Проект «Киберпреступность»
www.coe.int/cybercrime

и

Лиссабонская сеть
www.coe.int/lisbon-network

Департамент по вопросам информационного общества и борьбе против преступности, Генеральный директорат по правам человека и правовым вопросам, Страсбург, Франция

8 октября 2009 г.

Программа подготовки судей и прокуроров по вопросам киберпреступности: концепция

Проект финансируется на средства, предоставленные Румынией, компаниями «Майкрософт» и «МакАфи» и Советом Европы

Настоящий документ был подготовлен рабочей группой заинтересованных сторон в рамках проекта «Киберпреступность» и Лиссабонской сети Совета Европы по подготовке судей.

Контактная информация:

Для получения более подробной информации обращайтесь в:

Департамент по вопросам информационного общества и борьбы против преступности,
Генеральный директорат по правам человека и правовым вопросам,
Совет Европы,
Страсбург, Франция

Тел.: +33-3-9021-4506
Факс: +33-3-9021-5650
Электронная почта: alexander.seger@coe.int

Оговорка об ограничении ответственности:

Оглавление

1 Краткое содержание

Учитывая то, что общества во всем мире широкого используют информационные и коммуникационные технологии, судьи и прокуроры должны быть подготовлены к рассмотрению дел, связанных с киберпреступностью и использованием электронных доказательств. Несмотря на то, что во многих странах правоохранительные органы имели возможность укрепить свой потенциал знаний для расследования киберпреступлений и использования электронных доказательств, это, судя по всему, в меньшей степени коснулось судей и прокуроров. Опыт показывает, что при ведении большинства дел судьи и прокуроры сталкиваются с трудностями при взаимодействии с новыми реалиями компьютерного мира. В связи с этим, требуются специальные усилия, чтобы судьи и прокуроры могли вести судебное преследование и выносить постановления в отношении киберпреступлений и использовать электронные доказательства благодаря проведению программ повышения квалификации, сетевому взаимодействию и специализации.

Концепция настоящего документа предусматривает оказание поддержки этим усилиям. Она была разработана Советом Европы в Проекте «Киберпреступность» и Лиссабонской сетью Совета Европы по подготовке судей в сотрудничестве с многосторонней рабочей группой заинтересованных сторон в течение 2009 г.

Целью настоящей концепции является оказание помощи учебным заведениям в разработке программ подготовки судей и прокуроров по вопросам киберпреступлений и использования электронных доказательств и включение этих программ в традиционные курсы начальной подготовки и переподготовки (то есть обеспечение их институционализации). Кроме того, это будет способствовать сетевому взаимодействию между судьями и прокурорами в целях повышения их уровня знаний, а также оказания постоянной, а не единовременной поддержки инициативам заинтересованных сторон в области обучения.
Настоящая концепция включает следующие компоненты:

Цели

Существующая система начальной подготовки и переподготовки, как правило, не предоставляет судьям и прокурорам знаний, которые требуются для рассмотрения дел о киберпреступлениях и для использования электронных доказательств.

Таким образом, концепция обучения судей и прокуроров должна преследовать следующие цели:

- Предоставить возможность учебным заведениям проводить программы начальной подготовки и переподготовки, основанные на международных стандартах;
- Вооружить максимально возможное количество будущих и практикующих судей и прокуроров основными знаниями о киберпреступлениях и использовании электронных доказательств;
- Провести программы повышения квалификации значительного количества судей и прокуроров;
- Оказать помощь в проведении дальнейшей специализации и технической подготовки судей и прокуроров;
- Способствовать расширению знаний с помощью сетевого взаимодействия между судьями и прокурорами;
- Облегчить доступ к различным учебным инициативам и сетям.

Для достижения этих целей следует принять следующие меры:

1. Институционализация начальной подготовки

- Тем странам, где начальная подготовка представляет собой практические занятия на рабочем месте, рекомендуется, чтобы, по меньшей мере, часть этих занятий была связана с вопросами киберпреступлений и использования электронных доказательств;
- В тех странах, где начальная подготовка проводится в юридических учебных заведениях, учебные курсы этих заведений должны включать как минимум один модуль базового уровня по вопросам киберпреступлений и использования электронных доказательств. Эти вопросы должны дополнительно рассматриваться в обязательных модулях, охватывающих вопросы материального и процессуального права. Необходимо также предлагать учащимся факультативные модули для получения знаний по вопросам киберпреступности и использования электронных доказательств на продвинутом уровне;
- Специальные учебные модули следует привести в такое соответствие со стандартами, чтобы их можно было тиражировать и использовать для того, чтобы слушатели могли повышать уровень своих знаний, начиная с базового уровня и кончая продвинутым уровнем.

