Борьба с киберпреступностью

РЕГИОНАЛЬНАЯ РАБОЧАЯ ГРУППА НА УРОВНЕ ЭКСПЕРТОВ ПО ЦИФРОВОЙ ТОРГОВЛЕ ЦЕНТРАЛЬНОЙ АЗИИ

Вторник, 6 сентября | День 2

Кеонг Мин Юн, советник, Всемирный банк

THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP

ОБЗОР

1. Развитие и киберпреступность
2. Создание правовых рамок для борьбы с киберпреступностью
3. Законодательная база
4. Международное сотрудничество
5. Государственно-частное сотрудничество

1.РАЗВИТИЕ И КИБЕРПРЕСТУПНОСТЬ

Создание благоприятной среды для цифровой экономики

ВВЕДЕНИЕ

Киберпреступность представляет собой угрозу мировой экономике, а также миру и безопасности
- Правительства должны реагировать путем эффективного обучения, адаптивной правовой базы, улучшения обмена информацией и постоянных программ по работе с общественностью.

Киберпространство — виртуальный мир, неотделимый от реального, физического мира.

Киберпреступность — преступное поведение в киберпространстве, направленное против конфиденциальности, целостности и доступности данных, технологий и компьютерных систем.

Кибербезопасность — набор инструментов, политик, руководств, подходов к управлению рисками, действий, обучающих материалов, лучших практик, гарантий и технологий, которые можно использовать для защиты доступности, целостности и конфиденциальности активов в подключенных инфраструктурах, относящихся к правительству., частным организациям и гражданам.

ГЛОБАЛЬНЫЕ ТЕНДЕНЦИИ В ОБЛАСТИ КИБЕРПРЕСТУПНОСТИ

Трансграничный поток данных
- Облачные вычисления

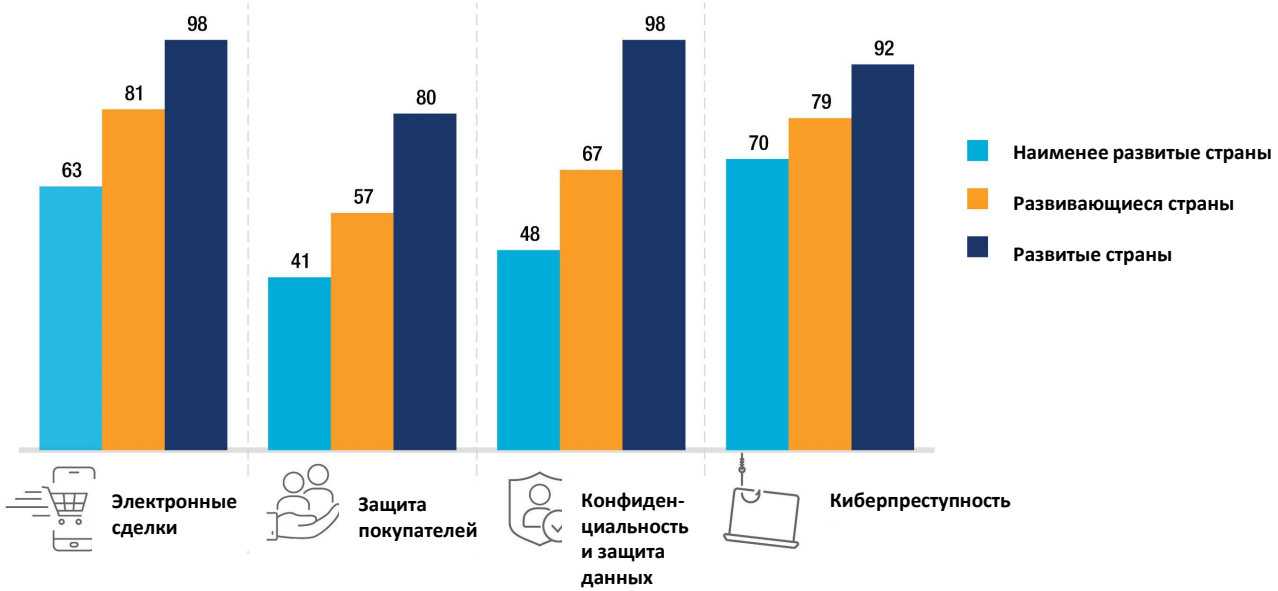
Восстановление активов
- Криптовалюта и даркнет

Потребительская чувствительность и ориентация на человека

Права
- Государственно-частное сотрудничество

Новые технологии
- ИИ, блокчейн, Интернет вещей и т. д.

Вставка D0.1: Принятие закона о кибербезопасности в 2021 г. (доля стран, процентное соотношение)



ЮНКТАД

РАЗВИТИЕ И КИБЕРПРЕСТУПНОСТЬ

Интернет стал очень важным для экономического развития

Киберпространство – виртуальный мир, неотделимый от реального, физического мира

Информационно-коммуникационные технологии (ИКТ) играют неотъемлемую роль в поддержании и управлении обществом

- здания, автомобили, авиационные услуги, источники питания и т. д.

Растущая зависимость от ИКТ означает увеличение числа киберугроз, рисков и уязвимостей

- *Отсутствие контроля может привести к уязвимостям для пользователей, предприятий и критически важной инфраструктуры*

РАЗВИТИЕ И КИБЕРПРЕСТУПНОСТЬ

Развивающиеся страны наиболее уязвимы для киберпреступности

- Нужны возможности для борьбы с киберпреступностью
- Рост и совершенствование киберпреступников

https://policyaccelerator.uncdf.org/policy-tools/brief-cybersecurity-digital-economy

КИБЕРПРЕСТУПНОСТЬ И ВСЕМИРНЫЙ БАНК

Международный институт развития, созданный в соответствии с его статьями соглашения

- Сокращение бедности, улучшение условий жизни и содействие устойчивому и всестороннему развитию во всем мире
- Оказание финансовой помощи странам для восстановления после Второй мировой войны

Финансовое учреждение с рейтингом AAA, акционерами которого являются суверенные правительства

- Имеет две цели: искоренить крайнюю нищету и способствовать всеобщему процветанию

