Лекция №7

Лекция 7. Цифровая экономика и киберпространство

План лекции

- Киберпространство, определение
- Свойства киберпространства
- 4 слоя потоков киберпространства
- Цирфовые платформы: классификация
- Киберщит и кибербезопасность

Определение киберпространства может быть раскрыто в трех различных перспективах:

1) физический аспект киберпространства;

2) информационный аспект киберпространства;

3) социальный аспект киберпространства.

- С точки зрения физического или материального восприятия киберпространства, важным является наличие определенных устройств (компьютеры, смартфоны, средства виртуальной реальности и т.п.), посредством которых киберпространство создается и функционирует.
- Киберпространство – это виртуальное место, создаваемое сетью взаимосвязанных компьютеров, в котором взаимодействуют агенты

Цифровая экономика существует в отличие от реальной экономики в киберпространстве и зависит от ИКТ.

- Киберпространство – это виртуальная сетевая среда, сформированная в результате действий пользователей, программ и сервисов в сети связи общего пользования посредством сетей передачи данных, коммуникационных технологий и информационных систем.
- Реальное пространство способно развиваться само по себе, без вмешательства цифровых технологий.

Понятие гиперпространства как потоки капитала, информации и технологий

- Современное общество оформляется посредством бесконечного числа потоков капитала, информации и технологий.
- Кастельс в теории сетевого общества описывает новую пространственную логику – пространство потоков, которая противопоставлена укорененной пространственной организации нашего общего опыта – пространству мест.
- Кастельс определяет потоки как “целенаправленные, повторяющиеся, программируемые последовательности обменов и взаимодействий между физически разъединенными позициями, которые занимают социальные акторы в экономических, политических и символических структурах общества”.
- По мнению исследователя, можно выделить четыре материальных слоя пространства потоков (Кастельс М. Галактика Интернет. Екатеринбург, 2004. Кастельс М. Власть коммуникации. М., 2016). Дб дёчц1 йы яы 3ьтопц3оФЬ

- 1. **Первая материальная опора пространства потоков состоит из цепи электронных импульсов – технологическая инфраструктура** информационных систем, телекоммуникационных систем и транспортных линий (микроэлектроника, телекоммуникации, компьютерная обработка, системы вещания и высокоскоростного транспорта и т.д.).
- Пространство потоков конституируется сетью взаимодействий, а цели и задачи каждой сети образуют различные пространства потоков.
- К примеру, финансовые рынки, высокотехнологичное производство, сфера развлечений, новостные СМИ и т.п. образуют свои специфические технологические системы и различные территориальные профили.

Второй слой пространства потоков

- 2. **Второй слой пространства потоков состоит из узлов, хабов и коммуникационных центров**.
- Пространство потоков не лишено мест (Уолл-Стрит или Гиндза – это узлы торговли, Беркли, Стэнфорд – узлы науки).
- Хабы представляют собой места коммуникации (аэропорты, автобусные или железнодорожные станции).
- Функционирование хабов основано на электронной сети, но эта сеть связывает между собой конкретные места с четко очерченными социальными, культурными, физическими и функциональными характеристиками.
- Узлы и коммуникационные центры организованы иерархически в соответствии со своим весом в сети и сетевая иерархия является гибкой.
- Главные процессы в современном мире отчетливо фиксируются в сетях, которые имеют способность связывать различные физические места (локалии) и наделяют каждое из них определенной ролью и соответствующим весом в иерархии создания богатства, обработки информации и реализации властных полномочий,которые, в конечном счете, и обусловливают судьбу каждой локалии.

3. **Третий слой пространства потоков относится к пространственной организации властвующих менеджерских элит.**

- Пространство потоков является доминирующей пространственной логикой, поскольку отражает интересы элиты. Особенностью современной элиты является ее космополитичный характер.
- Пространства власти и богатства пронизывают весь мир, тогда как жизнь и опыт народов укоренен в конкретных местах, в их культуре, истории и жизненном укладе. Чем больше социальная организация основана на внеисторических потоках, вытесняющих логику любого конкретного места, тем больше логика глобальной власти уходит из-под контроля со стороны местных и национальных сообществ31.

4. **Пространство потоков содержит электронные пространства, такие как сайты в интернете, мессенджеры и т.п.** (это могут быть как однонаправленные, так и интерактивные потоки).