2. Институционализация переподготовки

- Учебные заведения, проводящие программы переподготовки, должны включать в них, по меньшей мере, один модуль базового уровня по киберпреступности и использованию электронных доказательств, чтобы вооружить практикующих судей и прокуроров базовыми знаниями, которые они не получили во время начальной подготовки;
- Кроме того, они должны предлагать курсы обучения на продвинутом уровне.

3. Стандартизация и тиражирование курсов/модулей

- Необходимо разработать стандартизированные курсы или модули, которые можно было бы эффективно тиражировать в широких масштабах и использовать для того, чтобы слушатели и практикующие судьи и прокуроры могли повышать уровень своих знаний, начиная с базового уровня и кончая продвинутым уровнем.
- Следует провести оценку существующих базовых курсов, которые можно было бы включить в учебные планы программ начальной подготовки и переподготовки. Стандартный курс можно затем рекомендовать учебным заведениям для программ начальной подготовке и переподготовки.
- Аналогичную оценку можно было бы дать курсам на продвинутом уровне и затем рекомендовать учебным заведениям стандартный курс на продвинутом уровне.
- Преподавателям необходимо пройти такой курс подготовки по преподаванию этих курсов, чтобы обучение могли проводить местные преподаватели на местных языках лишь при ограниченном участии международных преподавателей.

4. Доступность учебных пособий/материалов для самообучения

- Необходимо разработать учебные пособия, соответствующие общим международным стандартам и передовой практике. Они должны быть доступны для учебных заведений с точки зрения экономической выгоды, чтобы обеспечить их распространение на местном уровне;
- Несмотря на то, что судьи и прокуроры должны в первую очередь проходить подготовку по применению национального законодательства, тем не менее, можно разработать стандартизированные учебные пособия таким образом, чтобы в них оставалось достаточно места для отражения особенностей национальных систем и законодательств;
- Следует разработать и обеспечить доступ к онлайновым курсам.

5. Пилотные центры обучения на базовом и продвинутом уровнях

- Необходимо создать ряд пилотных центров для подготовки судей и прокуроров по вопросам киберпреступности и использования электронных доказательств на базовом и продвинутом уровнях, чтобы апробировать эти курсы и затем разработать стандартизированные курсы и материалы, обеспечить распространение передовой практики, провести исследования процесса обучения, вести реестр преподавателей, проводить подготовку преподавателей, проводить программы обучения в других странах с аналогичными системами и языками;
- Пилотные центры должны координировать свою работу друг с другом при поддержке Совета Европы;
- Судья и следователи, которые прошли подготовку и стали специалистами, должны рассмотреть возможность участия в программах обучения в центрах повышения квалификации для представителей правоохранительных органов и промышленности.

6. Расширение объема знаний за счет сетевого взаимодействия

- Помимо обучения, контактов между коллегами, сетевого взаимодействия между судьями и прокурорами, также крайне важно осуществлять сетевое взаимодействие с широким кругом других заинтересованных сторон;
- Судьи и прокуроры должны использовать существующие сети для судей или прокуроров (например, GPEN);
- Совету Европы следует обсудить возможность создания международной сети по киберпреступлености или электронным преступлениям для судей (аналогичной сети GPEN для прокуроров);
- Совет Европы и Европейская сеть по подготовке судей должны оказать поддержку взаимодействию между европейскими учебными заведениями, проводящими программы по вопросам киберпреступности и использования электронных доказательств;
- В целях оказания содействия судьям и прокурорам в обеспечении доступа к этим и многим другим сетям, касающимся вопросов киберпреступности, Совет Европы должен составить карту инициатив и информационных сетей и создать портал с соответствующими ссылками, краткой информацией и подробными контактными данными разных сетей. Это также должно способствовать развитию сетевого сотрудничества. Кроме того, это также должно облегчить доступ к существующим учебным материалам и инициативам.