КИБЕРПРЕСТУПНОСТЬ И ВСЕМИРНЫЙ БАНК

Всемирный банк поддерживает развивающиеся страны в различных секторах таких, как ИКТ, транспорт, городское планирование, энергетика, здравоохранение, образование и социальная защита

- Примечательно, что подавляющее большинство проектов содержат компоненты ИКТ

Наряду с ключевыми партнерскими организациями ВБ предлагает многоаспектный подход

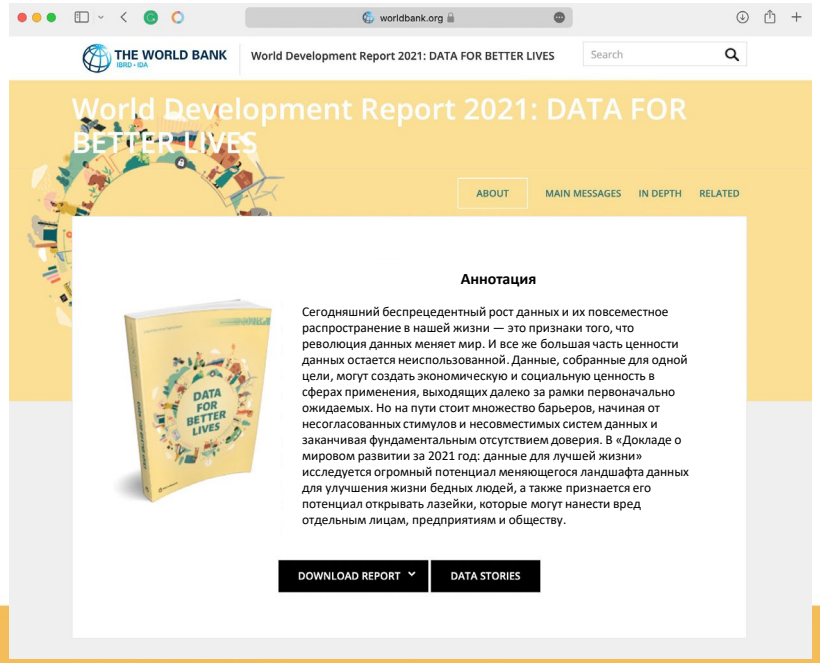
- Транснациональное сотрудничество между суверенными государствами

Киберпреступность и цифровая экономика

Политики, законы и правила в отношении данных: создание среды доверия

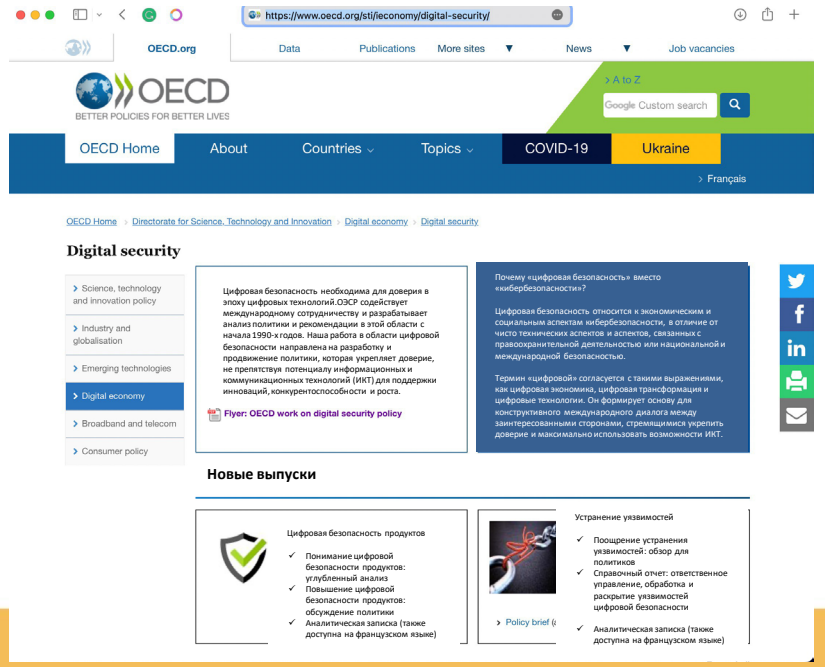
Основные идеи

1. Доверие к сделкам с данными поддерживается надежной нормативно-правовой базой, включающей как средства защиты, предотвращающие неправомерное использование данных, так и средства реализации, облегчающие доступ к данным и их повторное использование.
2. Меры предосторожности должны различать личные данные, требующие правового подхода с индивидуальной защитой, и неличные данные, что позволяет сбалансировать интересы при повторном использовании данных.
3. Механизмы совместного использования данных, как правило, более развиты в отношении данных, предназначенных для государственных целей, где государственная политика и законодательство, предписывающие доступ к данным и совместное использование, устанавливаются легче, чем в случае данных, предназначенных для частных целей, где влияние правительства более ограничено.
4. Работа по созданию атмосферы доверия ведется во всем мире, особенно в странах с низким уровнем дохода. Не существует универсальной нормативно-правовой базы. В странах со слабой нормативно-правовой базой может потребоваться тщательная адаптация разработки подходящих защитных и вспомогательных средств к местным приоритетам и возможностям.



https://www.worldbank.org/en/publication/wdr2021

Цифровая безопасность ОЭСР



Эффективная политика цифровой безопасности необходима для роста и благополучия

ОЭСР представляет собой уникальный форум для разработки и продвижения основанного на фактических данных анализа политики и рекомендаций по укреплению безопасности и доверия без ущерба для преимуществ цифровой трансформации и ее потенциала для повышения благосостояния, инноваций и роста. ОЭСР находится в авангарде усилий, направленных на содействие международному сотрудничеству в области политики цифровой безопасности с 1990-х годов. ОЭСР уделяет внимание экономическим и социальным аспектам кибербезопасности, а не чисто техническим аспектам, непосредственно связанным с правоохранительной деятельностью или национальной безопасностью.

