преодоления вызовов и угроз, распространяемых в киберпространстве. **ЦЕЛИ ИССЛЕДОВАНИЯ:** 1) проанализировать проблемы управления цифровыми рисками в условиях коронавирусного кризиса; 2) определить риски и потенциал злоупотреблений цифровой идентичностью; 3) показать развитие транснациональной организованной киберпреступности как огромного бизнеса; 4) раскрыть условия расцвета организованной киберпреступности и пути ее пресечения.

МЕТОДОЛОГИЯ ИССЛЕДОВАНИЯ: метод анализа и синтеза эксплицируется как элементарно-составные части или компоненты общей системы киберпреступности, объединённые в результате анализа компонентов, предметов, объектов киберпреступлений, которые проявляются в реальной информационной среде. В процессе анализа исследуемой темы нам удалось получить достоверное знание о процессах исследуемой действительности киберпреступности, опираясь на аналитико-синтетические методы и приемы. Аналитика помогла привести в систему все разрозненные факты, умозаключения и аргументации для получения истинно-достоверного знания. Большую роль сыграл метод сравнения, который предоставил возможность познать объект исследования с тех диспозиций, которые позволили его отличить от других объектов или предметов, показать сходство с родственными ему предметами и моделями, дискурсрезюмировать сущность и направление киберпреступлений, определить их свойства и характеристики. Благодаря использованным методам и подходам удалось сформулировать научно-концептуальное знание борьбы с киберпреступностью в информационном пространстве, заложенных в них эпистемологических научных знаний и отношения между объектами-предметами исследуемой сферы.

Авторы предлагают выработать конкретные практические рекомендации, которые помогут контролировать и предупреждать киберпреступления в будущем, для этого авторы предлагают заглянуть вглубь обратной стороны технологических инноваций и проанализировать последствия, которыми они угрожают взаимозависимому и крайне уязвимому миру, в который втянуто все человечество.

К Л Ю Ч Е В Ы Е СЛОВА: киберпреступления, информационные технологии, информационное пространство, сложные системы, риски и угрозы

CYBERCRIME AS THE NEWEST PHENOMENON OF INFORMATION AND COMMUNICATION SOCIETY AND THE MEANS OF ITS PREVENTION

ABSTRACT

The purpose of the research is to analyze cybercrime as the most recent phenomenon of the information society, induced by the technological breakthrough of the Fourth Industrial Revolution, which brought risks and challenges to all mankind. Objective of the study is the theoretical analysis of a rather complex and dangerous phenomenon of cybercrime, the occurrence of which is caused by a dynamic process of criminal use of disruptive technologies in selfish purposes of criminals for the enrichment and unlawful use.

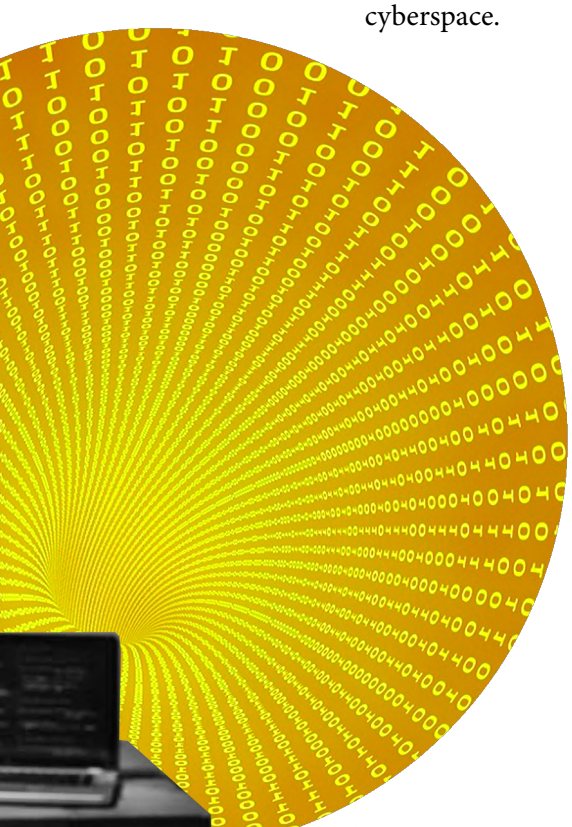
Cybercriminals are regularly updating techniques and tools to apply the latest technology to their illegal activities. Today, criminals are developing their clandestine mobile radio telecommunications systems in all countries and are demonstrating the highest level of technical expertise to improve them and in doing so outperform the defenders of law and order. Nowadays cybercriminals are practicing hacking into hundreds of millions of dollars' worth of accounts, and they are far ahead of the curve. Thus, today we must realize the threatening scale of both organized cybercrime and terrorist organizations, to which governments have fallen out of favor as they turn on the people. The control of cybercrime in the information space acts as an object of research. The subject of the study includes ways to overcome the challenges and threats spread in cyberspace.

