Лекция 14

ҚАЗАҚСТАННЫҢ АШЫҚ УНИВЕРСИТЕТІ

ЧЕТВЕРТАЯ ИНДУСТРИАЛЬНАЯ РЕВОЛЮЦИЯ

Национальная и глобальная
Часть 2

Цель: дать понимание того, как технологические изменения будут влиять на отношения государств и международную безопасность.

Основные идеи:
1) Международная безопасность.
2) Меняющаяся природа конфликтов и кибернетическая война.
3) Военные действия посредством самоуправляемых систем.

Международная безопасность

«Критически опасно то, что гиперсвязанность мира в условиях растущего неравенства может привести к усилению фрагментации, сегрегации и социальных волнений, которые в свою очередь создадут ситуацию для развития насильственного экстремизма», – Клаус Шваб.

Возможно, одно из самых важных последствий – это то, как технологические изменения будут влиять на отношения государств и международную безопасность. Однако, как один из наиболее важных элементов, он также является одним из наименее обсуждаемых, по крайней мере, за пределами правительств и оборонной промышленности. Как же тогда мы можем реагировать на эти изменения в международной безопасности? Ответ кажется ясным: по мере того как угрозы расширяются, мы также должны реагировать. Пока неясно, как будет выглядеть будущее международной безопасности, но одно можно сказать наверняка: только путем выхода из одной отрасли, политики и региональных группировок, и совместной работы, мы будем иметь конструктивную роль в формировании направления.

Меняющаяся природа конфликтов и кибернетические войны

Хотя фрагментация глобальной системы международных отношений сохраняется, масштабы и характер также меняются. Современные конфликты становятся все более гибридными по своей природе, сочетая традиционные методы видения боевых действий с элементами, которые ранее были в основном связаны с вооруженными негосударственными образованиями или субъектами.

Например, кибератаки. Когда инструмент используется только одинокими хакерами, они представляют одну из самых серьезных угроз нашего времени. Любой будущий конфликт между достаточно продвинутыми участниками почти наверняка будет включать кибер-измерение. Клаус Шваб утверждает, что «по мере того как идет этот процесс, и новые смертельно опасные технологии становится проще приобрести и использовать, мы понимаем, что четвертая промышленная революция предлагает частным лицам все более разнообразные способы причинять вред друг другу в крупных масштабах».

Помимо мира кибервойны, мы слышали от экспертов по искусству и робототехнике в Давосе, как автономное оружие, иногда называемое «роботами убийцами», может стать следующим оружием массового уничтожения. Беспокойство заключается в том, что с темпами технологических разработок политики, люди, занимающиеся вопросами международной безопасности и обороны, будут постоянно в статусе догоняющих, и будут необходимы требуемые нормативные умения.

Поскольку компании способствуют развитию 4-ой промышленной революции, защита кибербезопасности должна быть главным приоритетом для промышленных систем управления (ПСУ). Эти атаки являются финансово обременительными, сокращают производственные и деловые инновации. В прошедшие годы устаревшие ПСУ были разработаны с использованием запатентованной технологии и изолированы от внешнего мира, поэтому физическая безопасность периметра была признана адекватной, а кибербезопасность не была актуальной. Однако сегодня рост цифрового производства означает, что многие системы управления используют открытые или стандартизированные технологии для снижения затрат и повышения

производительности, используя прямую связь между системами управления и бизнес-системами. Теперь компании должны быть активнее, чтобы обеспечить безопасность своих систем как в сети, так и в автономном режиме.

Распространение кибер-угроз побудило владельцев активов в промышленных условиях искать решения в области безопасности, которые могут защитить их активы и предотвратить потенциально значительные денежные потери и эрозию бренда. Более открытые и совместные сети сделали системы более уязвимыми для атаки. Кроме того, осведомленность конечного пользователя и оценка уровня риска неадекватны для большинства отраслей, не относящихся к критическим средствам инфраструктуры.

Недостаточный опыт в промышленных сетях ИТ является общесекторальной задачей, общей проблемой. На этом фоне организации должны сотрудничать с поставщиком решений, который понимает уникальные характеристики и проблемы промышленной среды и готовит их к безопасности.