Подход ОЭСР к цифровой безопасности основан на управлении рисками и фокусируется на определении наиболее эффективных инструментов политики для решения экономических и социальных проблем, которые часто ограничивают способность заинтересованных сторон оптимально управлять рисками цифровой безопасности. Эти проблемы включают, например, нехватку навыков и талантов, отсутствие инноваций в области цифровой безопасности, нечеткое распределение ролей и обязанностей между экономическими субъектами, несогласованные рыночные стимулы, информационную асимметрию, а также культурные и правовые барьеры для эффективного трансграничного сотрудничества. и группы заинтересованных сторон. Работа ОЭСР над политикой цифровой безопасности:

- Осуществляется через Рабочую группу по безопасности в цифровой экономике (SDE);
- Основана на результатах Глобального форума по цифровой безопасности для процветания; а также
- Поддерживает разработку Рекомендаций ОЭСР по политике цифровой безопасности.

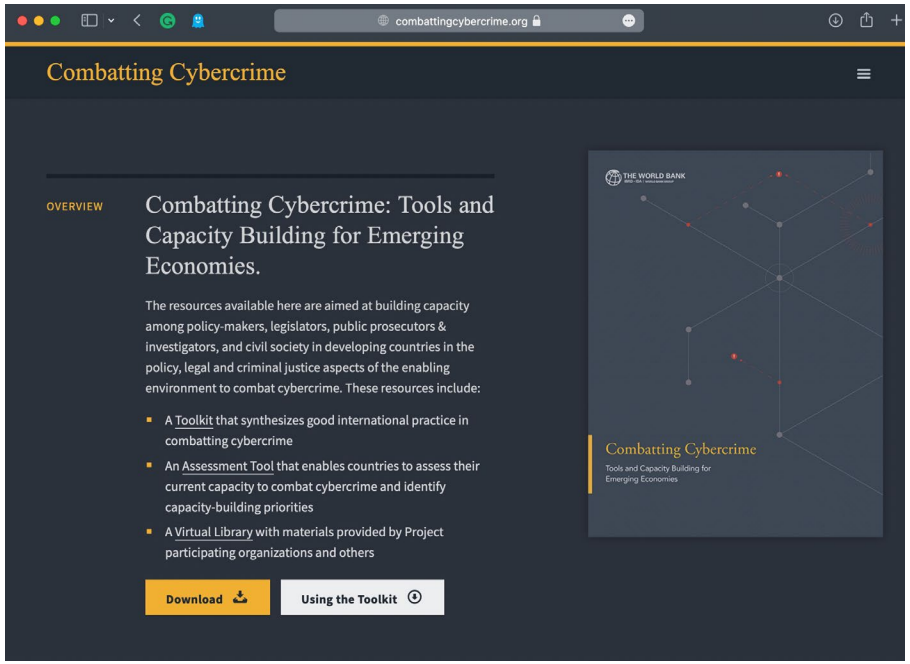
https://www.oecd.org/sti/ieconomy/digital-security/

ПРОЕКТ ВБ ПО БОРЬБЕ С КИБЕРПРЕСТУПНОСТЬЮ

Направлен на повышение потенциала политиков, законодателей, судей, юристов, прокуроров, следователей и гражданского общества по различным юридическим и неюридическим вопросам, связанным с борьбой с киберпреступностью.

Проект состоит из четырех частей:

- Инструментарий
  - Обобщает передовую международную практику борьбы с киберпреступностью и организован по девяти измерениям.
- Обучающий материал
  - Дает более краткое объяснение девяти аспектов с рекомендациями, примерами, случаями и новыми тенденциями.
- Инструмент оценки
  - Позволяет странам оценить свой текущий потенциал по борьбе с киберпреступностью и определить приоритеты в наращивании потенциала, а также выделить ограниченные ресурсы для наращивания потенциала
- Виртуальная библиотека
  - Предлагает материалы, предоставленные организациями-участниками проекта



7 АСПЕКТОВ ПРОЕКТА ПО БОРЬБЕ С КИБЕРПРЕСТУПНОСТЬЮ

7 основных аспектов борьбы с киберпреступностью

1. Рамочная политика
2. Материальное право
3. Процессуальное право
4. Благоприятные условия
5. Меры безопасности
6. Международное сотрудничество
7. Наращивание потенциала

ЛОГИКА СЕМИ АСПЕКТОВ ПРОЕКТА ПО БОРЬБЕ С КИБЕРПРЕСТУПНОСТЬЮ

Страны, начинающие борьбу с киберпреступностью, как правило, сосредотачиваются на аспекте «криминализации».

- Однако существуют и другие правовые нормы и неправовые системы, которые также важны и необходимы.
  - Например, хорошо разработанные статуты законов о киберпреступности не могут применяться без достаточных ресурсов для сбора и анализа электронных доказательств.

Обобщенные знания и опыт различных организаций в мире и их классификация по 7 аспектам:

- Для успешной борьбы с киберпреступностью ограниченные ресурсы должны быть адекватно распределены по каждому из 7 аспектов.
- В каждом аспекте представлены концепции, примеры, случаи и новые тенденции, а также рекомендации по наращиванию потенциала.

ПАРТНЕРСКИЕ ОРГАНИЗАЦИИ

Партнерские организации проекта

- Совет Европы (CE)
- Международная ассоциация уголовного права (AIDP)
- Глобальный форум киберэкспертизы (GFCE)
- Международный союз электросвязи (МСЭ)
- ИНТЕРПОЛ
- Верховная прокуратура Кореи (KSPO)
- Оксфордский центр повышения квалификации в области кибербезопасности (Оксфорд)
- Конференция ООН по торговле и развитию (ЮНКТАД)
- Межрегиональный научно-исследовательский институт ООН по вопросам преступности и правосудия (ЮНИКРИ)

Финансируется за счет гранта Министерства стратегии и финансов Кореи в рамках Целевого фонда партнерства Кореи и Всемирного банка (KWPF).