THE OBJECTIVES OF THE STUDY ARE: 1) to analyze the problems of digital risk management in the context of the coronavirus crisis; 2) to identify the risks and potential of digital identity abuse; 3) to show the development of transnational organized cybercrime as a huge business; 4) to reveal the conditions of organized cybercrime flourishing and ways to curb it.

METHODOLOGY OF RESEARCH: Analysis and synthesis method is exemplified as elementary parts or components of the overall system of cybercrime, united as a result of the analysis of components, subjects, objects of cybercrime, which manifest themselves in the real information environment. In the course of reviewing the research topic, we managed to acquire reliable knowledge regarding the processes of the reality of cybercrime under study, relying on analytical-synthetic methods and techniques. Analytics contributed to the system of all the disparate facts, inferences and arguments to obtain true and reliable knowledge. A great role is made of comparison method, allowing to cognize the object of research from those dispositions to distinguish it from other objects or subjects, to reveal similarity with related objects and models, to discourse the essence and direction of cybercrimes, to determine properties and characteristics of cybercrimes. Owing to the applied methods and approaches it was a success to formulate scientific-conceptual knowledge of combating cybercrime in the information space, epistemological scientific knowledge embedded therein and relations between objects-subjects of the investigated sphere.

The authors suggest developing specific practical recommendations to help control and prevent cybercrime in the future. For this purpose, we recommend to peer deep into the reverse side of technological innovations and analyze the consequences that they threaten the interdependent and highly vulnerable world in which all mankind is involved.

KEYWORDS: cybercrime, information technology, information space, complex systems, risks and threats



ВВЕДЕНИЕ

Актуальность исследования

Актуальность темы исследования заключается в том, что мы живем во взаимосвязанном мире, в котором все люди так или иначе уязвимы в силу того, что киберпреступность захлестнула информационное пространство. Киберпреступники разработали целый арсенал методов и приёмов для получения прибыли, отдав предпочтение цифровым данным, которые контролируются мошенниками, в результате чего возникла общая угроза достоверности информации и ее потери, которая накапливается во время «революции больших данных». Взаимосвязанность и повсеместность уязвимых по своей сути компьютерных систем свидетельствует о том, что ураган технологической надвигающейся опасности больше нельзя игнорировать. Безусловно, проблема заключается не в том, что технологии — это сплошное зло, а в том, что следует осмысливать ее уязвимые места. В результате этого весь спектр критически важных информационных инфраструктур, поддерживающих жизнедеятельность общества, находится под угрозой, не говоря уже о рисках от искусственного интеллекта и синтетической биологии. Вне всякого сомнения, наука и технологии, прорывные технологии выступают как положительные для всего человечества, однако, чтобы уверенно процветать в текущем веке, нам придется выдержать испытания технологическими рисками, которые неизбежно создают прогресс, порождают потребность в защите киберпространства, что является актуальной как никогда темой в контексте развития современной цивилизации [1].

ЗАДАЧИ ИССЛЕДОВАНИЯ:

1. проанализировать проблемы управления цифровыми рисками в условиях коронавирусного кризиса;
2. определить риски и потенциал злоупотреблений цифровой идентичностью;
3. показать развитие транснациональной организованной киберпреступности как огромного бизнеса;
4. раскрыть условия расцвета организованной киберпреступности и пути ее пресечения.

