Шаушенова Анаргуль Гимрановна,
канд. техн. наук, старший преподаватель
кафедры информационно-коммуникационных технологий;
Казахский агротехнический университет им. С. Сейфуллина,
г. Нур-Султан, Республика Казахстан

ЧЕТВЕРТАЯ ПРОМЫШЛЕННАЯ РЕВОЛЮЦИЯ И КОНФЛИКТЫ XXI ВЕКА

В статье рассматриваются особенности эпохи четвертой промышленной революции и конфликты, в особенности киберпреступления, свойственные данной эпохе, и меры их предотвращения.

Ключевые слова: четвертая промышленная революция, информационные и цифровые технологии, конфликты, киберпреступления, кибербезопасность.

Anargul G. Shaushenova
Ph.D in Technical Sciences, senior teacher
of the department of information and communication technologies
S. Seifullin Kazakh Agrotechnical University
Astana, Republic of Kazakhstan

FOURTH INDUSTRIAL REVOLUTION AND CONFLICTS OF THE XXI CENTURY

The article discusses the features of the era of the fourth industrial revolution conflicts, in particular cybercrime, characteristic of this era and measures to prevent them.

Key words: fourth industrial revolution, information and digital technologies, conflicts, cybercrime, cybersecurity**.**

Во второй половине XX века с создания цифровых компьютеров и последующей эволюции информационных технологий началась Третья промышленная революция, которую еще называют цифровой. Цифровая революция в данный период времени переходит в четвертую, особенности которой заключаются в массовом внедрении киберфизических систем в производство.

Как описывает промышленную революцию основатель Всемирного экономического форума Клаус Шваб, она стирает границы между физическими, цифровыми и биологическими сферами. «Речь идет о волне открытий, обусловленных развитием возможностей установления связи: роботы, дроны, умные города, искусственный интеллект, исследования головного мозга» [1].

Предполагается, что эти киберфизические системы будут объединяться в одну сеть, связываться друг с другом в режиме реального времени, самонастраиваться и учиться новым моделям поведения. Они смогут выстраивать производство с меньшим количеством ошибок, взаимодействовать с производимыми товарами и, при необходимости, адаптироваться под новые потребности потребителей. Например, изделие в процессе выпуска сможет само определить оборудование, способное произвести его, при этом в полностью автономном режиме, без участия человека. Товар в процессе выпуска сможет сам определить оборудование, способное произвести его.

Первыми шагами мира к новой промышленной революции стали облачные технологии, развитие способов сбора и анализа Big Data, краудсорсинг, биотехнологии, беспилотные автомобили и медицина, основанная на 3D-печати. В мире финансов это – криптовалюты Bitcoin и технологии Blockchain.

Понятие *Big Data* – это совокупность технологий, которые призваны совершать такие операции:

- обрабатывать большие по сравнению со «стандартными» сценариями объемы данных;
- уметь работать с быстро поступающими данными в очень больших объемах;
- уметь работать со структурированными и плохо структурированными данными параллельно в разных аспектах.

Internet of Things – концепция пространства, в котором всё из аналогового и цифрового миров может быть совмещено. Это не просто множество различных приборов и датчиков, объединенных между собой проводными и беспроводными каналами связи и подключенных к Интернету, а это более тесная интеграция реального и виртуального миров, в котором общение производится между людьми и устройствами.

Virtual reality – созданный техническими средствами мир, передаваемый человеку через его ощущения: зрение, слух, обоняние, осязание и другие. Виртуальная реальность имитирует как воздействие, так и реакции на воздействие. Дополненная реальность (augmented reality) подразумевает возможность добавлять физическим объектам виртуальные свойства, например, отображение информации о них, последняя, к тому же, может быть индивидуализирована под конкретного субъекта восприятия.

Печать на 3D-принтере может осуществляться разными способами и с использованием различных материалов, но в основе любого из них лежит принцип послойного создания (выращивания) твердого объекта. Существуют также экспериментальные биопринтеры, в которых печать 3D-структуры будущего объекта (органа для пересадки) производится каплями, содержащими живые клетки.