Военные действия посредством самоуправляемых систем

Более 100 руководителей компаний по искусственному интеллекту и робототехнике недавно подписали открытое письмо, в котором предупреждалось, что их работа может быть переделана для создания летального автономного оружия – «роботов-убийц». Они утверждали, что создание такого оружия равносильно тому, как открыть «Ящик Пандоры», что может навсегда изменить характер и специфику военных действий.

Более 30 стран имеют или разрабатывают вооруженные беспилотные летательные аппараты, и с каждым последующим поколением беспилотные летательные аппараты имеют большую автономию. Автоматизация уже давно используется в оружии, чтобы помочь определить цели и маневрировать ракетами. Но на сегодняшний день люди все еще контролируют решение о применении смертельной силы. Военизированные силы использовали только автоматические сражения в ограниченных условиях для защиты от высокоскоростных ракет.

В течение последних трех лет страны встретились для обсуждения смертоносного автономного оружия. Более 60 неправительственных организаций призвали к заключению договора о запрещении автономного оружия. Тем не менее большинство стран готовятся заранее к бесконтактным автономным военным действиям. Никакие крупные военные державы не заявили, что планируют строить автономное оружие, но мало кто может остановить их.

Автономная технология везде. Невозможно остановить развитие ИИ. Робототехнические компании не могут легко объединиться, чтобы остановить прогресс, из-за того, что одна компания нарушает соглашение и продвигает какую-то вредоносную технологию. Такая же динамика затрудняет сдерживание автономного оружия на международном уровне. Просить страны подписать договор о запрете оружия, которого еще нет, означает попросить их отказаться от потенциально полезного инструмента для защиты от угроз и спасения жизней. Более того, существует аналогичная проблема, как например проблема кибермошенников, которая тоже взвинчивает ставки. Вместо упущенной выгоды, нация может проиграть войну. История показывает, что даже когда международное сообщество широко осуждает химическое оружие как бесчеловечное, то многие страны все-таки используют их при любом удобном случае.

Подписавшие стороны просят страны в ООН «найти способ защитить нас от всех этих опасностей». Однако о запрете или регулировании новых технологий вооружений легче сказать, чем сделать. Оружие легче запретить, когда немногие страны имеют к ним доступ, когда они широко воспринимаются как ужасные, и когда они предоставляют небольшие военные льготы. Чрезвычайно сложно запретить оружие, которое считается решающим преимуществом, как ядерное оружие. Таким образом, основным фактором в том, что произойдет с автономным оружием, является то, как страны придут к тому, чтобы увидеть и понять выгоды и риски.

Автономное оружие представляет собой классическую дилемму для стран. Все страны могут быть лучше без них, но взаимная сдержанность требует сотрудничества. В прошлом страны

согласились создать более официальную Группу правительственных экспертов для изучения этого вопроса. Многие страны пытаются остановить потенциально опасную технологию до ее использования на войне.

Контрольные вопросы

1. Какие вызовы ждет международная безопасность?
2. Какие виды конфликтов появились в ходе 4-ой промышленной революции?
3. Какие изменения прогнозируются в военных действиях?

Дополнительные ресурсы по теме лекции

1. Cyber Warfare: Issues and Challenges Michael Robinsona, Kevin Jonesb , Helge Janickea, 2015.
2. Кибербезопасность на новом витке: готовимся противостоять киберугрозам 20-е международное исследование EY в области информационной безопасности за 2017–2018 годы: Николай Самодаев, 2017.
3. Цифровое сообщество готовится отражать кибератаки: Тим Клау, Роман Чаплыгин, 2018.

Глоссарий

Кибервойна – противоборство (война) и противостояние в кибернетическом пространстве (киберпространстве), в том числе компьютерное противостояние в Интернете, одна из разновидностей информационной войны.

Кибермошенничество (интернет-мошенничество) – это один из видов киберпреступления, целью которого является обман пользователей. Хищение конфиденциальных данных может привести к тому, что хакер незаконно получает доступ и каким-либо образом использует Вашу личную информацию, что предполагает мошенничество или обман.

Автономное оружие – нет единого международного согласованного определения, однако можно определить этот термин как оружие, которое самостоятельно обнаруживает цель, транспортирует боезапас или блок, выполняющий те или иные функции, до цели, а также самостоятельно обеспечивает выполнение целевой функции или решение боевой задачи.