МЕТОДОЛОГИЯ ИССЛЕДОВАНИЯ

Для нас большую роль играет системный метод и подход, в основе которого лежит рассмотрение явлений и процессов киберпреступлений как функционально-целостных и процессуально-генезисных мультисистем, рассматриваемых как целостные единицы. В основе целостности лежит анализ функций, механизмов, связей, процессов, которые интегрированы в единую систему киберпространства в зависимости от задач, целей, программы. Каждый элемент субсистемы кибепреступности можно классифицировать как отдельный элемент общей системы взаимосвязанного и целостного мира, проявляемого в их мультипроцессах и когеренциях. Метод анализа и синтеза эксплицируется как элементарно-составные части или компоненты общей системы, объединённые в результате анализа компонентов, предметов, объектов киберпреступлений, которые проявляются в реальной информационной среде в условиях глобализации [2]. В процессе анализа исследуемой темы нам удалось получить достоверное знание о процессах исследуемой действительности, опираясь на аналитико-синтетические методы и приемы. Аналитика помогла привести в систему все разрозненные факты, умозаключения и аргументации для получения истинно-достоверного знания. Большую роль сыграл метод сравнения, который предоставил возможность познать объект исследования с тех диспозиций, которые позволили его отличить от других объектов или предметов, показать сходство с родственными ему предметами и моделями, дискурсрезюмировать

их сущность и направление, определить свойства и характеристики исследуемого объекта информационного общества. Благодаря использованным методам и подходам удалось сформулировать научно-концептуальное знание борьбы с киберпреступностью в информационном пространстве, заложенных в них эпистемологических научных знаний и отношения между объектами-предметами исследуемой сферы. «*Научная возможность ученого заключается в том, что он берет на себя ответственность за исследование абстрактной категории (явление, феномен, проблема и пр.) и, проходя стадию за стадией, превращает ее в прикладную категорию*», - отмечает О. Мальцев [7, с. 64-70].

ИССЛЕДОВАНИЕ

1 ПРОБЛЕМЫ УПРАВЛЕНИЯ ЦИФРОВЫМИ РИСКАМИ В УСЛОВИЯХ КОРОНАВИРУСНОГО КРИЗИСА

Как свидетельствует анализ, пандемия COVID-19, с одной стороны, кардинально ускорила цифровую трансформацию во всемирном масштабе, по некоторым оценкам - на пять и даже больше лет [4]. С другой стороны, она привела к тому, что с такой же скоростью возрастают и цифровые риски. Компании сегодня более подвержены онлайн-угрозам из-за участившихся контактов, в результате чего появляется все большее количество проблем, к которым относится конфиденциальность данных, общественное здравоохранение. В связи с увеличивающимися атаками хакеров, возрастают страхи и тревоги людей, вовлечение людей в фишинговые операции, через обман загружаются вредоносные программы. Еще большую озабоченность в разгар пандемии вызывают угрозы кибератак на больницы с требованием выкупа и краж интеллектуальной собственности у производителей вакцин. Все это не ново: **степень осведомленности о киберрисках возросла и до пандемии.** Геополитическая напряженность и новые возможности для кибератак вызвали новые программы государств, негосударственных деятелей, стирая различия между шпионами и злонамеренными хакерами. Всемирный экономический форум признал эту угрозу еще в 2019 году, поставив кибербезопасность в число самых опасных рисков современности рядом с изменениями климата. Однако, масштабы и ландшафт угроз быстро меняются. Для стран, стремящихся воспользоваться выгодами цифровой трансформации, киберпреступность - только один из многих цифровых рисков [4]. Роль технологий в распространении дезинформации уже никому не требуется объяснять, и не только в Соединенных Штатах. Эксперты опасаются, что так называемые «дипфейки» (методика синтеза изображения, основанная на искусственном интеллекте) могут разжигать политическую напряженность путем распространения дезинформации, которую трудно опровергать, а этому помогает, как считает М. Лепский, социологическое наблюдение за пандемией [5]. Страх перед искусственным интеллектом возрастает в результате ускоренной автоматизации некоторых профессий, усиления гендерной и расовой предвзятости и так называемой проблемы «черного ящика» - когда искусственный интеллект принимает решения, который не могут объяснить даже его создатели [8].

Переход к гиперподключенному миру предоставляет миллиардам граждан уникальную возможность получить улучшенный доступ к образованию, здравоохранению, рынку труда и финансовым услугам. В текущем десятилетии мы станем свидетелями ускорения цифровизации, усложнения связанных с ней проблем и постоянного изменения цифровых рисков. Вопрос заключается в том, смогут ли правительства стать более гибкими и в состоянии ли они оперативно брать на вооружение более комплексные подходы к регулированию рисков и цифровой стратегии, чтобы получать выгоды от этого ускорения при одновременном ограничении рисков?