7. Государственно-частное сотрудничество

- Поддержка частного сектора в проведении подготовки судей и прокуроров могла бы быть полезной, учитывая то, что частный сектор обладает соответствующим опытом знания этого предмета. В то же время, судьи и прокуроры должны оставаться независимыми и беспристрастными;
- Учебные заведения по подготовке судей могут использовать опыт частного сектора при разработке учебных программ, подготовке учебных пособий и проведении курсов обучения;
- Поддержка учебных заведений со стороны промышленности не должна быть направлена на принятие потенциально благоприятных решений в суде или на развитие предпринимательства, а гарантировать предоставление судьям и прокурорам адекватной информации, позволяющей им принимать информированные решения;
- Частный сектор мог бы оказывать прозрачную поддержку международным или национальным организациям, научному сообществу, образовательным инициативам или другим третьим сторонам, которые могут в свою очередь помогать независимым учебным заведениям;
- Несмотря на то, что судьи и прокуроры должны иметь общее представление об Интернете и о киберпреступности, не менее важно предоставить им специальную информацию о

платформах. Промышленность могла бы предоставить конкретные модули (а не полные курсы) по вопросам функционирования соответствующих платформ.

Лиссабонская сеть Совета Европы одобрила настоящую концепцию в сентябре 2009 г. и рекомендовала ее для широкого распространения и применения учебными заведения по подготовке судей. Она приняла решение привлечь к ней внимание Консультативного совета европейских судей и Консультативного совета европейских прокуроров, а также Европейской комиссии по эффективности правосудия (ЕКЭП), чтобы обеспечить самую широкую поддержку настоящей концепции.

2 Введение

В последние годы общества во всем мире добились огромного прогресса в развитии информационного общества. Информационные и коммуникационные технологии (ИКТ) теперь проникли практически во все сферы жизни людей. При этом более широкое использование ИКТ и, следовательно, зависимость от их использования делают общество уязвимым для таких угроз, как киберпреступность, т.е. преступления, совершенные против компьютерных данных и систем или с их помощью.

Помимо большого количества правонарушений, совершенных против ИКТ или с их помощью, все больше других дел, заканчивающихся в суде, связано с электронными доказательствами, хранящимися в компьютерной системе или на других устройствах.

Таким образом, судьи и прокуроры должны быть готовы к рассмотрению дел, связанных с киберпреступленостью и использованием электронных доказательств. Как заявил Консультативный совет европейских судей[1], «крайне необходимо, чтобы судьи после прохождения полного курса юридического образования получали разнообразные знания и могли эффективно выполнять свои обязанности» (пункт 3), «эта подготовка также гарантирует их независимость и беспристрастность» (пункт 4), в ходе этой подготовки следует «принимать во внимание необходимость социальной информированности и широкого понимания различных предметов, отражающих сложности жизни в современном обществе» (пункт 27). ИКТ играют такую важную роль в жизни современного общества, что судьи и прокуроры должны, по меньшей мере, иметь базовое представление об этих технологиях и связанных с ними проблемах.

Несмотря на то, что во многих странах правоохранительные органы смогли повысить потенциал своих знаний для проведения расследований киберпреступлений и получения электронных доказательств, это, судя по всему, в меньшей степени касается судей и прокуроров, которые, тем не менее, играют важнейшую роль в процессе уголовного правосудия. Опыт показывает, что в большинстве случаев судьи и прокуроры сталкиваются с трудностями при взаимодействии с новыми реалиями компьютерного мира.

В связи с этим, требуются специальные усилия, чтобы судьи и прокуроры могли вести судебное преследование, выносить решения в связи с киберпреступлениями и использовать электронные доказательства благодаря проведению программ повышения квалификации, сетевому взаимодействию и специализации.

Опыт частного сектора в области новых технологий был необходимым условием подготовки работников правоохранительных органов. Он также будет полезен для подготовки судебных работников [2], но его потенциал пока недостаточно используется. В то же время, необходимо сохранить независимость и беспристрастность судей и прокуроров. Таким образом, инновационные подходы требуют сохранения независимости судей и прокуроров и в то же время предоставления им доступа к опыту частного сектора и обеспечения понимания ими методов функционирования промышленности и технологии. Концепция, предлагаемая в настоящем документе, показывает, каким образом учебные заведении по подготовке судей могут получить пользу от поддержки со стороны промышленности и научного сообщества через стандартизированные учебные программы и за счет использования других средств.

