ОБРАТНАЯ СТОРОНА ТЕХНОЛОГИЧЕСКИХ ИННОВАЦИЙ И ИХ ПОСЛЕДСТВИЯ В УСЛОВИЯХ ИННОВАЦИОННО-ИНФОРМАЦИОННОГО ОБЩЕСТВА

Череп Алла[1], Воронкова Валентина[2], Никитенко Виталина[2]

[1]Запорожский национальный университет, Запорожье, Украина

[2]Инженерный институт Запорожского национального университета, Запорожье, Украина

Аннотация

Актуальность темы исследования. Актуальность данного исследования заключается в том, что в условиях инновационно-информационного общества технологические инновации оборачиваются обратной стороной, так как преступные организации используют их против общества и человека, угрожают тем самым взаимосвязанному и взаимозависимому миру, который становится более уязвимым. Различные террористические и криминальные организации «оккупировали» новейшие

технологии и делают это так успешно, что человечество постоянно отстает со своими системами национальной защиты. Сегодня нет ни одного компьютера или смартфона, который не может быть сломан и ничего нельзя сохранить в тайне - от персональных данных к военным и биологическим разработкам, потому что мир перенасыщен алгоритмами, большими данными, битами и прогресс продвинулся далеко буквально на наших глазах. **Цель исследования** – теоретические и практические аспекты исследования обратной стороны технологических инноваций и их последствий в условиях инновационно-информационного общества, а также создание таких условий, чтобы защитить человека цифрового общества и разработать инновационные средства защиты. Преступные организации постоянно обновляют технические приемы и средства, чтобы применить самые новейшие технологии против человека и человечества. **Задачи исследования**: 1) проанализировать теоретические и практические аспекты исследования обратной стороны технологических инноваций и их последствий 2) выявить условия, которые способны защитить человека цифрового общества и разработать технические средства защиты, так как преступные организации постоянно обновляют технические приемы и средства; 3) разработать концепцию национальной безопасности в условиях инновационно-информационного общества. Обосновано применение **методологии исследования** как совокупности методов общенаучного, общефилософского и специального характера для того, чтобы глубоко проникнуть в сущность обратной стороны технологических инноваций, которые оборачиваются против человека и человечества. В основе таких методов – системный, системно-структурный, структурно-функциональный, институциональный, которые дают возможность показать обратную сторону технологических инноваций в условиях инновационно-информационного общества как сложную систему с множеством организационных подсистем подструктур организаций, которые строго иерархизированы, каждая из которых представляет собой генезисно-процессуальную и целостно-функциональную в их совокупности взаимосвязей с миром информационным, сетевым, цифровым, который представляет сложный механизм субсистем. **Результат исследования:** 1. Раскрыты теоретические и практические аспекты исследования обратной стороны технологических инноваций и их последствий, которые представляют движущую силу добра и зла, потому что компьютерная преступность получает большие выгоды от экспоненционального характера развития технологий, так как преступные организации постоянно работают над информацией. 2. Выявлены условия, которые способны защитить человека цифрового общества, для чего необходимо разработать технические средства защиты. 3.Обоснована концепция национальной безопасности в условиях инновационно-информационного общества, которое есть глубоко взаимосвязанным и технологически

небезопасным. **Практическое значение исследования** данной темы в том, чтобы правительства выделяли ресурсы, достаточные для принятия мероприятии для борьбы с технологиями как силой зла и осознали масштабы нашей технологической уязвимости.

Ключевые слова: инновационно-информационное общество, цифровое общество, информационно-компьютерные технологии, технологические инновации, обратная сторона технологического прогресса, национальная безопасность.