2 РИСКИ И ПОТЕНЦИАЛ ЗЛОУПОТРЕБЛЕНИЙ ЦИФРОВОЙ ИДЕНТИЧНОСТЬЮ

Для стран, стремящихся воспользоваться выгодами цифровой трансформации, киберпреступность - только один из многих цифровых рисков [9]. Соответствующие технологии уже вполне достигли зрелости. Например, алгоритмы безопасности и шифрования, такие как двухфакторная аутентификация и асимметрическое шифрование, улучшают целостность и повышают конфиденциальность данных. Искусственный ин-

теллект, машинное обучение и встраиваемые в мобильные устройства биометрические датчики значительно сокращают масштабы мошенничества. Они также могут улучшать технологии путем сканирования отпечатков пальцев, лица или голоса. Кроме этого, появившееся не так давно специализированное программное обеспечение с открытым кодом, решения на основе открытого интерфейса прикладного программирования (API) и международные стандарты позволяют сократить затраты на внедрение национальных программ цифровых удостоверений личности. Поставщики технологий уже идут на шаг впереди, и новое поколение решений для идентичности не заставляет себя ждать. В некоторых странах, включая Эстонию, начинают тестировать удостоверения личности на основе блокчейна. Эта потенциально прорывная технология могла бы передать контроль и собственность на данные от правительств гражданам при сохранении прерогативы правительств по выпуску и подтверждению удостоверений личности и связанных с ними услуг. Однако, риски и потенциал злоупотреблений цифровой идентичностью остаются реальными и требуют тщательного и постоянного внимания со стороны разработчиков политики и регуляторов. Хотя пандемия, вне всякого сомнения, сделала очевидными выгоды цифровых удостоверений личности, она выявила и ту опасность, которая угрожает конфиденциальности в сочетании с другими технологиями, такими как приложения для отслеживания. Независимо от того, какие технологии будут использоваться, успешные системы цифровой идентичности должны быть безопасными, инклюзивными и взаимно совместимыми, для того чтобы оказать трансформирующее воздействие на миллиарды людей [10].

3 РАЗВИТИЕ ТРАНСНАЦИОНАЛЬНОЙ ОРГАНИЗОВАННОЙ КИБЕРПРЕСТУПНОСТИ КАК ОГРОМНЫЙ БИЗНЕС

Транснациональная организованная преступность - это сегодня огромный бизнес, который зарабатывает 2 триллиона долларов в год: деньги поступают от торговли наркотиками, краж интеллектуальной собственности, торговли людьми, детской порнографии, похищения личных данных, движения людей и контрабандных товаров, получения доступа к

частным учетным записям почтового сервиса Gmail, доступа к системе паролей, что дало возможность пользователям входить в ряд служб Google и успешно взламывать базу данных по всему миру [10]. Компания неоднократно оказывалась под прицелом ловких хакерских компаний, в результате чего хакеры еще в 2010 году похитили текст программы для системы управления паролями, которая позволяла пользователям одновременно заходить в разные приложения Google. Кража вызвала панику среди высшего руководства Google - компании, которая гордится своей системой безопасности пользователей и их персональных данных и построившая себе репутацию, гарантируя эту безопасность. Агентство проводит политику покупки информации об уязвимостях и платит за это самую высокую цену, а также проводит наступательные кибероперации, которые могут нанести им поражение. К созданию киберармии подталкивают масштабные шпионские операции, направленные против оборонных предприятий. В общем, как считают эксперты, организованная преступность, которая формирует современные корпоративные структуры, создает от 15 до 20% мирового ВВП [4]. Локальные криминальные сети и группировки, быстро собираются и подстраиваются, чтобы использовать любые незаконные возможности и каналы для своей незаконной деятельности, хорошо структурированные и саморегулирующиеся, создают клиринговые центры (посредников, финансовых организаций, предлагающих разнообразные услуги взаиморасчетов), гарантируют незаконные продукты или похищенную информацию. Преступные корпорации имеют онлайн-учебники по всем важнейшим вопросам и навыкам - от проблем с преодолением файерволов к клонированию кредитных карточек [11]. Преступники имеют доступ к созданным корпорациями онлайн-курсов, где они учатся запускать компании с «фишинга», распространять спам, а также пользоваться заготовками для создания вредоносного программного обеспечения, усваивая ремесло цифровой преступности и кибермошенничества. В киберподпольном мире созданы своеобразные «Википедии», содержащие подробные ссылки, которые разбиты по категориям - как взламывать все имеющиеся устройства, программное обеспечение и операционные системы. Киберпреступники намного мощнее и дальновиднее, более успешнее и технологически подготовленнее уголовными командами, которые обеспечивают себя высокими доходами при относительно малых рисках. Судебные расследования киберпреступлений являются чрезвычайно редкими, потому что приговоры по ним составляют менее тысячной доли процента всех уголовных наказаний, которые продолжают осуществлять агрессивные кибероперации, направленные на похищение информации, причем наиболее активно хакерские контратаки осуществляются в банковской сфере [12].