Именно этот слой пространства потоков характеризуется сегодня наибольшей динамикой развития, и оказывает определяющее воздействие

Характеристики киберпространства

- Виртуальность.
- Связь между киберпространством и сетью. Киберпространство нельзя отождествлять с сетью или описывать как совокупность данных, хранящихся на компьютерах, и предоставляемых через компьютерные сети. Однако киберпространство во многом зависит от функционирования информационно-коммуникационных сетей (преимущественно речь идет об интернете).
- Множественность связей сетевой структуры киберпространства
- Киберпространство является социальным пространством

Систематизированная классифкация цифровых платформ

Лекция 8

Воздействие ИКТ на региональное экономическое развитие

Особое внимание требует решение принципиально значимых вопросов, связанных с анализом перспектив реализации преимуществ цифровой экономики в разрезе регионов.

В этой связи становится вопрос о выявлении предпосылок и перспектив цифровизации экономики регионов Казахстана.

Воздействие ИКТ на региональное экономическое развитие осуществляется по двум основным направлениям:

Во-первых, в сфере производства цифровых продуктов и услуг ИКТ. Сегодня это одно из самых динамичных и инновационных отраслей экономики, оказывающая огромный вклад в инновационный рост, как регионов, так и страны в целом.

Во-вторых, в сфере потребления и внедрения ИКТ в различных сферах экономики и в области жизнедеятельности общества.

Это направление не менее важно, поскольку содействуют внедрению цифровых технологий. Например, повышение производительности, сокращение разнообразных трудозатрат и рутинных операций, повышение оперативности и качественного уровня обслуживания, улучшению качества жизни и др.

Задачи регулирования специализации экономики региона

основные программы, связанные с реализацией политики цифровизации экономики Казахстана:

- Стратегия индустриально-инновационного развития Республики Казахстана 2003-2015 годы;
- Программа по формированию и развитию национальной инновационной системы Республики Казахстана 2005-2015 годы;
- Государственная программа развития «электронного правительства» на 2008-2010 годы;
- - Программа развития отрасли телекоммуникаций Республики Казахстана 2006-2008 годы;
- - Программа снижения информационного неравенства в Республике Казахстана 2007-2009 годы;
- - Программы развития «электронного правительства» Республики Казахстан на 2008-2010 годы»;
- - Концепция формирования и развития единого информационного пространства казахстанского сегмента сети Интернет (Казнета) на 2008-2012 годы;

Схема реализации интересов Казахстана в сфере цифровой экономики

СИСТЕМЫ ИНДИКАТОРОВ И КРИТЕРИЕВ ОЦЕНКИ УРОВНЯ ИННОВАЦИОННОГО РАЗВИТИЯ РЕГИОНОВ

- интегрированные показатели оценки инновационной деятельности Комиссии Европейских сообществ (КЕС), используемые для сравнительного анализа оценки развития инновационной деятельности в странах ЕС;

- индикаторы технологической конкурентоспособности стран (Global Competitiveness Index, GCI), разработанные американским Национальным научным фондом (NSF);

- методические подходы оценки готовности и возможности стран к переходу на инновационную модель развития, разработанная Всемирным банком в рамках программы «Знания для развития» (на англ. Knowledge for Development, K4D;

- сводный индекс инновационного развития регионов США (на англ. Portfolio Innovation Index, PII), присваивающие различные весовые коэффициенты

СИСТЕМЫ ИНДИКАТОРОВ И КРИТЕРИЕВ ОЦЕНКИ УРОВНЯ ИННОВАЦИОННОГО РАЗВИТИЯ РЕГИОНОВ

- Различные международные организации разрабатывают собственные системы индикаторов и критериев оценки уровня инновационного развития регионов.
- В качестве наиболее часто используемых подходов, как в мировой практике, так при страновом сопоставлении, оценки ффективности инновационной среды отметим следующие:
- - индекс научно-технического потенциала (Technology Index, TI), разработан Всемирным экономическим форумом (ВЭФ), как составляющая интегрального показателя оценки уровня конкурентоспособности страны в глобальной экономике;

- В целом основная структура индикаторов оценки у странового и регионального инновационного мониторинга остается общей.
- Применение системы мониторинга инновационного потенциала на практике позволяет обоснованно пересмотреть стратегические ориентиры деятельности региона по внедрению инноваций и получить экономический эффект.
- В последние годы специализированной организацией ООН Международным союзом электросвязи (International Telecommunication Union, ITU) ежегодно рассчитывается уровень развития информационного общества в 167 странах мира.
- Важным результатом исследования считается подсчет комбинированного показателя - индекса развития ИКТ (ICT Development Index). Данный индекс был разработан в 2007 г. на основе 11 различных показателей. Казахстан в 2017 г. в данном рейтинге занимает 23-е место. Это говорит о том, что Казахстан обладает положительным уровнем развития ИКТ-сектора и значительным потенциалом в сфере цифровых ресурсов.