Введение

Актуальность темы исследования. Актуальность данного исследования заключается в том, что проблема обратной стороны технологических инноваций и их последствий в условиях инновационно-информационного общества приобретает все большее значение, потому что мы живем в цифровую эру, которая движет алгоритмами, битами, большими данными, которые используются в работе криминальных и террористических организаций для высокотехнологических преступлений. Это свидетельствует о том, что мир вступил в новый этап инновационно-информационного общества, в котором незаконно используется применение передовых прорывных технологий, которые стоят в том числе и на службе криминального мира (хакеры и их подрывные организации), уровень технической подготовки которых настолько высок, что в своих преступных целях они могут создавать коммуникационные сети, которые функционируют по всех странах и владеют ошеломляющими деньгами и мастерством. Организованные преступные структуры зарекомендовали себя пионерами современной технологии, которую успешно использовали в онлайн-мире еще задолго до того, когда защитники правопорядка обратили на это внимание, опережая их во многих вопросах, включая трансфер технологий (Андросова, Череп, 2007). Они продвинулись далеко в сфере робототехники, виртуальной реальности, синтетической биологии, искусственного интеллекта, 3D-печати и много чего другого. Человечество сегодня должно осознать угрожающие масштабы развития технологий, не говоря об увеличивающемся объеме их использования как организованной преступностью, так и террористическими организациями, примером чего стала биологическая и бактериологическая (гибридная) война против человечества. Сегодняшние хакеры стали высокоорганизованными и сформировали глабальные он-лайновые преступные синдикаты, которые в массовом порядке воруют персональные данные, так как 80% людей находится в сети Интернет, а в 2025 году произойдет переломный момент. Присутствие в цифровом мире стремительно возросла за последние 20 лет, а лишь только 20 лет назад это означало наличие номера мобильной связи, электронного адреса и персонального веб-сайта или профиля в сети MySpace. Сегодня цифровым присутствием считается цифровое взаимодействие на многих

интернет-платформах и в социальных сетях, включая становление и развитие SMART-общества как высокоразумного, высокотехнологического, высокоинтеллектуального общества (Андрюкайтене и др., 2017).

Цель исследования – теоретические и практические аспекты исследования обратной стороны технологических инноваций и их последствий в условиях инновационно-информационного общества, а также создание таких условий, чтобы защитить человека цифрового общества и разработать технические средства защиты, так как преступные организации постоянно обновляют технические приемы и средства, чтобы применить самые новейшие технологии против человека и человечества.

Задачи исследования: 1) раскрыть теоретические и практические аспекты исследования обратной стороны технологических инноваций и их последствий; 2) выявить условия, которые способны защитить человека цифрового общества и разработать технические средства защиты, так как преступные организации постоянно обновляют технические приемы и средства; 3) обосновать концепцию национальной безопасности в условиях инновационно-информационного общества.

Методология исследования

Обосновано применение методологии исследования как совокупности методов общенаучного, общефилософского и специального характера для того, чтобы глубоко проникнуть в сущность обратной стороны технологических инноваций, которые оборачиваются против человека и человечества в контексте концептуализации smart-общества и smart-технологий (Андрюкайтене и др., 2017). В основе таких методов – системный, системно-структурный, структурно-функциональный, институциональный, которые дают возможность показать обратную сторону технологических инноваций в условиях инновационно-информационного общества как сложную систему с множеством организационных подсистем подструктур организаций, которые строго иерархизированы, каждая из которых представляет собой генезисно-процессуальную и целостно-функциональную в их совокупности взаимосвязей с миром информационным, сетевым, цифровым, который представляет сложный механизм субсистем (Аль-Халілі, 2018). Данные методы исследуют процессы управления в системах разной природы этих организаций, которые сопричастны к методам кибернетики (программного обеспечения, информационно-компьютерных технологий, прорывных технологий), менеджмента (гибкого, адаптивного менеджмента, принятия управленческих решений, командного и операционного менеджмента), системного анализа устойчивого развития. Методология исследования - в применении вышеперечисленных методов анализа организаций, которые действуют в

условиях нелинейного мира, которые дают возможность проанализировать нелинейный мир как сложную диссипативную систему и раскрывают новые явления современных явлений и процессов научного дискурса инновационно-информационного общества, названного еще цифровым. К анализу проблем нелинейного мира может быть применима методология сложности как методология анализа проблем сложного XXI века для того, чтобы показать современный нелинейный мир как динамическую систему знаний, которые раскрывают новые явления в обществе, природе, технике в условиях глобализации (Воронкова, 2008).