[1] Заключение № 4 о надлежащих программах начальной подготовки и переподготовки судей на национальном и европейском уровнях (ЕКЭП (2003), Заключение № 4).

[2] См. исследование, опубликованное в марте 2009 г.: "Co-operation between LE, Industry and Academia to deliver long term sustainable training to key cybercrime personnel"(«Сотрудничество между учебными заведениями, промышленностью и научным сообществом в целях обеспечения долгосрочной устойчивой подготовки основного персонала по вопросам киберпреступности»).

Целью настоящей концепции является оказание помощи учебным заведениям в разработке для судей и прокуроров программ по вопросам киберпреступности и использования электронных доказательств и включении этих программ в традиционные курсы начальной подготовки и переподготовки (то есть, их институализация).

Концепция основана на информации, полученной из учебных заведений Бельгии, Хорватии, Грузии, Германии, Франции, Нидерландов, Польши, Португалии, Румынии, Испании, «бывшей югославской Республики Македония» и Великобритании (ответы на вопросы анкеты, полученные в июне 2009 г.), на практическом семинаре для представителей Бельгии, Ирландии, Италии, Португалии, Нидерландов и Великобритании, а также частного сектора, проходившем в Португалии в июле 2009 г., и на практическом семинаре, состоявшемся в Страсбурге 3-4 сентября при участии представителей учебных заведений, судей и прокуроров из вышеперечисленных стран, частного сектора, а также Европейской сети по подготовке судей и Лиссабонской сети Совета Европы [3].

Этот процесс с участием многочисленных заинтересованных сторон впервые привел к разработке концепции подготовки судей и прокуроров по вопросам киберпреступности и использования электронных доказательств. Коллективный характер этого процесса, несомненно, будет способствовать сотрудничеству между разными заинтересованными сторонами и выработке согласованной стратегии использования знаний и опыта при применении настоящей концепции.

Лиссабонская сеть Совета Европы одобрила настоящую концепцию в сентябре 2009 г. и рекомендовала ее для широкого распространения и применения учебными заведения по подготовке судей. Она приняла решение привлечь к ней внимание Консультативного совета европейских судей и Консультативного совета европейских прокуроров, а также Европейской комиссии по эффективность правосудия (ЕКЭП), чтобы обеспечить самую широкую поддержку настоящей концепции.

.

[3] Лиссабонская сеть для обмена информацией между частными лицами и юридическими лицами, отвечающими за подготовку судей.

3 Учебные заведения[4] и системы

В Европе, а также в других регионах существуют разнообразные системы подготовки судей и прокуроров.[5]

Что касается начальной подготовки, то, как правило, эти системы включают один или несколько следующих элементов[6]:

- Система A: Слушатели, получившие университетское образование, которые, как правило, после успешной сдачи вступительного экзамена проходят специальный курс подготовки в юридическом учебном центре, чтобы стать судьями и/или прокурорами. Иногда будущие судьи и прокуроры учатся вместе, а иногда в разных учебных заведениях.
- Система B: Слушатели, получившие университетское образование, получают практический опыт на рабочем месте (иногда в рамках прохождения официальной стажировки) в прокурорских службах, юридических конторах или в других учреждениях, чтобы затем сдать экзамен на получении квалификации для работы адвокатами, прокурорами и судьями. Это не связано с централизованной подготовкой в специальном учебном заведении[7].

Переподготовка, то есть дальнейшее профессиональное обучение работающих судей и прокуроров, проводится в государственных юридических учебных заведениях, которые также отвечают за начальную подготовку (например, во Франции, Грузии, Нидерландах, Польше, Португалии, Румынии, Испании, «бывшей югославской Республике Македонии», Хорватии), в учебных заведениях, которые специально были созданы для переподготовки кадров (например, в Германии), или в других государственных учреждениях, неправительственных организациях, международных организациях или в частном секторе. В некоторых случаях это предусмотрено в ежегодных учебных планах или в рамках специальных программ. В большинстве случаев переподготовка является необязательной, если только судьи и прокуроры не выполняют свои обязанности в специализированных судах (например, в Румынии).