- Digitalization in the oil and gas industry is aimed not only at optimizing processes, but also at ensuring safety and improving operational efficiency. The oil and gas industry is in greater demand:
- Internet of Things: Used to monitor and control various production processes and collect data from various sensors and equipment in real-time.
- Big Data: Big data analysis can help companies make more informed decisions based on actual data, thereby improving efficiency and reducing costs.
- Artificial Intelligence (Artificial Intelligence): Used in exploration and remote management of oil production facilities, resulting in reduced costs and improved process efficiency.
- Machine Learning is used to improve the speed and accuracy of processing information streams coming from the field and enables integration and analysis of heterogeneous data, which helps improve operational performance
- Digital Twin is a virtual replica of physical assets used to model and optimize production processes and help reduce downtime, lower capital and operating costs, and improve the efficiency of companies' capital assets.

методический инструментарий (определяющий масштабы и уровень развития ИКТ), выполнен по алгоритму, состоящего из четырех этапов

.

- Первый этап – это оценка уровня использования интернета (доля пользователей сети интернет).
- Второй этап – оценка уровня затрат на производство ИКТ.
- Третий этап – оценка уровня цифровой грамотности населения (готовность населения к повсеместному использованию ИКТ).
- Четвертый этап - оценка уровня отраслевой специализации регионов в сфере ИКТ (выявление перспективных регионов в сфере ИКТ).

Концепция кибербезопасности

- Концепция кибербезопасности ("Киберщит Казахстана") разработана в соответствии с Посланием Президента Республики Казахстан "Третья модернизация Казахстана: Глобальная конкурентоспособность" с учетом подходов Стратегии "Казахстан-2050" по вхождению Казахстана в число 30-ти самых развитых государств мира.
- Концепция основана на оценке текущей ситуации в сфере информатизации государственных органов, автоматизации государственных услуг, перспектив развития "цифровой" экономики и технологической модернизации производственных процессов в промышленности, расширения сферы оказания информационно-коммуникационных услуг.
- Концепция определяет основные направления реализации государственной политики в сфере защиты электронных информационных ресурсов, информационных систем и сетей телекоммуникаций, обеспечения безопасного использования информационно-коммуникационных технологий.
- Концепция призвана обеспечить единство подходов к мониторингу обеспечения информационной безопасности государственных органов, физических и юридических лиц, а также выработку механизмов предупреждения и оперативного реагирования на инциденты информационной безопасности, в том числе в условиях чрезвычайных ситуаций социального, природного и техногенного характера, введения чрезвычайного или военного положения.

Кибербезопасность

- Киберпространство нуждается в защите
- Кибербезопасность (ее иногда называют компьютерной безопасностью) – это совокупность методов и практик защиты от атак злоумышленников для компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных.
- Кибербезопасность находит применение в самых разных областях, от бизнес-сферы до мобильных технологий. В этом направлении можно выделить несколько основных категорий.

Направления кибербезопасности

- **Безопасность сетей**– действия по защите компьютерных сетей от различных угроз, например целевых атак или вредоносных программ.
- **Безопасность приложений**– защита устройств от угроз, которые преступники могут спрятать в программах. Зараженное приложение может открыть злоумышленнику доступ к данным, которые оно должно защищать. Безопасность приложения обеспечивается еще на стадии разработки, задолго до его появления в открытых источниках.
- **Безопасность информации**– обеспечение целостности и приватности данных как во время хранения, так и при передаче.
- **Операционная безопасность**– обращение с информационными активами и их защита. К этой категории относится, например, управление разрешениями для доступа к сети или правилами, которые определяют, где и каким образом данные могут храниться и передаваться.