Результат исследования

1. *Проанализированы теоретические и практические аспекты исследования обратной стороны технологических инноваций и их последствий*, так как технологии широко доступны криминальным группам и хакерам. В условиях переделов финансовых рынков и капиталов возрастает число обратной стороны технологических инноваций, которые не останавливаются перед финансовыми прибылями. В условиях нового передела мира преступники цифрового мира осознают, что мир «больших данных» шаг за шагом стал мобильным и именно в этой сфере аккумулируются усилия для получения максимальных прибылей от инвестиций в разработку вредоносного программного обеспечения. И компьютерные преступники адаптируются к этому, быстро разрабатывая нововведения. Злоумышленники могут украсть вашу информацию из сайта (например, пароли данные кредитных карточек, сообщения и т.п.), демонстрируя ненадежность мобильной системы. Начиная с использования мобильных телефонов и смартфонов, программное обеспечение которых можно легко сломать, так как системы защиты этих устройств есть примитивными и абсолютно несовершенными, смартфоны и мобильные телефоны есть теми устройствами, которые легче всего поддаются взламыванию, так как вредоносные программы для мобильных телефонов нацелены на операционную систему Android от Gogle. Компания Gogle не в состоянии обеспечить надежную систему и сделать обновление системы безопасности доступными для базового контента своих пользователей и дает возможность злоумышленникам воспользоваться личными данными пользователей в своих интересах (Nikitenko и др., 2019). В условиях нового передела мира преступники цифрового мира осознают, что мир «больших данных» шаг за шагом стал мобильным и именно в этой сфере аккумулируются усилия для получения максимальных прибылей от инвестиций в разработку вредоносного программного обеспечения, поэтому компьютерные преступники адаптируются к этому, быстро разрабатывая свои нововведения (Олексенко, 2017). Злоумышленники могут украсть вашу информацию из сайта (например, пароли данные кредитных карточек, сообщения и т.п.), потому что смартфоны есть теми устройствами,

которые легче всего поддаются взламыванию. В наше время разработано большое количество вирусов и троянских программ, которые дают злоумышленникам доступ к микрофонам ваших телефонов и позволяют записывать все даже того, когда человек не пользуется телефоном. Любое сообщение, адресная книга, фото, журнал вызовов, пароли социальных сетей и состояние счета – все это может быть перехвачено, декодировано и отправлено злоумышленникам и их организациям для дальнейшего использования в их интересах (Олексенко, 2013). Мелверы для смартфонов способны постоянно отслеживать ваше местопребывание, видеть это место благодаря Google Mars почти в реальном времени, а видеокамера вашего смарфона может быть включена без предупредительного сигнала и будет снимать вас и ваше окружение. Киберпреступники разработали новые способы еще большего количества дополнений в сфере банковского обслуживания. На сегодня выявлены пакеты вредносного программного обеспечения, в 2012 г. было изобретено 67 банковских троянських вирусов, согласно «лаборатории Касперского» их количество в 2013 г. превышало 1300. Сегодня выявлены пакеты вредоносного программного обеспечения, нацеленного на клиентов наибольших банков мира Citibank, ING, Deutshe Bank, HSBC, Barclaysи еще 66 финансовых учреждений мира. В результате отсутствия проверки безопасности с троянскими вирусами, они могут существовать вечно, обеспечивая преступным группировкам постоянные доходы. Финансовые аналитики в 2020 году засвидетельствовали, что лабораторный вирус, распространяемый спецслужбами США через сеть кофеен в крупных торговых центрах мегаполисов Китая, имел целью обвалить финансовые рынки конкурентов США – Китая и Европы, что привело к появления коронавируса и смерти тысяч людей. Мы стали свидетелями криминализации финансового мира, в том числе большого количества финансовых и других махинаций.

