CyberCrime@EAP

Восточное партнерство ЕС/СЕ – механизм Совета Европы:
Сотрудничество в области противодействия киберпреступности

Стратегические приоритеты сотрудничества в области противодействия киберпреступности в странах Восточного партнерства

Утверждены на Конференции по стратегическим приоритетам
в рамках проекта «CyberCrime@EAP»

Киев, Украина, 31 октября 2013 г.

Отдел по защите данных и борьбе с киберпреступностью
Совет Европы
Страсбург, Франция, проект от 24 октября 2013 г.

www.coe.int/cybercrime

Funded by the European Union
EUROPEAN UNION
COUNCIL OF EUROPE CONSEIL DE L'EUROPE
Implemented by the Council of Europe

Содержание

Примечание: данный документ разработан при поддержке совместного проекта Совета Европы и Европейского Союза «CyberCrime@EAP» по сотрудничеству в сфере противодействия киберпреступности в рамках механизма Восточноевропейского партнерства.

Контактная информация

Для получения дополнительной информации обращайтесь по адресу:

Отдел по защите данных и борьбе с киберпреступностью
Генеральная дирекция по правам человека и верховенству права
Совет Европы
Страсбург, Франция
Тел. +33-3-9021-4506
Факс: +33-3-9021-5650
Эл. почта: alexander.seger@coe.int

Декларация о стратегических приоритетах сотрудничества в борьбе с киберпреступностью

Мы, представители министерств внутренних дел и безопасности, министерств юстиции и генеральных прокуратур государств-участников проекта «CyberCrime@EAP» в рамках механизма Восточного партнерства,

- встречаясь на этой региональной конференции по вопросам стратегических приоритетов в сфере борьбы с киберпреступностью, организованной в г. Киев, Украина, 30 и 31 октября 2013 года в сотрудничестве с Советом Европы и Европейским Союзом;

- принимая во внимание «Совместную декларацию о сотрудничестве в сфере юстиции и внутренних дел», одобренную министрами, ответственными за вопросы юстиции и внутренних дел стран-членов Европейского Союза и государств-участников «Восточного партнерства» (Люксембург, 8 октября 2013 г.), в которой, в частности, подчеркивается важность укрепления сотрудничества в противодействии киберпреступности путем эффективного применения стандартов Будапештской конвенции о киберпреступности;

- сознавая преимущества информационно-коммуникационных технологий, преобразующих наше общество;

- проявляя обеспокоенность в связи с угрозой киберпреступности, которая оказывает негативное влияние как на доверие граждан к информационным технологиям, так и на права и безопасность людей, в частности, детей;

- признавая позитивные обязательства государств по защите граждан от киберпреступности;

- помня о необходимости соблюдения основных прав и свобод при защите общества от преступности, включительно с защитой граждан в связи с обработкой персональных данных;

- принимая во внимание необходимость сотрудничества между государственным и частным секторами в области предотвращения и контроля киберпреступности и защиты компьютерных систем;

- полагая, что эффективные меры по борьбе с киберпреступностью требуют действенного регионального и международного сотрудничества;

- подчеркивая значение Будапештской конвенции о киберпреступности, которая обеспечивает методические рекомендации для законодательства отдельных стран и основу международного сотрудничества;

- отмечая с признательностью возрастающее внимание к вопросам кибербезопасности и мерам по борьбе с киберпреступностью со стороны Европейского Союза;

- считая необходимым, в частности, создание партнерских отношений между Европейским Центром по борьбе с киберпреступностью при Европоле и нашими правоохранительными органами;

- с благодарностью за поддержку, оказываемую Европейским Союзом и Советом Европы в рамках регионального проекта «CyberCrime@EAP»;

- используя наработки и действия, предпринятые государствами региона в области борьбы с киберпреступностью, и при этом отмечая необходимость принятия дальнейших мер;

утверждаем

стратегические приоритеты сотрудничества в области противодействия

киберпреступности, представленные на этой конференции,

и берем на себя следующие обязательства по

- внедрению стратегий борьбы с киберпреступностью в целях обеспечения эффективного реагирования со стороны системы уголовного правосудия как на правонарушения, направленные против компьютерных систем и совершенные с использованием компьютеров, так и на любое правонарушение, в котором фигурируют электронные доказательства;