Направления кибербезопасности

- **Аварийное восстановление и непрерывность бизнеса** – реагирование на инцидент безопасности (действия злоумышленников) и любое другое событие, которое может нарушить работу систем или привести к потере данных.
- Аварийное восстановление – набор правил, описывающих то, как организация будет бороться с последствиями атаки и восстанавливать рабочие процессы. Непрерывность бизнеса – план действий на случай, если организация теряет доступ к определенным ресурсам из-за атаки злоумышленников.
- **Повышение осведомленности**– обучение пользователей. Это направление помогает снизить влияние самого непредсказуемого фактора в области кибербезопасности – человеческого.
- Даже самая защищенная система может подвергнуться атаке из-за чьей-то ошибки или незнания.
- Поэтому каждая организация должна проводить тренинги для сотрудников и рассказывать им о главных правилах: например, что не нужно открывать подозрительные вложения в электронной почте или подключать сомнительные USB-устройства.

Масштаб распространения киберугроз

- Год за годом в мире становится все больше угроз и происходит все больше утечек данных. И рост утечки информации из года в год возрастает в кратных размерах
- Чаще всего утечке данных подвергаются медицинские и государственные учреждения или организации из сферы розничной торговли.
- Некоторые организации привлекают злоумышленников по краже финансовых данных и медицинских данных.
- . По прогнозам Gartner, в целом расходы на кибербезопасность в мире достигнут $188,3 млрд в 2023 году, а к 2026 году превысят $260 млрд.
- Национальный институт стандартов и технологий США (National Institute of Standards and Technology, NIST) разработал принципы безопасной IT-инфраструктуры.
- NIST рекомендуют проводить постоянный мониторинг всех электронных ресурсов в реальном времени, чтобы выявить вредоносный код, пока он не нанес вреда, и предотвратить его распространение.
- Национальный центр кибербезопасности (National Cyber Security Centre) правительства Великобритании выпустил руководство 10 steps to cyber security (10 шагов к кибербезопасности).
- В Австралии рекомендации по борьбе с новейшими киберугрозами регулярно публикует Австралийский центр кибербезопасности (Australian Cyber Security Centre, ACSC).

Виды киберугроз

- Кибербезопасность борется с тремя видами угроз.

1. **Киберпреступление**– действия, организованные одним или несколькими злоумышленниками с целью атаковать систему, чтобы нарушить ее работу или извлечь финансовую выгоду.
2. **Кибератака** – действия, нацеленные на сбор информации, в основном политического характера.
3. **Кибертерроризм** – действия, направленные на дестабилизацию электронных систем с целью вызвать страх или панику.

- Как злоумышленникам удается получить контроль над компьютерными системами?
- Они используют различные инструменты и приемы – ниже мы приводим самые распространенные

- **Вредоносное ПО**
- Название говорит само за себя. Программное обеспечение, которое наносит вред, – самый распространенный инструмент киберпреступников. Они создают его сами, чтобы с его помощью повредить компьютер пользователя и данные на нем или вывести его из строя. Вредоносное ПО часто распространяется под видом безобидных файлов или почтовых вложений. Киберпреступники используют его, чтобы заработать или провести атаку по политическим мотивам.
- Вредоносное ПО может быть самым разным, вот некоторые распространенные виды:
- **Вирусы –** программы, которые заражают файлы вредоносным кодом. Чтобы распространяться внутри системы компьютера, они копируют сами себя.
- **Троянцы–** вредоносы, которые прячутся под маской легального ПО. Киберпреступники обманом вынуждают пользователей загрузить троянца на свой компьютер, а потом собирают данные или повреждают их.
- **Шпионское ПО –** программы, которые втайне следят за действиями пользователя и собирают информацию (к примеру, данные кредитных карт). Затем киберпреступники могут использовать ее в своих целях.
- **Программы-вымогатели** шифруют файлы и данные. Затем преступники требуют выкуп за восстановление, утверждая, что иначе пользователь потеряет данные.
- **Рекламное ПО –** программы рекламного характера, с помощью которых может распространяться вредоносное ПО.
- **Ботнеты –** сети компьютеров, зараженных вредоносным ПО, которые киберпреступники используют в своих целях.
- **SQL-инъекция**
- Этот вид кибератак используется для кражи информации из баз данных. Киберпреступники используют уязвимости в приложениях, управляемых данными, чтобы распространить вредоносный код на языке управления базами данных (SQL).
- **Фишинг**

Фишинг – атаки, цель которых – обманом заполучить конфиденциальную информацию пользователя (например, данные банковских карт или пароли). Часто в ходе таких атак преступники отправляют жертвам электронные письма, представляясь официальной организацией.