2. *Выявлены условия, которые способны защитить человека цифрового общества и разработать технические средства защиты*, так как преступные организации постоянно обновляют технические приемы и средства. Сегодня человек выступает объектом хакерских преступных группировок, которых интересуют большие данные BIG DATA - первичных данных компьютеров, которые могут не только свободно продавать продукты «Adobe», в частности, Photoshop, GoldFusion і Acrobat, но и способны поменять код и встроить в продукт неизлечимое количество продуктов, которые можно отнести к вредоносным программам, в контексте которых осуществляется воровство персональных данных. В виртуальном пространстве преступные группировки используют спам, фитинг, фейковые рекламные объявления, распространение детской порнографии, получении информации незаконными способами. Не случайно на борьбу с киберпреступностью сегодня тратится почтим 400 миллиардов долларов. Усовершенствование искусственного интеллекта может

еще более усовершенствовать эти инструменты. Алгоритмическое хакерство может создать серьезные проблемы для общества и его критических инфраструктур. Есть точка зрения, что к 2030 году искусственный интеллект достигнет уровня человеческого, а к 2045 г. в миллиард раз увеличится биологически-машинный интеллект нашей цивилизации, что еще более усилит нашу компьютерную незащищенность. Цифровое производство станет материалом для преступных группировок, которые молниеносно могут сделать – ключи от вашей машины или офиса, создать дубликат чего-угодно. Большинство технологических угроз должны уже сегодня рассматриваться на системном уровне, поэтому мы сами должны понимать риски и брать на себя ответственность, а для этого быть подготовленными в правовом поле (Соснін, 2016).

*3. Разработана концепция национальной безопасности в условиях инновационно-информационного общест*ва. Концепция национальной безопасности связана с понятиями экономическая безопасность, региональная безопасность, экологическая безопасность, чтобы противодействовать всем вызовам, которые ставит перед нами новое общество – информационное, инновационное, цифровое, чтобы научиться противодействовать преступным группировкам хакерского общества, способного дестабилизировать общую глобальную безопасность (пример коронавируса). *В основе концепции национальной безопасности в условиях инновационно-информационного общест*ва – исследование влияния глобализации на национальную безопасность государства в контексте соотношения экономических, военных, технологических, информационных, экологических компонентов национальной безопасности, борьба с транснациональной организованной преступностью, вредоносным программным обеспечением и надежным и безопасным функционированием компьютерных технологий. Очень важной функцией есть обеспечение компьютерной инфраструктуры организации и ее развития, информационная безопасность, управление сетями, которые делают безпечной нашу жизнь. В информационном мире должна бать защищена глобальная информационная матрица, чтобы защитить мир, в котором каждый физический объект может быть подключен к сети. Поэтому через 10-20 лет инфраструктурой разумных городов будут «управлять цифровые технологии – искусственный интеллект, автомобили с автопилотами, дополненная реальность, генетически модифицированная еда, новые и активные источники энергии, разумные материалы, неизлечимое количество гаджетов и устройств, соединенных между собой различными способами обмена информацией (Аль-Халілі, 2018). Граница между человеком и машиной, онлайн-и офлайн мирами становится все более размытой. Дополненная реальность (ДР) обеспечивает прямой пересмотр физической среды через экран компьютера

или же мобильного телефона в режиме реального времени, накладывая на него дополнительную цифровую информацию, другие изображения, GPS-данные.

Выводы

Таким образом сделаем вывод, что мы живем в эпоху конвергенции, когда биты цифрового царства сливаются с атомами физического мира. Информационные технологии и цифровые изменения становятся одним из проявлений выразительной тенденции к взаимозависимости, когда взаимодействуют и взаимовлияют друг на друга цифровой, физический и реальный миры (Череп и др., 2019). Цифровые технологии становятся движущей силой и главным фактором развития как экономического базиса, так и общества в целом, способствуя многообразию проявления цифрового мира в виртуальной, дополненной и настоящей реальности. Квантовые технологи в будущем могут стать таким прорывом, что их создание позволит обеспечить коммуникации, которые невозможно сломать, поскольку будет наблюдение или даже перехват квантового ключа ширфровния, что автоматически изменит его смисл. В мире, переполненном гаджетами, компьютерами, алгоритмами, портативними устройствами, REID-чипами и смартфонами, только незначительная часть людней имеет представление, как они работают. Поэтому мы должны повышать техническую, правовую грамотность населения, чтобы противостоять этому миру хакерской культуры, преступные организации которого используют их против общества и человека, угрожают тем самым взаимосвязанному и взаимозависимому миру, который становится более уязвимым. Различные террористические и криминальные организации «оккупировали» новейшие технологии и делают это так успешно, что человечество постоянно отстает со своими системами национальной защиты, поэтому техническая грамотность всего населения поможет бороться с этим преступным миром и заставит работать весь этот технически-информационный мир на пользу мира, добра, разума, прогресса, науки.