- принятию полноценного и эффективного законодательства в области киберпреступности, отвечающего требованиям соблюдения прав человека и обеспечения законности;

- усилению специализированных правоохранительных подразделений и прокурорских служб, которые специализируются на киберпреступности и электронных доказательствах;

- внедрению устойчивых стратегий обучения сотрудников правоохранительных органов;

- поддержке повышения квалификации судей и прокуроров в сфере киберпреступности и использования электронных доказательств;

- внедрению комплексных стратегий по защите детей от сексуальной эксплуатации в виртуальном пространстве и сексуального насилия в соответствии с требованиями Лансаротской конвенции;

- содействию финансовым расследованиям, предотвращению и контролю мошенничества и отмывания денег в Интернете;

- расширению сотрудничества с частным сектором, в частности, между правоохранительными органами и Интернет сервис провайдерами;

- участию в эффективном региональном и международном сотрудничестве;

- обмену опытом с другими регионами в мире для усиления потенциала в области борьбы с киберпреступностью;

- содействию соблюдению требований Будапештской конвенции о киберпреступности на глобальном уровне.

Декларация принята в порядке всеобщего одобрения

в г. Киев, Украина, 31 октября 2013 г.

Приложение: стратегические приоритеты сотрудничества в борьбе с киберпреступностью

1. Стратегический приоритет: принципы и стратегии борьбы с киберпреступностью

По мере того, как общество трансформируется под влиянием информационно-коммуникационных технологий, вопросы безопасности ИКТ становятся приоритетными для многих государств, что отражается в принятии правительствами многих стран стратегий кибербезопасности с основным акцентом на защите критически важной информационной инфраструктуры. В то же время, у правительств также есть положительные обязательства по защите от киберпреступности граждан и их прав, а также по привлечению правонарушителей к ответственности.

Таким образом, правительства могут рассматривать вопросы подготовки отдельных стратегий борьбы с киберпреступностью или усиления компонентов борьбы с киберпреступностью в рамках общей стратегии обеспечения кибербезопасности.

Соответствующие органы могут рассмотреть следующие действия:

- **Внедрение принципов и стратегий борьбы с киберпреступностью** с целью обеспечения эффективного реагирования со стороны уголовного правосудия как на правонарушения, направленные против компьютерных систем, правонарушения с использованием компьютеров, так и на любое правонарушение, в котором фигурируют электронные доказательства. Элементами таких программ или стратегий можно считать профилактические мероприятия, законодательство, специализированные правоохранительные подразделения и прокурорские службы, межведомственное сотрудничество, обучение сотрудников правоохранительных и судебных органов, государственно-частное сотрудничество, эффективное международное сотрудничество, финансовые расследования, предупреждение мошенничества и отмывания денег, защита детей от сексуального насилия.

- Обеспечение выполнения в борьбе с киберпреступностью требований по соблюдению прав человека и законности.

- **Создание виртуальных платформ публичной отчетности по киберпреступности.** Это должно обеспечить более глубокое понимание угроз и тенденций в области киберпреступности и содействовать деятельности органов уголовного правосудия. Такие платформы также можно использовать в целях информирования граждан и предупреждения об угрозах.

- Обеспечение информированности и содействие принятию профилактических мер на всех уровнях.

- **Участие в государственно-частном сотрудничестве,** включая, в частности, сотрудничество между органами правопорядка и Интернет-сервис провайдерами.

- **Участие в возможно более широком международном сотрудничестве.** Это подразумевает использование в полной мере имеющихся двухсторонних, многосторонних и региональных договоров – в частности, Будапештской конвенции о киберпреступности. Следует принимать меры и организовывать обучение для обеспечения оперативности правовой взаимопомощи. Государствам (участникам

конвенции и наблюдателям) следует принимать активное участие в работе Комитета конвенции о киберпреступности (T-CY), а также в сотрудничестве с Европейским центром борьбы с киберпреступностью и другими инициативами Европейского Союза.