2. СОЗДАНИЕ ПРАВОВЫХ РАМОК ДЛЯ БОРЬБЫ С КИБЕРПРЕСТУПНОСТЬЮ

Первый шаг к борьбе с киберпреступностью

ОБОСНОВАНИЕ И ЦЕЛИ СИСТЕМЫ БОРЬБЫ С КИБЕРПРЕСТУПНОСТЬЮ

Цель: повышение готовности субъектов уголовного правосудия к различным формам киберпреступности

Обширный объем данных и транснациональный характер киберпреступности требуют:

- Развитие способности бороться не только с электронной формой киберпреступности, но и с ее международным аспектом
  - Например, получение, сохранение и защита электронных доказательств требует специального набора знаний
- Сотрудничество на всех уровнях:
  - Государственно-частное (в частности, правоохранительные органы/интернет-провайдер) и международное сотрудничество

НОРМАТИВНАЯ БАЗА КАК НАЧАЛО БОРЬБЫ С КИБЕРПРЕСТУПНОСТЬЮ

1-й шаг к борьбе с киберпреступностью

Ключевые элементы

- Политический инструмент
  - Национальная стратегия кибербезопасности (NCS)
- Институциональное управление
  - Централизованная координация борьбы с киберпреступностью
  - Организационные и координирующие органы

ПРИМЕР: UK NCS 2016-2021

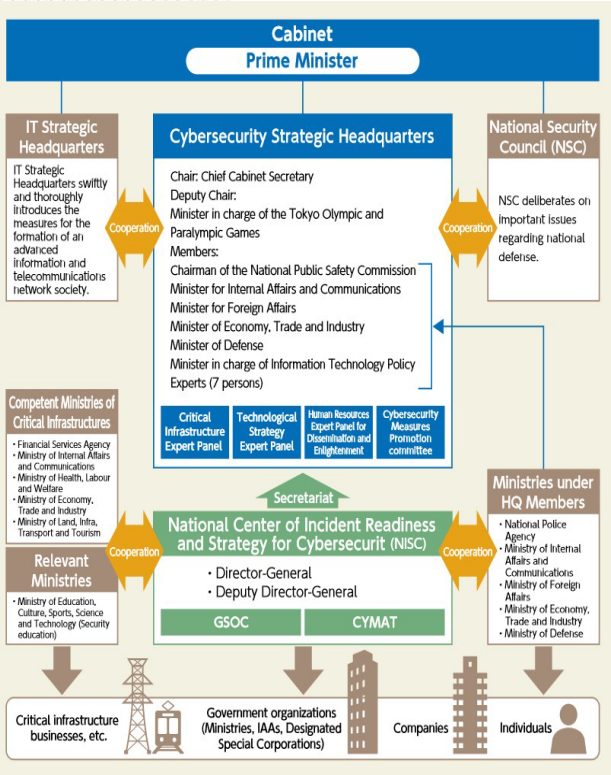
National Cyber Security Centre
a part of GCHQ

Национальный центр кибербезопасности
Часть Центра британской правительственной связи (GCHQ)

ЧЕТЫРЕ БОЛЬШИХ И ОСНОВНЫХ ЦЕЛИ

1. ***Борьба с киберпреступностью,***
2. ***Повышение устойчивости к кибератакам***
3. ***Помощь в формировании и открытии киберпространства***
4. ***Устранение разрозненности***

ИНСТИТУЦИОНАЛЬНОЕ УПРАВЛЕНИЕ: ИНСТИТУЦИОНАЛЬНАЯ ОСНОВА КИБЕРБЕЗОПАСНОСТИ ЯПОНИИ



Централизованная координация борьбы с киберпреступностью
Национальных центр киберзащиты
Группа реагирования на компьютерные инциденты (CIRT)

Кабинет премьер-министра - Стратегический штаб ИТ -Стратегический штаб ИТ оперативно и обстоятельно внедряет меры по формированию передового информационно-телекоммуникационного сетевого общества. <Сотрудничество> Стратегический штаб кибербезопасности - Председатель: главный секретарь кабинета министров - Заместитель председателя: Министр, отвечающий за Олимпийские игры в Токио и Председатель Национальной комиссии общественной безопасности - Министр внутренних дел и коммуникаций - Министр иностранных дел - Министр экономики, торговли и промышленности - Министр обороны - Министр по политике в области информационных технологий - Эксперты (7 человек) - Группа экспертов по критической инфраструктуре - Экспертный совет по технологической стратегии - Экспертная группа по кибербезопасности отдела кадров для гаспространения и просвещения - Комитет по продвижению мер кибербезопасности <Сотрудничество> Совет национальной безопасности (СНБ) - СНБ обсуждает важные вопросы, касающиеся национальной защиты. Компетентные министерства важнейших инфраструктур - Агентство финансовых услуг - Министерство внутренних дел и коммуникаций - Министерство здравоохранения, труда и социального обеспечения - Министерство экономики, торговли и промышленности - Министерство земли, инфраструктуры, транспорта и туризма - Соответствующие министерства - Министерство образования, культуры, спорта, науки и технологий (Обучение безопасности) - Предприятия критической инфраструктуры и т.д. <Сотрудничество> Секретариат - Национальный центр готовности к инцидентам и стратегии кибербезопасности (NISC)• Генеральный директор• Заместитель генерального директора – GSOC – CYMAT - Государственные организации (АА, специальные корпорации) – Компании <Сотрудничество>Министерства при членах штаб-квартиры- Национальное полицейское агентство- Министерство внутренних дел и коммуникаций- Министерство иностранных дел- Министерство экономики, торговли и промышленности• Министерство обороны - Физические лица

ИНСТИТУЦИОНАЛЬНАЯ ОСНОВА ДЛЯ БОРЬБЫ С КИБЕРПРЕСТУПНОСТЬЮ КОРЕИ

Категории	Ответственные агентства	Соответствующие законы
Информационная и коммуникационная политика	Министерство науки, ИКТ и планирования будущего Комиссия по связи Кореи	Закон о содействии использованию информационно-коммуникационных сетей и защите информации Закон о цифровой подписи Закон о защите, использовании и т. д. информации о местоположении
Кибербезопасность	Министерство науки, ИКТ и планирования будущего (для частного сектора) K/CERT Национальная разведывательная служба (для государственного сектора)	Закон о защите информации и коммуникационной инфраструктуры Закон о содействии использованию информационно-коммуникационных сетей и защите информации
Защита пользователей	Министерство внутренних дел Комиссия по связи Кореи Комиссия по финансовым услугам	Закон о защите личной информации Закон о содействии использованию информационно-коммуникационных сетей и защите информации Специальный закон о возмещении суммы ущерба, причиненного телекоммуникациями
Киберпреступность	Национальное полицейское агентство Прокуратура Министерство юстиции	Банковское мошенничество Уголовный закон Уголовно-процессуальный закон Закон о защите тайны обмена информацией