---

[4] В целях настоящего документа термин «учебное заведение» относится к любому учреждению, отвечающему за обучение.

[5] Как отмечал Консультативный совет судей Совета Европы в 2003 г.: «В европейских странах наблюдаются существенные различия в вопросах начальной подготовки и переподготовки судей. Эти различия отчасти могут быть связаны с особенностями разных судебных систем, но в определенном отношении не представляются неизбежными и необходимыми. В одних странах проводится долгосрочное официальное обучение в специализированных заведениях, за которым следует интенсивная дальнейшая подготовка. В других странах проводится стажировка под контролем опытного судьи, который передает знания и дает профессиональные рекомендации на основании конкретных примеров, показывающих, какой подход следует применять и как следует избегать нравоучительности. Страны прецедентного (общего) права в значительной мере полагаются на продолжительный профессиональный опыт, как правило, в сфере адвокатской практики. Наряду с этими вариантами существует широкий перечень стран, где подготовка в различной мере носит организованный и обязательный характер».
Заключение № 4 Консультативного совета европейских судей (CCJE) для Комитета министров Совета Европы по надлежащей начальной подготовке и переподготовке судей на национальном и европейском уровнях (CCJE (2003) Заключение № 4; ноябрь 2003 г.).

[6] Более подробную информацию см. в Приложении.

[7] Следует упомянуть об особенностях систем общего права. Например, в Великобритании судей назначают на неполное рабочее время сроком не менее одного месяца в год, а затем большинство из них назначают на полную ставку. Кроме того, на неполный рабочий день назначают членов трибуналов (гражданское право) и судов магистрата (в основном, уголовное право). До любого назначения и во время пребывания в должности проводятся отдельные программы подготовки.

Учебный план по начальной подготовке и переподготовке в большинстве случаев требует официального рассмотрения и одобрения, хотя в отношении переподготовки применяется более гибкий подход. Например:

- Во Франции учебный кур проводится после консультаций с участием судебного персонала и представителей департаментов министерства юстиции. Затем программу подготовки подают на одобрение Совета директоров учебного заведения.
- В Германии за разработку учебного курса переподготовки в академии отвечает Программная конференция Немецкой академии по подготовке судей, в состав которой входят представители разных административных органов системы правосудия, а также профессиональных ассоциаций судей и прокуроров.
- В Польше к 30 апреля каждого года департаменты министерства юстиции, председатели судов и прокурорские службы подают свои предложения. На основании этих предложений директор Национальной школы представляет Программному совету план учебных мероприятий на следующий год, который должен быть одобрен к 30 июля. После одобрения министра юстиции учебный план направляют в соответствующие департаменты министерства юстиции, председателям апелляционных судов и государственным обвинителям апелляционных судов.
- В Румынии стратегию начальной подготовки и переподготовки утверждает Научный совет Национального института судей и Верховный совет судей.
- В Испании учебные планы и программы разрабатывает педагогический комитет, состоящий из экспертов по правовым вопросам, в рамках консультаций с ассоциациями судей или отдельными судьями. Учебный план по начальной подготовке и переподготовке судей окончательно одобряет Генеральный судейский совет.
- В Португалии учебную программу ежегодно тщательно продумывает и разрабатывает Центр судебных исследований. Программа начальной подготовки предусматривается законом, а программа переподготовки ежегодно меняется с учетом потребностей, выявленных на практике. Учебная программа принимается после консультаций с Верховными советами судей, Налоговыми и Административными судами и Прокурорской службой.
- В Бельгии общие и более специальные образовательные программы ежегодно разрабатывает или контролирует их разработку «Институт подготовки судей» (« Institut de formation judiciaire »). Этот институт был создан недавно в соответствии с законом от 31/01/07 и активно работает с начала 2009 г. Вопросы киберпреступности могут быть включены (нередко факультативно) в программы переподготовки.
- В Нидерландах Совет судей и Совет генеральных прокуроров (которые вместе являются образовательной организаций и обеспечивают работу Института по подготовке прокуроров и судей - SSR) принимают решение о наличии бюджета на проведение предлагаемых программ подготовки. Предложения могут поступать, например, от прокуроров, судей или лекторов SSR, и при наличии и выделении бюджета учебные программы затем разрабатывают соответствующие эксперты прокурорской службы, судьи и, при необходимости, третьи стороны, например, частные лица.
- В Хорватии учебный план начальной подготовки и планы переподготовки разрабатываются в рамках сотрудничества между Консультативным советом и Программным советом Юридической академии. Программный совет определяет приоритетные направления обучения и подает заявку на разработку проекта годового учебного плана профессиональной подготовки. Консультативный совет одобряет документ и направляет руководящие указания по разработке стратегии профессиональной подготовки. Члены двух советов являются видными экспертами в области права и представителями всех целевых групп Юридической академии.