- **Регулярная оценка эффективности реагирования со стороны органов уголовного правосудия на киберпреступления и ведение статистики**. Такой анализ поможет определять и совершенствовать эффективность мер, предпринимаемых органами уголовного правосудия, и эффективно распределять ресурсы.

2. Стратегический приоритет: полноценная и эффективная законодательная база в основе деятельности органов уголовного правосудия

Надлежащее законодательство лежит в основе мер по борьбе с киберпреступностью, предпринимаемых органами уголовного правосудия, и использования электронных доказательств в уголовном производстве. Государства-участники проекта «CyberCrime@EAP» сделали большой шаг вперед в приведении своего законодательства в соответствие с требованиями Будапештской конвенции, соответствующими стандартами Совета Европы и Европейского Союза по защите данных, защите детей от сексуального насилия или стандартами противодействия легализации доходов, полученных от преступной деятельности, или отмыванию денег.[1] Тем не менее, его необходимо усиливать, и нередко законодательство должно выдерживать испытание жизнью, что особенно актуально для полномочий, которые предусматриваются отдельными процессуальными законами.

Принятие полного и эффективного законодательства, отвечающего требованиям обеспечения прав человека и законности, должно стать стратегическим приоритетом.

Соответствующие органы должны рассмотреть следующие действия:

- **Дальнейшее совершенствование положений процессуального законодательства с целью обеспечения электронных доказательств органами правопорядка.** Это должно включать не только законы и исполнительные распоряжения по использованию положений Будапештской конвенции относительно ускоренного порядка обеспечения сохранности данных (вслед за оценкой Комитета конвенции о киберпреступности), но и другие правила относительно доступа к данным, которые находятся в распоряжении организаций частного сектора.

- **Оценка эффективности законодательства.** Применение законодательства и регламентов на практике должно анализироваться на регулярной основе. Следует вести статистику дел, по которым проводилось расследование, дел, переданных в суд, и дел, по которым суд вынес решение или приговор, а процедуры должны фиксироваться документально.

[1] См., например, Конвенцию Совета Европы по защите граждан в отношении автоматизированной обработки персональных данных (ETS 108), "Лансаротскую конвенцию" по вопросам сексуальной эксплуатации и сексуального насилия над детьми (CETS 201), конвенции по противодействию отмыванию денег, поиску, наложению ареста и конфискации доходов от преступной деятельности, недопущению финансирования терроризма (CETS 198).

- **Обеспечение соответствия полномочий правоохранительных органов и гарантий требованиям статьи 15 Будапештской конвенции.** Это должно подразумевать не только судебный контроль над полномочиями на вмешательство, но также и соблюдение принципов пропорциональности и необходимости.

- **Усиление законодательства в области защиты данных в его соответствии с международными и европейскими стандартами.** Государствам рекомендуется обеспечить соответствие своего внутреннего законодательства по защите данных принципам конвенции Совета Европы по защите данных ETS 108 и принять участие в текущем процессе модернизации Конвенции. То же распространяется и на будущие стандарты Европейского Союза по защите данных. Это будет способствовать обмену данными между странами также и в правоохранительных целях.

- **Завершение работы над законодательством и внедрение защитных мер по защите детей от сексуального насилия в Интернете**. В то время, как многие положения Лансаротской конвенции уже внедрены, некоторым государствам или регионам все еще необходимо решать такие вопросы как "владение детской порнографией", "умышленное получение доступа" и "груминг".

- Адаптация законодательства в части финансовых расследований, конфискации доходов от преступной деятельности, отмывания денег и финансирования терроризма к виртуальному пространству. В частности, правила и регламенты должны обеспечивать оперативный обмен информацией внутри и между странами.