КЛЮЧЕВЫЕ ЭЛЕМЕНТЫ ПОЛИТИКИ И СТРАТЕГИИ В ОТНОШЕНИИ КИБЕРПРЕСТУПЛЕНИЙ

1. Вовлеченные лица, принимающие решения

2. Синергетические стратегии кибербезопасности

3. Многостороннее участие в разработке стратегии

4. Подходы поддерживают права человека и требования верховенства закона

5. Стратегии киберпреступности требуют вертикального и горизонтального управления

6. Согласование взносов доноров и партнерского сотрудничества

3. ЗАКОНОДАТЕЛЬНАЯ БАЗА

Многомерность законов о киберпреступности

МЕЖДУНАРОДНЫЕ ПРАВОВЫЕ ТЕНДЕНЦИИ

Специальный комитет по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях

2-й протокол к Будапештской конвенции

Шремс II

Двусторонние соглашения (Закон США об облачных технологиях)

ЗАКОНОДАТЕЛЬНАЯ БАЗА ДЛЯ КИБЕРПРЕСТУПЛЕНИЙ

ЗАКОНЫ

- (1) Управление поведением в киберпространстве и
- (2) Установление стандартизированных процедур

Задача

- Глобальная совместимость и гармонизация национальных законов

РОЛЬ ЗАКОНОДАТЕЛЬНОЙ БАЗЫ

Создает санкции за нарушение законов

Защищает владельцев и пользователей ИКТ, предотвращая причинение вреда людям, имуществу, данным, услугам и инфраструктуре

Признает и защищает права человека

Обеспечивает надлежащее расследование и судебное преследование конкретных преступлений, а также

Обеспечивает сотрудничество между странами в преследовании и наказании киберпреступников

ОГРАНИЧЕНИЯ ТРАДИЦИОННОГО УГОЛОВНОГО ЗАКОНОДАТЕЛЬСТВА

НЕ МОЖЕТ всегда охватывать уникальные технологические аспекты киберпреступности

«[конкретное и обширное законодательство о киберпреступности обеспечит судебную последовательность…, а также облегчит соблюдение закона».

РАЗРАБОТКА ЗАКОНОДАТЕЛЬСТВА О КИБЕРПРЕСТУПЛЕНИЯХ

Центральная часть развития потенциала страны по борьбе с киберпреступностью и повышения оперативной совместимости

Должна поддерживаться другими заинтересованными сторонами, государственными и частными, в соответствующей адаптации, адресности и формулировках любого такого законодательства

ПЯТЬ АСПЕКТОВ ЗАКОНОДАТЕЛЬНОЙ БАЗЫ

1. Материальное право
2. Процессуальное право
3. Закон об электронных доказательствах
4. Юрисдикция
5. Меры безопасности

УСЛОВИЯ И ГАРАНТИИ ЕСПЧ

Условия, которые необходимо соблюдать при ограничении прав - Конвенция Совета Европы о защите прав человека и основных свобод (ЕСПЧ)

Исключительная компетенция закона (правовая основа)

Необходимость преследовать законную цель (законная цель)
«Необходимость вмешательства в демократическое общество»… что означает, что вмешательство должно:

- Соответствовать «насущной общественной потребности» (необходимость)
- Быть соразмерным преследуемой цели (соразмерность)

Требования, вытекающие из принципов «необходимости» и «соразмерности», можно отнести к тому или иному понятию.

Источник: Совет Европы (CoE)

ЗАКОННОЕ ОСНОВАНИЕ

Уголовные кодексы должны быть «доступными, понятными и предсказуемыми»

- «Известно и предсказуемо»

Для предъявления обвинения подсудимому должны быть «правовые основания»

- Конкретный закон или постановление, публично устанавливающее и четко определяющее незаконность лежащего в его основе поведения

ЗАКОННАЯ ЦЕЛЬ

Предпосылка для ограничения правительством осуществления или выражения основных прав человека.

«Законная цель» обычно включает следующее:

- Общественная безопасность
- Здоровье и нравственность населения
- Содействие экономическому благополучию общества
- Национальная безопасность, а также
- Защита прав меньшинств и наиболее уязвимых членов общества

США: ЗАКОН О СОХРАНЕННЫХ СООБЩЕНИЯХ (SCA)

Пять случаев, когда достаточно убедительные обстоятельства оправдывают тайное вторжение правительства в личную учетную запись электронной почты человека:

- (1) «Угроза жизни или физической безопасности человека»;
- (2) «Бегство от судебного преследования»;
- (3) «Уничтожение или подделка улик»;
- (4) «Запугивание потенциальных свидетелей»; а также
- (5) «Серьезно ставящий под угрозу расследование или неоправданно затягивающий судебное разбирательство».

ДОСТАТОЧНОСТЬ

Гарантии должны оставаться применимыми к конкретным обстоятельствам

- Принимая во внимание права, защищаемые в соответствии с внутренними и международными правовыми обязательствами государства
  - Как внутренние, так и международные обязательства

БУДАПЕШТСКАЯ КОНВЕНЦИЯ: СТ. 15

Статья 15. Условия и гарантии

- Каждая Сторона обеспечивает, чтобы установление, осуществление и применение полномочий и процедур, предусмотренных в настоящем Разделе, регулировались условиями и гарантиями, предусмотренными ее внутренним законодательством, которые обеспечивают надлежащую защиту прав и свобод человека, включая права, возникающие в соответствии с обязательствами, взятыми на себя согласно Конвенции Совета Европы о защите прав человека и основных свобод 1950 г., Международным пактом Организации Объединенных Наций о гражданских и политических правах 1966 г. и другими применимыми международными договорами о правах человека, и которые включают принцип соразмерности.

ПРОПОРЦИОНАЛЬНОСТЬ

Связь между целью, которую необходимо достичь, и средствами, используемыми для достижения этой цели.

- Полномочия и процедуры расследования должны оставаться «пропорциональными» обстоятельствам.

СВЕРХКРИМИНАЛИЗАЦИЯ

Чрезмерное распространение уголовного права на действия, которые «ненадлежащим образом или безответственно применяются такими мерами», например:

- Законодательство о морали без идентифицируемой жертвы
- Политически мотивированные законы

НЕОБХОДИМОСТЬ

Европейский суд по правам человека:

- Вмешательство допустимо только в том случае, если оно «необходимо в демократическом обществе».
  - Наличие «насущной социальной потребности» и «уместных и достаточных» причин.