4 УСЛОВИЯ РАСЦВЕТА ОРГАНИЗОВАННОЙ КИБЕРПРЕСТУПНОСТИ И ПУТИ ЕЕ ПРЕСЕЧЕНИЯ

Так называемые криминальные предприятия создают собственные структуры, всегда пользуются собственной юрисдикцией оффшорных зон или стран со слабым государственным управлением, нестабильными политическими режимами, которые за определенную плату готовы закрывать глаза на нелегальную деятельность криминальных структур [13]. В рамках этих преступных синдикатов формируются отделы труда и управления поставками, руководители отделов, внешние консультанты и команды исполнителей. Хакеры совершенствуют и демонстрируют свое мастерство во взламывании технологий, продолжая постоянный поиск новых возможностей, а количество киберпреступлений растет, в то время как компании не имеют технических ресурсов, чтобы защитить себя. Существует рынок для кибернаемников, которые разрабатывают и продают шпионское программное обеспечение (ПО) и хакерские инструменты, не уступая при этом государственным разработкам США. Шпионские программы участников киберподполья способны контролировать компьютер, копировать файлы и записывать каждое слово, технологические инновации выходят из подпольного мира и процветают, а коллективный преступный интеллект уверенно берет верх над антивирусными компаниями. Убытки от программного обеспечения. Сегодня, когда мы сталкиваемся с фактами плохого состояния мирового программного обеспечения, программисты говорят, что нет идеального программного обеспечения, так как оно будет сломано, каким бы оно ни было [14]. Пользователи стремятся иметь

мощное многофункциональное программное обеспечение, определяя безопасность приоритетом и ключевым компонентом надежных вычислений. Эта проблема растет по мере того, как все больше и больше устройств начинают общаться друг с другом и все ошибки ПО, дефекты безопасности имеют кумулятивный характер в контексте глобальной информационной сети. Именно поэтому 75% компьютерных систем можно взломать за считанные минуты [15]. Учитывая, что ПО управляет глобальной экономикой и всеми критическими инфраструктурами, от электричества до телефонных сетей, правительства не имеют права терять время. Правительства должны помочь компаниям понять, что, учитывая долгосрочную перспективу, в их интересах создать более безопасное и стабильное ПО, необходимое для общего технологического будущего и отказ осуществить это будет иметь для них тяжелые последствия, поэтому необходимо правовое регулирование глобальной кибербезопасности, направленное на то, чтобы выработать геном безопасности [6, с.1-13].

5 ПРАВОВЫЕ ОСНОВЫЙ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ В УКРАИНЕ