3. Стратегический приоритет: специализированные подразделения по борьбе с киберпреступностью

Киберпреступность и электронные доказательства требуют специализированного реагирования со стороны органов уголовного правосудия. Правоохранительным органам и прокурорским службам необходимо уметь расследовать и привлекать к ответственности лиц за совершение преступлений с компьютерными данными и системами, преступлений с помощью компьютеров, а также работать с электронными доказательствами в связи с любым преступлением. Все государства-участники проекта «CyberCrime@EAP» создают по типу органов правопорядка или усиливают подразделения по борьбе с киберпреступностью, а некоторые из них рассматривают вопросы специализации прокуроров. Этот процесс следует продолжить. Очень важно понимать, что технологии меняются изо дня в день, и нагрузки на подразделения по борьбе с киберпреступностью и криминалистов постоянно растут. Вопросы обеспечения ресурсами (кадрами, оборудованием, программным обеспечением), соответствующей квалификации и адаптации таких подразделений под новые требования не теряют своей актуальности.

Постоянное укрепление специализированных подразделений по борьбе с киберпреступностью должно становиться стратегическим приоритетом.

Соответствующим органам следует рассмотреть следующие действия:

- **Создание – там, где это еще не сделано – специализированных подразделений по борьбе с киберпреступностью в структуре уголовной полиции.** Точная организация и функции должны определяться по результатам тщательного анализа потребностей и основываться на принципах законности.

- **Усиление специализации прокуроров.** Рассмотрение вопроса создания специализированных подразделений в органах прокуратуры или, как вариант – группы прокуроров, которые будут специалистами в этом направлении и будут давать рекомендации или оказывать помощь другим прокурорам в производстве дел, связанных с киберпреступлениями, или дел, в которых фигурируют электронные доказательства.

- **Обзор функций и порядка обеспечения специализированных подразделений ресурсами на постоянной основе.** Это должно позволить вносить необходимые изменения под новые задачи и возрастающие требования.

- Содействие сотрудничеству и обмену практическим опытом между специализированными подразделениями на региональном и международном уровнях.

- **Улучшение порядка расследования киберпреступлений и работы с электронными доказательствами.** Исследовать и рассмотреть вопрос внедрения национальных и международных стандартов и соответствующей практики в этом отношении. Рассмотреть вопрос использования пособия по работе с электронными доказательствами, разработанного в рамках проекта «CyberCrime@IPA» в сотрудничестве с экспертами региона восточноевропейского партнерства.

4. Стратегический приоритет: обучение сотрудников органов правопорядка

Органы правопорядка должны уметь не только расследовать преступления в области и с помощью компьютерных систем, но и работать с электронными доказательствами, которые фигурируют в преступлениях любого вида. С ростом в геометрической прогрессии использования информационных технологий в обществе не меньшими темпами растут и задачи, которые возлагаются на органы правопорядка. Все сотрудники органов правопорядка – от тех, которые первыми выезжают на место до высокоспециализированных следователей-криминалистов – должны уметь работать с киберпреступлениями и электронными доказательствами на своем уровне. Элементы стратегий подготовки сотрудников органов правопорядка уже определены, но последовательные стратегии такой подготовки еще не приняты.

Подготовка и внедрение устойчивых стратегий обучения сотрудников органов правопорядка на соответствующем уровне должна стать стратегическим приоритетом.

Соответствующим органам следует рассмотреть следующие действия:

- **Внедрение внутригосударственной стратегии обучения сотрудников органов правопорядка.** Цель должна заключаться в том, чтобы обеспечить необходимую квалификацию и компетентность сотрудников органов правопорядка в расследовании киберпреступлений, работе с электронными доказательствами, осуществлении криминалистического анализа компьютеров в части уголовного производства, оказании помощи другим ведомствам и внесении своего вклада в обеспечение сетевой безопасности. Учитывая зависимость общества от информационных технологий и связанные с этим риски, капиталовложения в такое обучение себя оправдывают.

- **Включение регламентов и протоколов работы с электронными доказательствами на всех уровнях внутригосударственной системы**

обучения. Важно понимать значение электронных доказательств в раскрытии преступной деятельности и необходимость обучения распознаванию и работе с электронными доказательствами всех оперативников органов правопорядка, а не только сотрудников специализированных подразделений. Такое обучение можно организовывать с использованием пособия по работе с электронными доказательствами, разработанного в рамках проекта «CyberCrime@IPA».

- **Рассмотрение вопроса внедрения планов индивидуального обучения следователей-специалистов.** Изменение технологий и способов использования этих технологий в преступных целях означает потребность в наличии соответствующего количества хорошо подготовленных кадров, которые будут знать, как, и уметь проводить расследование и (или) экспертизу электронных доказательств на высшем уровне. Это также укрепит их статус в системе уголовного правосудия.