Обеспечение того, чтобы влияние полномочий и процедур на права, обязанности и законные интересы привлеченных и третьих лиц соответствовало общественным интересам.

СУДЕБНЫЙ / НЕЗАВИСИМЫЙ НАДЗОР

Традиционная защита в верховенстве закона

- «[Необходимым] для верховенства закона в любой стране является наличие независимой судебной системы, судей, не находящихся под контролем других ветвей власти и, следовательно, способных беспристрастно применять закон».

Обеспечение законности законов и укрепление легитимности правительства за счет разрешения «отдельным судьям… основывать свои решения исключительно на законах и фактах отдельных дел».

Судебные органы = нейтральные и обособленные органы

- Надзор за объемом и продолжительностью полномочий или процедур
- Мониторинг честности и соблюдения процедур и полномочий

ГАРМОНИЗАЦИЯ НАЦИОНАЛЬНОГО ЗАКОНОДАТЕЛЬСТВА

Международная гармонизация и интероперабельность внутренних законов не позволяют киберпреступности стать безопасным убежищем.

- Международная гармонизация материального права и процессуального права
  - Устраняет препятствия для глобального сбора доказательств и обмена ими
- Общие процессуальные правила
  - обеспечить, чтобы электронные доказательства, собранные в одной юрисдикции, соответствовали стандартам допустимости в другой

Законы многих стран уже содержат положения, обеспечивающие более эффективное международное сотрудничество.

4. МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО

Преодоление проблем юрисдикционного характера

МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО

Международное сотрудничество является важнейшим аспектом международного мира и гармонизации и поддерживает

(i) Наращивание потенциала;

(ii) Обмен информацией, опытом, учебными программами, исследованиями и техническими знаниями, передовым опытом расследования и судебного преследования киберпреступлений и передачу вышеперечисленного; а также

(iii) Техническую и экономическую помощь

ВЫЗОВЫ, СВЯЗАННЫЕ С ТРАНСНАЦИОНАЛЬНЫМ ХАРАКТЕРОМ КИБЕРПРЕСТУПНОСТИ

Внутренние правоохранительные органы не могут продвигать уголовное судопроизводство, когда преступники, а также ключевые доказательства, свидетели и потерпевшие находятся за пределами их юрисдикции.

ПРИНЦИП ДВОЙНОЙ ПРЕСТУПЛЕННОСТИ

Требование о том, чтобы предполагаемое деяние, являющееся предметом официального запроса об экстрадиции или соглашения о взаимной правовой помощи (ВПП), также квалифицировалось как уголовное преступление в соответствии с уголовным законодательством как государства, направляющего запрос, так и государства, чье содействие запрашивается.

Одно из самых больших препятствий юрисдикционного характера для расследования киберпреступлений и судебного преследования

Двойная преступность «существует, если правонарушение является преступлением как по законам запрашиваемой стороны, так и по законам запрашивающей стороны».

Барьеры:

- Юрисдикциям труднее, чем когда-либо, поддерживать актуальные и единообразные определения киберпреступлений.
- Часто существуют пробелы между различными юрисдикциями, что может привести к отказу в экстрадиции преступников.

ПРЕОДОЛЕНИЕ ПРОБЛЕМ, СВЯЗАННЫХ С ТРАНСНАЦИОНАЛЬНЫМ ХАРАКТЕРОМ КИБЕРПРЕСТУПЛЕНИЙ

1. Официальное международное сотрудничество
   - Многосторонние договоры о киберпреступности, договоры о взаимной правовой помощи и договоры о выдаче

2. Неформальное международное сотрудничество
   - Различные формы сотрудничества, которые обычно носят более практический и личный характер и осуществляются на оперативном уровне между правительствами.

ТРИ ЗАДАЧИ УСТАНОВЛЕНИЯ ОФИЦИАЛЬНОГО МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА

1. Заполнение пробелов в национальном уголовном законодательстве против транснациональной киберпреступности;

2.Предложение процессуальных полномочий там, где страны не имеют надлежащего оборудования для борьбы с киберпреступностью; а также

3.Разработка обязательных к исполнению положений о взаимной правовой помощи, которые упростили бы и ускорили обмен информацией и помощь в вопросах, связанных с киберпреступностью.

ГЛОБАЛЬНЫЙ ЛАНДШАФТ ОФИЦИАЛЬНОГО МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА

Во всем мире более восьмидесяти государств подписали и/или ратифицировали один или несколько обязательных документов о киберпреступности, и многие из этих государств имеют национальное законодательство о киберпреступности.

- (A) Многосторонние договоры

Помимо многосторонних договоров, страны подписали двусторонние договоры и соглашения напрямую.

- (B) Договоры о взаимной правовой помощи (MLAT)
- (C) Договоры о выдаче
- (D) Соглашения об облачных технологиях

МНОГОСТОРОННИЕ ДОГОВОРЫ О КИБЕРПРЕСТУПНОСТИ

a. БУДАПЕШТСКАЯ КОНВЕНЦИЯ О КИБЕРПРЕСТУПНОСТИ (БУДАПЕШТСКАЯ КОНВЕНЦИЯ) 2001 ГОДА
b. СОГЛАШЕНИЕ О СОДРУЖЕСТВЕ НЕЗАВИСИМЫХ ГОСУДАРСТВ (СНГ)
c. СОГЛАШЕНИЕ О ШАНХАЙСКОЙ ОРГАНИЗАЦИИ СОТРУДНИЧЕСТВА (ШОС)
d. КОНВЕНЦИЯ ЛИГИ АРАБСКИХ ГОСУДАРСТВ О БОРЬБЕ С ПРЕСТУПЛЕНИЯМИ В ОБЛАСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ (АРАБСКАЯ КОНВЕНЦИЯ)
e. КОНВЕНЦИЯ АФРИКАНСКОГО СОЮЗА О КИБЕРБЕЗОПАСНОСТИ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ (КОНВЕНЦИЯ АС)
f. ДОГОВОР ООН О ПРОТИВОДЕЙСТВИИ ИСПОЛЬЗОВАНИЮ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В ПРЕСТУПНЫХ ЦЕЛЯХ