Учебные заведения могут использовать опыт и знания независимых экспертов, в частности, если речь идет о специализированных или технических предметах, например, о киберпреступности и электронных доказательствах. Например:

- В Германии Академия по подготовке судей Германии широко использует привлеченных лекторов, большинство из которых являются профессионалами или исследователями в области права, но иногда для проведения занятий приглашают промышленных экспертов.
- В Нидерландах консультанты и промышленные эксперты принимают участие в разработке учебных курсов и в проведении учебных занятий.
- В Румынии Национальный институт судей пользуется услугами приглашенных преподавателей и лекторов по таким специализированным предметам, как киберпреступность (например, из Совета Европы, министерства юстиции США, ФБР, Секретной службы США, а также из частного сектора - компаний *eBay, Visa, American Express, Amazon, PayPal, Microsoft*), а также для подготовки преподавателей.
- В Испании Генеральный совет судей подписал договоры с компаниями частного сектора (*CYBEX, Logality*) о проведении подготовки по куберпреступности и киберкриминалистике. Кроме того, эксперты из частного сектора принимают участие в подготовке судебных работников.
- В Португалии большинство преподавателей Центра судебных исследований являются судьями или прокурорами. Для проведения занятий по переподготовке (например, семинаров или кратких курсов) Центр может приглашать преподавателей из частного сектора и других экспертов.
- В Хорватии в разработке и преподавании учебных курсов принимают участие специалисты из полицейских подразделений, которые борются с организованной преступностью и экономическими преступлениями.
- В Бельгии значительный процент бюджета, выделяемого на подготовку судей и прокуроров, находится в распоряжении университетов. Таким образом, у них есть возможность привлекать к проведению некоторых программ экспертов из частного сектора.

Суть подготовки судей и прокуроров по вопросам киберпреступности и электронных доказательств заключается в следующем:

- Судьи и прокуроры, как правило, начинают получать свое образования с изучения права на уровне университета. Следует отметить, что чем больше вопросов, связанных с киберпреступностью и электронными доказательствами, будут регулироваться законом, тем более широкое освещение получат эти вопросы в учебниках и учебных планах в области права. Вместе с тем, возможно, было бы полезно направить предложения по этим вопросам лицам, ответственным за подготовку материалов для университетских курсов.
- В странах, где начальная подготовка проводится в юридических учебных заведениях, было бы целесообразно включить в учебные планы вопросы, связанные с киберпреступностью и электронными доказательствами.
- Это в меньшей степени актуально в тех случаях, когда начальная подготовка проводится на рабочем месте.
- В большинстве стран существуют юридические учебные заведения, которые проводят курсы начальной подготовки, и было бы целесообразно включить в их учебные планы вопросы, связанные с киберпреступностью и электронными доказательствами.
- Учитывая то, что программы переподготовки носят нерегулярный характер, необходимо ввести официальные процедуры одобрения и внесения в учебные планы вопросов, связанных с киберпреступностью и электронными доказательствами и, таким образом придать им официальный статус.
- Программы переподготовки, как правило, носят необязательный характер. Задача заключается в том, чтобы убедить судей и прокуроров в необходимости обучения в таких технических областях, как киберпреступность и электронные доказательства[8].

[8] В Португалии программы переподготовки являются обязательными (т.е. каждый судья и прокурор должен посетить не менее двух учебных мероприятий в год), а в Румынии переподготовка может быть обязательной при определенных условиях.

- Необходимо использовать опыт и знания государственного и частного сектора и учитывать его при разработке учебных курсов, подготовке преподавателей и проведении учебных мероприятий.