- **Рассмотрение вопроса внедрения порядка обеспечения эффективности капиталовложений в обучение в сфере борьбы с киберпреступностью.** Обучение в сфере борьбы с киберпреступностью и проведения экспертизы компьютеров стоит очень дорого. Для того, чтобы обеспечить окупаемость капиталовложений, государства должны обеспечить назначение на должность и нахождение кадров на таком посту, который отражает уровень их знаний и квалификации. В этом отношении стратегии обучения и кадрового обеспечения должны дополнять одна другую.

5. Стратегический приоритет: обучение сотрудников судебных органов

Помимо преступлений в отношении и с помощью компьютерных систем, во все возрастающем количестве преступлений другого рода фигурируют улики, которые хранятся в компьютерных системах или на других носителях. Это значит, что практически всем судьям и прокурорам нужно быть готовыми к работе с электронными доказательствами. Все государства-участники проекта «CyberCrime@EAP» четко определились в отношении необходимости системного и постоянного обучения судей и прокуроров.

Обеспечение умения всех судей и прокуроров привлекать к ответственности, преследовать в судебном порядке лиц за совершение киберпреступлений и использовать электронные доказательства в уголовном производстве должно оставаться стратегическим приоритетом.

Соответствующим органам следует рассмотреть следующие действия:

- **Адаптация текущих учебных материалов и обучение инструкторов**. Совет Европы уже разработал концепции обучения и учебные материалы, которые можно адаптировать к нуждам внутригосударственных учебных заведений. Инструкторов необходимо обучить методике подачи материалов.

- **Массовость обучения судей и прокуроров в области киберпреступлений и электронных доказательств.** Внутригосударственные учебные заведения для судей и прокуроров должны интегрировать модули базовой подготовки судей и прокуроров в области киберпреступлений и электронных доказательств и курсы повышения квалификации в свои штатные учебные программы начальной подготовки и программы повышения квалификации по месту работы.

- **Внедрение мер по обеспечению обязательности обучения сотрудников судебных органов и органов прокуратуры в области киберпреступлений и электронных доказательств.** В ходе проекта стал очевидным факт обучения судей и прокуроров по большинству направлений проекта на добровольной основе. Это привело к тому, что во многих случаях участники посещали курсы очень непродолжительное время и не воспользовались в полной мере всем тем, что могло им дать предложенное обучение.

- **Внедрение порядка учета прохождения обучения отдельными судьями и прокурорами.** В целях достижения максимальной пользы от курсов подготовки судей и прокуроров рекомендуется вести учет пройденного лицами обучения, с помощью которого будут определяться требования по дальнейшей специализированной подготовке, те лица, которых действительно необходимо обучать, и квалификация которых найдет нужное применение.

6. Стратегический приоритет: финансовые расследования, предотвращение и контроль мошенничества и отмывания денег в Интернете

По большей части, преступления с использованием Интернета и других информационных технологий направлены на получение прибылей путем разного рода мошенничества и других форм экономических и тяжких преступлений. Таким образом, в Интернете генерируются и циркулируют в больших объемах средства, полученные преступным путем.

Соответственно, финансовые расследования, направленные на поиск, изъятие и конфискацию средств, полученных преступным путем, а также меры по предотвращению мошенничества, предотвращению и контролю отмывания денег в Интернете должны стать стратегическим приоритетом.

Государственным органам следует рассмотреть следующие действия:

- **Создание виртуальной платформы для информирования граждан о случаях мошенничества в Интернете и киберпреступности в общем.** Использование стандартных шаблонов сообщений позволит лучше анализировать угрозы и тенденции, преступную деятельность и организации, схемы денежных потоков и отмывания денег. Это будет способствовать принятию мер со стороны органов уголовного правосудия и подразделений финансовой разведки по привлечению к ответственности лиц, совершивших преступление, а также по изъятию и конфискации средств, полученных преступным путем. Платформа также должна служить в профилактических целях (информирование и просвещение граждан, предупреждение об угрозах, предоставление инструментов и рекомендаций). Чем более гармонизированы будут внутригосударственные платформы с платформами других государств, тем легче будет осуществлять региональный и международный анализ и принимать меры.