Становление рыночных отношений в Украине, информатизация и интеллектуализация производства, рост уровня конкуренции между субъектами хозяйствования, которая не всегда имеет добросовестный характер, способствуют усилению значения информации во всех сферах общества. Процесс расширенного производства информационных ресурсов, их использования и защита, начиная с середины XX в., обеспечил переход к информационному обществу, в котором усилия человека все меньше сосредоточены на производстве материальных ценностей, а одновременно актуальными становятся коммуникации и обработка информации. В условиях модернизации информационных отношений, постоянного расширения возможностей использования информационного пространства сети Интернет, развития конкурентоспособной хозяйственной деятельности, как никогда остро стоит проблема защиты информации о производстве, технологиях, управлении, финансовой и другой деятельности в сфере хозяйствования, а также безопасности общества и государства в целом. Актуальным является принятие Закона Украины «Об основных принципах обеспечения кибербезопасности Украины» от 5 октября 2017 года, который определяет правовые и организационные основы обеспечения защиты жизненно важных интересов человека и гражданина, общества и государства, национальных интересов Украины в киберпространстве (ст.1) [17]. Правовую основу обеспечения кибербезопасности Украины составляют Конституция Украины, законы Украины относительно основ национальной безопасности, основ внутренней и внешней политики, электронных коммуникаций, защиты государственных информационных ресурсов и информации, требование по защите которой установлено законом. Правовую основу кибербезопасности в Украине составляют – Законы Украины, Конвенция о киберпреступности, другие международные договоры, согласие на обязательность которых предоставлено Верховной Радой Украины, указы Президента Украины, акты Кабинета Министров Украины, а также другие нормативно-правовые акты, принимаемые во исполнение законов Украины. Так, Конвенция о киберпреступности ЕС (ETS №185 от 23 ноября 2001 №994_575, ратифицированная Верховной Радой Украины 7 сентября 2005) признает, что страны ЕС обеспокоены риском того, что компьютерные сети и электронная информация могут использоваться для осуществления уголовных преступлений, и поэтому уверены в первоочередной необходимости совместной уголовной политики, направленной на защиту общества от киберпреступности путем создания соответствующего законодательства и укрепления международного сотрудничества. Кибершпионаж, определяет Закон Украины – это шпионаж, осуществляемый в киберпространстве (виртуальном пространстве), которое предоставляет возможности для осуществления коммуникаций и/или реализации общественных отношений, образованном в результате функционирования совместимых (соединенных) коммуникационных систем и обеспечения электронных коммуникаций с использованием сети Интернет и/или других глобальных сетей передачи данных или его использованием. Соответственно, от кибератак предполагается использование киберзащиты, которая представляет совокупность организационных, правовых, инженерно-технических мероприятий, а также мероприятий криптогра-

фической и технической защиты информации, направленных на предотвращение киберинцидентов, выявление и защиту от кибератак, ликвидацию их последствий, восстановление постоянства и надежности функционирования коммуникационных, технологических систем.

ВЫВОДЫ

Через осознание и признание угроз, которые технологии несут для всего человечества, следует начать изменения, необходимые для укрепления фундамента нашего технологического будущего. Необходимо усиление государственного контроля в сфере киберпреступности, уровень активности которой растет в сетях.

Необходимо повышать стандарты безопасности и гарантировать кибербезопасность (какими бы сложными ни были технологии или интернет-сервисы), участники цифрового подполья уже наготове, чтобы по своему усмотрению использовать новомодные средства и ориентироваться прежде все на деньги за счет более масштабных, но точно выверенных краж, способных бросить вызовы власти и идти на нарушение правил и законов, создавая вредоносное обеспечение, стремясь стимулировать инновации и создавать новые направления преступлений в отношении бизнеса, разрабатывая новые виды киберафер, поэтому государство должно предотвратить хакерские атаки, создавая препятствия для них.

Государство должно разработать различные технические, организационные, образовательные рекомендации информационной политики, направленной на уменьшение рисков, связанных с технологиями; оно (государство) должно определить, как применять те или иные инструменты для получения максимально возможной пользы при минимизации негативных последствий, и только так мы сможем выдержать испытания прогрессом.

Для современного общества и экономики доверие к киберпространству является крайне важным, поскольку уровень угроз сегодня увеличился, хакеры ежедневно похищают данные, а государство не в состоянии их защитить, тогда как компании не имеют технического ресурса, чтобы самостоятельно защититься.