РОЛЬ МНОГОСТОРОННИХ ДОГОВОРОВ О КИБЕРПРЕСТУПНОСТИ

Гармонизация национальных законов

Развитие возможностей для проведения расследований киберпреступлений

Продвижение и укрепление международного сотрудничества

Предоставление подписавшим сторонам рекомендаций по реализации национальных мер

Договор о взаимной правовой помощи для тех государств, у которых еще нет соглашения с государством-участником, нуждающимся в помощи

БУДАПЕШТСКАЯ КОНВЕНЦИЯ О КИБЕРПРЕСТУПНОСТИ (БУДАПЕШТСКАЯ КОНВЕНЦИЯ) 2001 ГОДА

Важнейший международный документ о киберпреступности

- Открыт для подписания государствами-членами, не входящими в Совет Европы (СЕ)

Предлагает руководство для государств-членов по созданию и гармонизации своего национального законодательства о киберпреступности

Имеет обязательную юридическую силу для государств-членов

Четкое определение уголовных преступлений как сбалансированных с процессуальными гарантиями

Присоединение государств, не входящих в СЕ, ограничено теми, кто «приглашен» при единодушном согласии договаривающихся сторон Конвенции

ПОЛОЖЕНИЯ БУДАПЕШТСКОЙ КОНВЕНЦИИ О ВПП

Обязывает стороны обеспечить наличие процессуальных инструментов для расследования перечисленных преступлений, а также других преступлений, не перечисленных в Конвенции.

- Признание важности электронных расследований по любому виду преступлений и на любой стадии развития.
  - Например, данные мобильного телефона
- Процедурные инструменты Конвенции предназначены для предотвращения нарушений суверенитета и прав человека, но при этом позволяют государствам должным образом расследовать преступления.

Достигает значительных успехов в повышении своевременности рассмотрения между сторонами дел о киберпреступлении

Требование к каждому государству создать «сеть 24/7»

ВТОРОЙ ДОПОЛНИТЕЛЬНЫЙ ПРОТОКОЛ К БУДАПЕШТСКОЙ КОНВЕНЦИИ (2-й ПРОТОКОЛ)

Решает проблемы, обеспечивая более широкое международное сотрудничество, сосредоточивая внимание на 4 ключевых элементах:

- Меры по совершенствованию международного сотрудничества между правоохранительными и судебными органами, в том числе по правовой помощи между органами («взаимная правовая помощь»);
- Сотрудничество между органами власти и поставщиками услуг в других странах;
- Условия и гарантии доступа к информации органов власти других стран; а также
- Другие меры безопасности, включая требования по защите данных

ОБЛАСТИ УЛУЧШЕНИЯ ОФИЦИАЛЬНЫХ МЕЖДУНАРОДНЫХ СОГЛАШЕНИЙ

Интеграция

Многосторонний подход

Учет извлеченных уроков

Преодоление постоянных ограничений в масштабе

Осуществление на национальном уровне

Международные инструменты усугубляют разногласия между государствам

Меры предосторожности

МЕСТО ДЛЯ НЕФОРМАЛЬНОГО СОТРУДНИЧЕСТВА

Неофициальные механизмы международного сотрудничества необходимы для заполнения пробелов, которые не могут быть устранены с помощью официальных механизмов.

Правительства, международные организации и неправительственные организации (НПО) в равной степени предложили различные варианты, поддерживающие международную интероперабельность.

- Пример: принятие Генеральной Ассамблеей ООН резолюции, касающейся законодательства о компьютерных преступлениях (1990 г.)
- Пример: выпуск Коммюнике министров «Большой восьмерки», которое включало план действий и принципы борьбы с киберпреступностью, а также защиты данных и систем от несанкционированного доступа (1997 г.)
- Пример: Всемирный саммит по вопросам информационного общества (ВВУИО) опубликовал Женевскую декларацию принципов и План действий (2003 г.)

Министерство юстиции США (DoJ) использует термин «оперативное сотрудничество между полицией», а не «неформальное сотрудничество», чтобы подчеркнуть, что такое сотрудничество разрешено внутренним законодательством.

НЕФОРМАЛЬНЫЕ МЕХАНИЗМЫ СОТРУДНИЧЕСТВА

Различные формы и практики «неформального» международного сотрудничества в контексте киберпреступности включают:

- Сети 24/7, работающие круглосуточно и без выходных
- Центры обмена информацией и координационные центры
- Межведомственное сотрудничество
- Государственно-частное сотрудничество

СЕТИ 24/7

Назначенные напрямую контактные лица, доступные круглосуточно и без выходных, с актуальной контактной информацией.

Для эффективной работы сетей 24/7 национальные координаторы должны понимать:

- Собственную правовую и политическую базу;
- Как их внутренние механизмы пересекаются и взаимодействуют с более крупными международными системами; а также
- Владеть минимальными техническими знаниями для понимания поведения киберпреступников;
- Уметь общаться на иностранных языках, с минимальным знанием английского языка.

ПОЛОЖЕНИЯ БУДАПЕШТСКОЙ КОНВЕНЦИИ О КОНТАКТНЫХ СЕТЯХ 24/7 ПО ПРЕСТУПЛЕНИЯМ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

Требует от сторон создания круглосуточной сети контактных лиц по борьбе с преступлениями в сфере высоких технологий.

Стороны обязаны

«назначить контактную сеть, доступную круглосуточно, семь дней в неделю, для обеспечения оказания немедленной помощи в целях расследования или судебного разбирательства в отношении уголовных преступлений, связанных с компьютерными системами и данными, или для сбора доказательств в электронной форме об уголовном правонарушении».

5. ГОСУДАРСТВЕННО-ЧАСТНОЕ СОТРУДНИЧЕСТВО

Работа с частным сектором

ГОСУДАРСТВЕННО-ЧАСТНОЕ СОТРУДНИЧЕСТВО

Частный сектор владеет большей частью электронных доказательств

- Большая часть киберинфраструктуры принадлежит частному сектору

Общая ответственность: нужен единый подход между государственным и частным секторами

Непрерывный процесс с возможностью совершенствования

- Новые угрозы: Интернет вещей

ПРИНЦИПЫ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ СОТРУДНИЧЕСТВА

Принцип 1. Использование общего повествования для коллективных действий против киберпреступности. Общее повествование необходимо для надлежащего вовлечения, расширения возможностей и прав всех участников и заинтересованных сторон.