Атаки Man-in-the-Middle («человек посередине»)

Это атака, в ходе которой киберпреступник перехватывает данные во время их передачи – он как бы становится промежуточным звеном в цепи, и жертвы об этом даже не подозревают. Вы можете подвергнуться такой атаке, если, например, подключитесь к незащищенной сети Wi-Fi.

DoS-атаки (атаки типа «отказ в обслуживании»)

Киберпреступники создают избыточную нагрузку на сети и серверы объекта атаки, из-за чего система прекращает нормально работать и ею становится невозможно пользоваться. Так злоумышленники, например, могут повредить важные компоненты инфраструктуры и саботировать деятельность организации.

Новейшие киберугрозы

С какими из новейших киберугроз сталкиваются пользователи и организации? Рассмотрим некоторые из тех, что попали в отчеты правительств Великобритании, США и Австралии.

Троянец Dridex

В декабре 2019 года Министерство юстиции США обвинило лидера группы киберпреступников в участии в атаке с использованием зловреда Dridex. Эта кампания затронула общественные, правительственные и деловые структуры по всему миру.Dridex – банковский троянец с широким набором возможностей, который появился в 2014 году. Он проникает на компьютеры жертв с помощью фишинговых писем и вредоносных программ. Dridex может красть пароли, данные банковских карт и личную информацию пользователей, которые затем используют мошенники. Размер причиненного им финансового ущерба исчисляется сотнями миллионов.

Чтобы защититься, Национальный центр кибербезопасности Великобритании рекомендует устанавливать на устройства последние обновления безопасности и антивирусное ПО свежих версий, а также регулярно выполнять резервное копирование файлов.

- **Мошенничество на сайтах и в приложениях для знакомств**
- В феврале 2020 года ФБР предупредило граждан США о случаях мошенничества на сайтах знакомств, а также в чатах и приложениях. Эксплуатируя стремление найти партнера, киберпреступники выманивают у жертв личную информацию.
- Как следует из отчета ФБР, в 2019 году жертвами таких киберугроз стали 114 жителей штата Нью-Мексико, их финансовые потери составили около 1,6 миллиона долларов США.
- **Emotet**
- В конце 2019 года Австралийский центр кибербезопасности предупредил организации о распространении киберугрозы под названием Emotet.
- Emotet – сложно устроенный троянец, способный похищать данные, а также загружать вредоносное ПО на устройства. Его жертвами часто становились те, кто использовал простые пароли – это в очередной раз напомнило пользователям, что нужно использовать более сложные комбинации.

КОНЦЕПЦИЯ «КИБЕРЩИТ»

- Целью Концепции «КИБЕРЩИТ Казахстана» является достижение и поддержание уровня защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз, обеспечивающего устойчивое развитие Республики Казахстан в условиях глобальной конкуренции (О концепции «Киберщит»).

отчет по Глобальному индексу кибербезопасности.

- 29 июня 2021 года состоялась конференция Международного союза электросвязи (МСЭ) при ООН, в рамках которой опубликовали 4-е издание отчета по Глобальному индексу кибербезопасности.
- Так, по результатам проведенного анализа экспертами МСЭ ООН, Республика Казахстан поднялась на 9 позиций и занимает 31 место (ранее – 40-е) в Глобальном индексе кибербезопасности.
- В Региональном рейтинге Казахстан расположился на 2-м месте после Российской Федерации.
- Критериями рейтинга являются: законодательная база, технические и организационные мероприятия, деятельность на международной арене и создание потенциала для развития сферы кибербезопасности.
- Глобальный индекс кибербезопасности МСЭ является основным индикатором в сфере кибербезопасности в стратегических программах Республики Казахстан, таких как «Киберщит Казахстана» и «Цифровой Казахстан».

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ (DATA PROTECTION AGENCY)

- Общий регламент о защите данных (правила по обработке линых данных) является законом прямого действия в 28 странах Евросоюза.
- На основании общего регламента будет функционировать организация по Защите персональных данных (Data protection agency) в Казахстане.