- **Внедрение упредительных параллельных финансовых расследований** при расследовании киберпреступлений или преступлений с использованием информационных технологий/Интернета. Это требует расширенного межведомственного сотрудничества между органами, которые отвечают за киберпреступность и финансовые расследования, и органами финансовой разведки. Совместное обучение может способствовать такому межведомственному сотрудничеству.

- **Создание пользующихся доверием форумов** (национальных и региональных) с целью обмена информацией касательно киберугроз в финансовом секторе между государственными и частными организациями. Внутригосударственные форумы должны быть доступны всем ключевым заинтересованным сторонам (представителям финансового сектора, Интернет сервис провайдерам, подразделениям по борьбе с киберпреступностью, подразделениям финансовой разведки, группам компьютерной безопасности). Их задача состоит в выявлении угроз, определении тенденций, инструментов и решений по защите финансового сектора от киберпреступности. Региональный форум должен состоять из форумов, созданных на национальных уровнях.

- **Создание законодательной базы для наложения ареста и конфискации средств, полученных преступным путем** и цифровых активов, а также для предотвращения отмывания денег в Интернете. Это должно включать цифровые активы, электронные деньги и виртуальные валюты. Правила, регламенты и процедуры должны также распространяться на платежные системы в Интернете.

- **Использование возможностей для более эффективного международного сотрудничества.** Связывание мер противодействия отмыванию денег и финансовых расследований с расследованием киберпреступлений и компьютерной криминалистикой предлагает дополнительные возможности для международного сотрудничества. Государствам следует использовать возможности, предлагаемые Будапештской конвенцией Совета Европы о киберпреступности и конвенцией об отмывании денег, поиске, изъятии и конфискации средств полученных преступным путем, и финансировании терроризма (CETS 198) и пересмотренными 40 рекомендациями группы по борьбе с финансовыми злоупотреблениями (FATF). Следует также принять во внимание результаты типологического исследования комитета MONEYVAL по вопросам криминальных денежных потоков в Интернете, проведенного в марте 2012 года.[2]

7. Стратегический приоритет: сотрудничество между органами правопорядка и Интернет сервис провайдерами

сотрудничество между органами правопорядка и Интернет сервис провайдерами (ИСП) и другими организациями частного сектора имеет важное значение для защиты прав Интернет пользователей и их защиты от преступности. Нередко эффективное расследование киберпреступлений невозможно без сотрудничества ИСП. В то же время, такое сотрудничество должно учитывать различную роль органов правопорядка и ИСП, а также право пользователей на конфиденциальность.

Углубленное сотрудничество между органами правопорядка и ИСП, обмен информацией между государственным и частным сектором в соответствии с положениями о защите данных должно стать стратегическим приоритетом.

Государственным органам следует рассмотреть следующие действия:

- **Создание четких правил и порядка на отечественном уровне, определяющего доступ органов правопорядка к данным,** которые хранят ИСП и другие организации частного сектора. В соответствии с положениями о защите данных четкая законодательная база, которая соответствует положениям

[2] http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/MONEYVAL_2012_6_Reptyp_flows_en.pdf

процессуального законодательства, гарантиям и условиям, предусмотренным в Будапештской конвенции о киберпреступности, поможет соответствовать требованиям об обеспечении прав человека и законности. Методические рекомендации[3], принятые на конференции Совета Европы «Octopus» в 2008 году, могут помочь органам правопорядка и ИСП в организации и определении структуры своего сотрудничества. Государства должны содействовать использованию положений Будапештской конвенции об ускоренном порядке обеспечения сохранности данных (статьи 16, 17, 29, 30) с учетом результатов оценок, данных Комитетом конвенции о киберпреступности.[4]

- **Содействие культуре сотрудничества между органами правопорядка и ИСП.** Меморандумы о взаимопонимании между органами правопорядка и Интернет сервис провайдерами являются непреложным инструментом в этом отношении. Региональная координация таких меморандумов могла бы способствовать осуществлению органами правопорядка расследований с пересечением региональных границ, зная, что сопоставимые стандарты приняты на территории других государств. Меморандумы о взаимопонимании в сочетании с четкими правилами и процедурами могут также способствовать сотрудничеству с многонациональными ИСП и другими организациями частного сектора – в том числе, в вопросах раскрытия данных, которые хранятся в зарубежных юрисдикциях или на облачных серверах. которыми ведают такие ИСП.