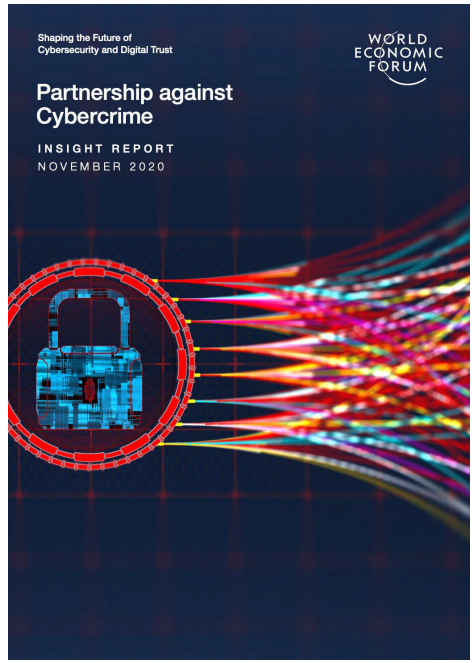
Принцип 2. Сотрудничество на основе долгосрочного стратегического согласования. Борьба с киберпреступностью и обеспечение безопасности киберпространства — это долгосрочная задача, требующая постоянной приверженности поиску общей основы для взаимодействия на основе периодически обновляемого и улучшенного понимания соответствующих потребностей, целей и ценностей каждой заинтересованной стороны.

Принцип 3. Действия, направленные на укрепление доверия. Прежде чем собираться вместе для изучения возможных точек сотрудничества, важно, чтобы участники работали независимо и самостоятельно, чтобы зарекомендовать себя как ответственные киберграждане.

Принцип 4. Систематизация сотрудничества. Сотрудничество должно быть закреплено на институциональном уровне, оставляя место для роста личных связей. Построение сотрудничества на институциональных отношениях поможет обеспечить преемственность, гарантируя, что преемники смогут вступить в сотрудничество и роль как можно более плавно.

Принцип 5. Обеспечение ценности участия в сотрудничестве. Взаимное признание усилий и вкладов помогает получить результаты, а также добиться лучшего понимания ожиданий.

Принцип 6. Учет проблем и задач. Государственно-частные совместные усилия не следует рассматривать как юридическое или договорное обязательство, а скорее как действие, разработанное на основе консенсуса.



https://www.weforum.org/projects/partnership-against-cybercime

ВИДЫ СОТРУДНИЧЕСТВА

Обязательное сотрудничество

Добровольное сотрудничество

Источник: Совет Европы (СЕ).

ОБЯЗАТЕЛЬНОЕ СОТРУДНИЧЕСТВО

Требуется в соответствии с правовыми документами такими, как договоры о взаимной правовой помощи, и соответствующим внутренним законодательством

- Например, Закон США о правомерности использования данных, хранящихся за рубежом

Взаимная правовая помощь через государственные органы

Запрашиваемые государства обеспечивают выполнение запросов о взаимной правовой помощи посредством своих собственных внутренних мер

Source: Council of Europe (CoE)

США: ЗАКОН CLOUD

Закон США о правомерности использования данных, хранящихся за рубежом

- Разрешение США вступать в переговоры об исполнительных соглашениях с другими странами, которые соответствуют определенным критериям, для облегчения трансграничного обмена данными напрямую между американскими компаниями и иностранными правительствами
- При расследовании серьезных преступлений соглашения CLOUD могут помочь снять ограничения в соответствии с законами каждой страны, чтобы поставщики коммуникационных услуг могли выполнять соответствующие законные приказы в отношении электронных данных, изданные другой страной.

ДОБРОВОЛЬНОЕ СОТРУДНИЧЕСТВО

Прямое сотрудничество с зарубежными поставщиками услуг

Информация о подписчиках запрашивается у компаний США

- У американских компаний своя политика
- Требования зависят от вида данных

БАРЬЕРЫ ДЛЯ СОТРУДНИЧЕСТВА

Сложность трансграничных ограничений данных

Помимо *законности* обмена информацией, есть проблема способности (правительства) защитить эту информацию

Репутационный ущерб при обмене информацией (потеря конкурентного преимущества)

Забота об ответственности как следствие сотрудничества

Ключевое соображение: правоохранительные органы и национальная безопасность

1. Необходимые гарантии в третьих странах для правоохранительных органов и обеспечения национальной безопасности с целью ограничения вмешательства в основные права

2. Стандарт:
    1. Обработка должна основываться на четких, точных и доступных правилах (правовая основа)
    2. Должны быть продемонстрированы необходимость и соразмерность в отношении преследуемых законных целей
    3. Обработка должна подлежать независимому контролю
    4. Эффективные средства правовой защиты должны быть доступны для физических лиц

Проблемы государственно-частного сотрудничества

Установление доверия между секторами

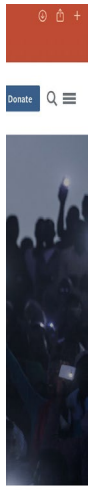
- Субъекты частного сектора могут рассматривать возможность активного сотрудничества с правительством только в случае реального инцидента и в кризисном режиме
- Организации частного сектора могут опасаться побочных последствий вовлечения правительства в реагирование на киберинциденты
- Обеспокоенность на уровне «доверия» по поводу (чрезмерного) проникновения правительства в дела частного бизнеса, когда границы неясны
- Отсутствие четких правил обмена информацией
- Широкое применение подходов частного сектора к малым и средним предприятиям (МСП) и индивидуальным предпринимателям

Просмотр:

Показатель общей свободы | Показатель свободы интернета | Показатель демократии

Быстрый поиск: Название страны

Страна	Общий показатель и статус	Препятствия к доступу	Ограничения контента	Нарушения прав пользователей
Исландия	96 Своб.	25	34	37
Эстония	94 Своб.	25	32	37
Канада	87 Своб.	23	32	32
Коста Рика	87 Своб.	20	33	34
Тайвань	80 Своб.	24	31	25
Германия	79 Своб.	22	29	28



КОНЕЦ