Сегодня необходимо усиление государственного контроля в сфере защиты общества и личности в противодействии киберпреступности, чтобы повысить стандарты безопасности и гарантировать усиления киберохраны на критически важные объекты государственной инфраструктуры. Государство должно сформировать эффективную концепцию национальной безопасности, обнародовав информацию о хакерах и усилении контроля, чтобы защититься от хакерских преступных атак, опираясь на кибермию.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ:

1. *Андрюкайтене Регина, Воронкова Валентина, Кивлюк Ольга, Романенко Татьяна, Ирина Рижова Ирина. Концептуализация smart-общества и smart-технологий в контексте развития современной цивилизации. Mokslas ir praktika : aktualijos ir perspektyvos. 2017. P. 11-12.*
2. *Voronkova V. H. The philosophy of globalization: the socioanthropological, socioeconomic and sociocultural dimensions. Monograph. Zaporozhye : DIG Publishing, 2010, 276.*
3. *Воронкова В.Г., Соснін О.В. Формування інформаційного суспільства в Україні: виклик чи потреба часу? Гуманітарний вісник Запорізької державної інженерної академії. 2015. Випуск 60. С.13-24.*
4. *Воронкова Валентина, Андрюкайтене Регина, Никитенко Виталина. Развитие общества искусственного интеллекта в условиях постмодерности: проблемы, риски, вызовы.). Вестник «Результаты работы ученых: социология, криминология, философия и политология. Том 1 № 5 (2020): «Результаты работы ученых: социология, криминология, философия и политология. С.52-62 https://sci-result.de/journal/issue/view/5/5*
5. *Гудмен Марк. Злочини майбутнього: усе взаємопов'язане, усі вразливі і що ми можемо з цим зробити/ пер з англ. І.Мазарчук, Я. Машико. К.: Вид-во Ранок: Фабула, 2019. 592 с.*
6. *Лепский М.А. Социологическое наблюдение за пандемией: связанность, паника, волны кризиса. Немецкий научный/научно-популярный Вестник «Результаты работы ученых: социология, криминология, философия и политология». 2020. Том 1, No 2. С.27-40.*
7. *Мальцев О. «Цивилизация XXI века: геном безопасности». Журнал Немецкого научного/научно-популярного журнала Вестник «Результаты работы ученых: социология, криминология, философия и политология». 2020. Том 1 (4). С.1-13.*
8. *Мальцев О.В. Методология науки. Абстрактная и прикладная категории науки. Немецкий научный/научно-популярный Вестник «Результаты работы ученых: социология, криминология, философия и политология». 2020. Том 1, No 3. С. 64-70.*
9. *Nikitenko Vitalina, Andriukaitiene Regina, Punchenko Oleg. Formation ofsustainable digital economical concept: challenges, threats, priorities. Humanities Studies. 2019. Випуск 1(78). С. 140-153.*
10. *Oleksenko, Roman. Position and role of modern economic education as the main megatrend of innovative development of Ukraine. Humanities Studies. Запоріжжя: ЗНУ 2020. 2 (79). С. 169-181.*
11. *Панченко Ольга. Римская формула. Наука и деньги. Советы молодым ученым (Интервью с профессором Массимо Интровинье). Вестник «Результаты работы ученых: социология, криминология, философия и политология. Том 1 № 5 (2020): «Результаты работы ученых: социология, криминология, философия и политология. С.52-62.*
12. *Punchenko Oleg. Punchenko Natalia. Basic strategic technology of intellectual duality of humanity in information technology. Humanities Studies. 2019. Випуск 2(79). С. 95-114.*
13. *Шейн Гарріс. Війн@ : битви в кіберпросторі. Київ : Ніка-Центр; Львів: Видавництво Анетти Антоненко, 2019. 296 с.*
14. *Шваб Клаус. Четверта промислова революція, Формуючи четверту промислову революцію. Харків : Клуб сімейного дозвілля, 2019. 426 с.*
15. *Череп А.В. Концептуальні засади економічної безпеки підприємств. Журнал Запорізького національного університету : Економічні науки. 2010. С.62.*
16. *Cherep Alla, Voronkova Valentyna, Muts Luai Faisal, Fursin Alexander. Information and innovation technologies as a factor of improving the efficiency of digital economy and business in the Globalization 4.0. Humanities Studies. 2019. Випуск 1(78). С.170-181.*
17. *Voronkova Valentyna, Kapitanenko Nataliia, Nikitenko Vitalina. Правові засади захисту інтелектуальної власності у цифровому суспільстві. ScienceRise: Juridical Science.2019. 4 (10). С.32-37.*
18. *Об основных принципах обеспечения кибербезопасности Украины: Закон Украины от 5 октября 2017 № 2163-VIII / Верховная Рада Украины. 2017. № 45. ст.403.*