- **Содействие трансграничному обмену информацией между государственными и частными структурами.** Структуры частного сектора владеют массой информации об инцидентах, связанных с кибербезопасностью. Обмен такой информацией между странами может помочь в укреплении безопасности информационной инфраструктуры и отслеживании преступников. Государствам следует рассмотреть вопросы обеспечения законодательства и заключения договоров, которые позволят частным и государственным структурам обмениваться информацией, будут способствовать разработке методических рекомендаций по обеспечению обмена информацией внутри страны и за ее пределами с учетом процессуальных, технических, правовых вопросов и гарантий по защите данных.

8. Стратегический приоритет: более эффективное региональное и международное сотрудничество

Киберпреступность и электронные доказательства являются транснациональными по своей сути, что требует эффективного международного сотрудничества. Требуется принятие незамедлительных шагов по обеспечению сохранности электронных доказательств в иностранной юрисдикции и получению таких доказательств. В то же время, неэффективность международного сотрудничества – в частности, в вопросах взаимной правовой помощи – по-прежнему считается одним из основных препятствий к принятию эффективных мер по борьбе с киберпреступностью.

Обеспечение более продуктивного сотрудничества в области киберпреступности и электронных доказательств должно стать стратегическим приоритетом.

Государственным органам следует рассмотреть следующие действия:

[3] http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/LEA_ISP/default_en.asp.
[4] Отчет по результатам оценки, принятый Комитетом T-CY в декабре 2012 года http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/TCY2013/TCYreports/TCY_2012_10_Assess_report_v30_public.pdf

- **Использование возможностей, предоставляемых Будапештской конвенцией о киберпреступности и другими двухсторонними, региональными и международными договорами о сотрудничестве в области уголовного правосудия**. Это включает использование в полной мере статей 23 - 35 Будапештской конвенции, которыми предусматривается сотрудничество между органами полиции и судебными органами, а также внесение изменений в законодательные акты и совершенствование процедур. Государства (участники конвенции и наблюдатели) должны поучаствовать в полной мере в оценке положений Будапештской конвенции о международном сотрудничестве в 2013 году. которая осуществляется Комитетом конвенции о киберпреступности (T-CY), и в дальнейших шагах по результатам такой оценки. Они должны осуществить необходимые шаги по результатам оценки Комитета от 2012 года и способствовать использованию статей 23 - 35 Будапештской конвенции в части международных запросов на сохранение данных.

- **Организация обучения и обмена практическим опытом.** Органам, задействованным в организации сотрудничества между органами полиции и судебными органами, следует принять участие во внутренних, региональных и международных тренингах и обмене практическим опытом. Это должно способствовать сотрудничеству, основанному на доверии.

- **Оценка эффективности международного сотрудничества.** Министерствам юстиции, внутренних дел, прокурорским службам следует вести сбор статистических данных международного сотрудничества по запросам в части киберпреступлений и электронных доказательств – по типу запросов на оказание помощи, срокам исполнения и процедурам, которые были задействованы. Это должно помочь в определении надлежащей практики и снятии преград на пути к сотрудничеству. Они могут совместно с региональными партнерами участвовать в анализе вопросов, которые оказывают серьезное влияние на международное сотрудничество.

- **Усиление эффективности круглосуточной связи с координаторами.** Такие координаторы назначены во всех государствах в соответствии с требованиями, предусмотренными статьей 35 Будапештской конвенции, но их роль необходимо усилить, работу можно направить в более упреждающее русло, и обеспечить их полную функциональность.

- **Регулярный сбор статистических данных, анализ эффективности круглосуточной и ежедневной деятельности координаторов** и других форм международного сотрудничества.