Практическое значение исследования данной темы в том, чтобы правительства выделяли ресурсы, достаточные для принятия мероприятии для борьбы с технологиями как силой зла и осознали масштабы нашей технологической уязвимости, потому что правительственные усилия, направленные на защиту людей от киберпреступности и угроз безопасности, выявились абсолютно неадекватными и неэффективными. Десятки тысяч нападений, успешно осуществленных против самого Вашингтона вражескими иностранными государствами, террористами и хакерами, свидетельствует о том, что правительство США не способно защитить даже себя. Очевидно, что есть необходимость в более серьезном и глубоком сотрудничестве гражданских и частных секторов. Без этого не произойдет существенного прогресса в улучшении общего состоянии дел, связанных с безопасностью в

век цифровой революции. Для защиты нашего современного цифрового века необходимым есть сотрудничество правительства и промышленности, но главный вопрос в том, как это осуществить. Следует развивать программы, направленные на стимулирование сотрудничества между теми, кто отвечает за критические инфраструктуры мира, наладить всесторонний обмен информацией; лучше реагировать на киберугрозы, проводить совместные совещания для координации действий при возникновении инцидентов и угроз безопасности компьютерных сетей; способствовать улучшению координации и реагировании между специалистами данной сферы, которые занимаются сбором информации о компьютерных инцидентах, их классификацией и нейтрализацией, заслуживают на доверие такой организации, как CERT, которая и занимается анализом этих феноменов, чтобы содействовать изменениям в сфере кибербезопасности путем создания эффективных правительственных и частных структур.

Литература

Андросова, О. Ф., Череп, А. В. (2007). Трансфер технологій як інструмент реалізації інноваційної діяльності: *монографія.*

Андрюкайтене, Р., Воронкова, Г., Кивлюк, О., Никитенко, В. (2017). Становление и развитие SMART-общества как высокоразумного, высокотехнологического, высокоинтеллектуального. *Гуманітарний вісник Запорізької державної інженерної академії,* 71, 17 – 25.

Андрюкайтене, Р., Воронкова, В., Кивлюк, О., Романенко, Т., Рижова І. (2017). Концептуализация smart-общества и smart-технологий в контексте развития современной цивилизации. *Mokslas ir praktika: aktualijos ir perspektyvos,* 11-12.

Аль-Халілі, Д. (2018). *Що далі? Все, що наука знає про наше майбутнє*/пер. з англ. М.Климчука. Київ: Кі Фонд Медіа.

Воронкова, В. Г. (2008). Глобалізація як процес універсалізації стосунків між державою та ринком. *Гуманітарний вісник Запорізької державної інженерної академії*, 35, 15-35.

Nikitenko, V., Andriukaitiene, R., Punchenko, O. (2019). Developing corporate management to improve the quality of customer service. *Humanities studies: Collection of Scientific Papers, 1*(78), 140-153.

Олексенко, Р. (2017). Людина в умовах інформаційного суспільства як об'єкт соціально-економічної рефлексії. *Становлення і розвиток інформаційного суспільства як основи забезпечення конкурентоспроможності України у світі та сталого розвитку суспільства і держави*, 59-62.

Олексенко, Р. І. (2013). Глобальні проблеми філософії від Античності до сьогодення в дискурсі ринкових трансформацій. *Придніпровські соціально-гуманітарні читання: у 6-ти частинах. . ч 2: матеріали Дніпропетровської сесії II Всеукр. наук.-практ. конф. з міжнародною участю,* 148-151.

Соснін, О. В., Воронкова, В. Г., Ажажа, М. А. (2016). *Філософія гуманістичного менеджменту (соціально-політичні, соціально-економічні, соціально-антропологічні виміри): навчальний посібник.* Запоріжжя: Дике поле.

Череп, А., Воронкова, В., Муц, Л., Фурсін, О. (2019). Інформаційні та інноваційні технології як чинник підвищення ефективності цифрової економіки та бізнесу в умовах глобалізації 4.0. *Humanities studies: Collection of Scientific Papers, 1*(78), 170-181.