Общество пронизано цифровыми технологиями. Больше 30% населения земного шара сегодня использует социальные сети и медиа для общения, обучения и распространения информации. Технологии, порожденные Четвертой промышленной революцией, все сильнее и сильнее влияют на жизнь человека

Новые технологии влияют на все сферы жизнедеятельности человека, они могут обострить проблемы безопасности. Как считает К. Шваб, будущие конфликты будут носить гибридный характер и совмещать прямые действия на поле боя с негосударственными явлениями и элементами. «Граница между войной и миром, солдатом и гражданским и даже насилием и ненасилием

(кибертерроризм) оказывается пугающе размытой. С развитием военных технологий, появлением биологического и автономного вооружения негосударственные объединения людей достигнут того же уровня смертоносности, что и государства» [1].

Сегодня актуальность проблемы кибербезопасности не вызывает никаких сомнений. Ежедневно каждый из нас сталкивается с необходимостью использования информационных технологий. Заголовки новостей содержат множество сообщений о взломах коммерческих структур, утечке данных, электронном мошенничестве, нарушениях функционирования государственных структур или критически важных объектов инфраструктуры, кражах интеллектуальной собственности, утечке информации, связанной с национальной безопасностью, и потенциальном киберуничтожении. Та сфера, которая когда-то считалась электронной войной или информационной войной, и в которой преобладали специалисты по сетевой безопасности, сегодня преобразовывается в более широкую сферу, именуемую *«кибербезопасность»*.

Надлежащая защита от киберпреступников, в первую очередь, зависит от самих граждан, которые очень часто легкомысленно и неосторожно относятся к электронным платежам и своим персональным данным. Именно персональные данные, которые вы предоставляете банку, являются наиболее востребованными мошенниками, а именно: фамилия и имя, номер мобильного телефона, адрес электронной почты. Обычно такую информацию продают на «черном» рынке, а затем используют для рассылок СМС спама, телефонных звонков рекламного характера. Очень часто указанные данные перехватываются в публичных местах с открытым Wi-Fi доступом при использовании электронной почты или социальных сетей. В этом случае специалисты советуют пользоваться средствами защиты, предлагаемыми почтовыми серверами или социальными сетями.

К сожалению, киберпреступность постоянно совершенствуется и идет в ногу с технологиями, что в свою очередь, затрудняет обнаружение и

противодействие указанным противоправным действиям. Следует помнить, что на практике потерянные деньги очень трудно возместить, ведь виновного в такой ситуации найти не просто, банк несет ответственность только в том случае, если будет доказано, что преступление было совершено по его вине. Сейчас банки активно сотрудничают с правоохранительными органами по предупреждению преступности, связанной с вмешательством в компьютерные системы, однако законодательство по киберпреступности и практика свидетельствуют о значительных пробелах в этой сфере. Мировой опыт показывает, что на сегодняшний день вопросы кибербезопасности носят глобальный характер, что в свою очередь обусловливает потребность в разработке не только национальной, но и соответствующей международной стратегии безопасности [2].

По данным «Лаборатории Касперского», Казахстан находится на 6-м месте в списке стран, пользователи которых наиболее часто подвергаются веб-атакам, и на 9-м – по количеству пользователей, атакованных троянцами-вымогателями для мобильных устройств.

Именно поэтому основным ориентиром и приоритетами законодательства Республики Казахстан, также как и в зарубежных странах, является защита критически важных объектов информационно-коммуникационной инфраструктуры, в том числе и информационно-коммуникационной инфраструктуры «электронного правительства», нарушение или прекращение функционирования которых приводят к чрезвычайной ситуации социального и (или) техногенного характера или значительным негативным последствиям для обороны, безопасности, международных отношений, экономики, отдельных сфер хозяйства, инфраструктуры Республики Казахстан или жизнедеятельности населения, проживающего на соответствующей территории.

Вместе с тем, на сегодняшний день, с целью реализации государственной политики в области информационной безопасности в сфере информатизации и связи (кибербезопасности), Указом Президента Республики Казахстан от 6

октября 2016 года было образовано Министерство оборонной и аэрокосмической промышленности Республики Казахстан. Этим же Указом Правительству РК поручено обеспечить создание Комитета по информационной безопасности, который фактически теперь будет выполнять функции уполномоченного органа (регулятора) по разработке государственной политики в сфере национальной информационной безопасности, что, безусловно, является важным шагом в вопросах обеспечения кибербезопасности страны.

СПИСОК ЛИТЕРАТУРЫ

1. Клаус Шваб. Четвертая промышленная революция. – М.: Эксмо, 2016.

2. U.S. Department of Defense, The DoD Cyber Strategy. – April 2015, Washington, DC. World Economic Forum, Partnering for C.