4 Навыки и знания, необходимые судьям и прокурорам

Не вызывает сомнения тот факт, что все большее количество уголовных дел, а также многие гражданские и административные дела, рассматриваемые судами, будут в той или иной степени связаны с информационными и коммуникационными технологиями, и что большинство судей и прокуроров будут сталкиваться - если не с киберпреступностью – но с вопросами, касающимися электронных доказательств. Для этого недостаточно провести специализированную подготовку только судей и прокуроров.

Необходимы широкие массовые знания в области киберпреступности и электронных доказательств. Таким образом, всем или максимально возможному количеству судей и прокуроров необходимо пройти, по меньшей мере, базовую подготовку по вопросам, связанным с киберпреступностью и электронными доказательствами. Эти базовые знания необходимо предоставить во время начальной подготовки будущих судей и прокуроров и при проведении программ переподготовки практикующих судей и прокуроров.

В то же время, эти вопросы относятся к сфере высоких технологий, которые постоянно развиваются, и мы не можем рассчитывать на то, что судьи и прокуроры в целом смогут быть в курсе технических новинок на протяжении всей жизни. С учетом этого, необходимо предоставить знания на продвинутом уровне достаточному количеству судей и прокуроров, которые специализируются на вопросах киберпреступности и электронных доказательств.

4.1 Базовые знания

В большинстве судебных систем невозможно предсказать, какой судья будет рассматривать конкретное дело (принцип естественного права), и поэтому, в конечном счете, *все* судьи, судьи следственных органов и прокуроры должны обладать базовыми знаниями по вопросам, связанным с киберпреступностью и электронными доказательствами. «Базовые знания» означают, что они должны иметь представление о следующих аспектах:

- Компьютеры и сети: как они работают, базовые принципы функционирования Интернета, роль поставщиков услуг, конкретные задачи судей и прокуроров;
- Киберпреступность: какие информационные и коммуникационные технологии используются для совершения преступления;
- Законодательство о киберпреступности: национальное законодательство (включая прецедентное право) и международные стандарты;
- Юрисдикция и территориальная компетентность;
- Электронные доказательства: технические процедуры и правовые соображения.

В результате прохождения базового курса судьи и прокуроры должны уметь:

- Сопоставлять преступное поведение с положениями национального законодательства;
- Одобрять методы расследования;
- Отдавать распоряжения о поиске и изъятии компьютерных систем для получения электронных доказательств;
- Содействовать международному сотрудничеству;
- Опрашивать свидетелей и экспертов;
- Представлять/обосновывать электронные доказательства.

Ниже приводится пример типичного курса базовой подготовки для судей и прокуроров.

Пример: Подготовка по вопросам киберпреступности и электронным доказательствам – типичный модуль базовых знаний

Цель курса	После окончания курса обучения судьи и прокуроры должны обладать базовыми знаниями о том, что представляет собой киберпреступность и электронные доказательства, как судьи и прокуроры могут рассматривать эти вопросы, какие положения материального и процессуального права, а также какие методы можно применять, насколько оперативными и эффективными были принятие меры и насколько широким было международное сотрудничество.
Занятие 1	О киберпреступности
	➢ Почему киберпреступность вызывает беспокойство? ➢ Что такое «киберпреступность»? ➢ Задачи судей и прокуроров. ➢ Национальное законодательство и международные стандарты.
Занятие 2	Технология
	➢ Функционирование Интернета (базовые принципы) ➢ Глоссарий терминов ➢ Протоколы
Занятие 3	Киберпреступление как уголовное преступление в национальном законодательстве
	➢ Преступления против компьютерных данных и систем ➢ Компьютерное мошенничество и фальсификация ➢ Преступление, связанные с контентом (детская порнография, ксенофобия, расизм) ➢ Преступления, связанные с правом на интеллектуальную собственность ➢ Судебные постановления/прецедентное право
Занятие 4	Электронные доказательства
	➢ Об электронных доказательствах: определения и характеристики ➢ Требования к электронным доказательствам ➢ Криминалистическая компьютерная экспертиза
Занятие 5	Процессуальное право/методы расследования
	➢ Юрисдикция и территориальная компетенция ➢ Оперативное сохранение компьютерных данных ➢ Судебные приказы/ордеры ➢ Поиск и изъятие компьютерных данных ➢ Перехват данных о трафике и контенте ➢ Меры по обеспечению безопасности
Занятие 6	Взаимодействие с частным сектором
Занятие 7	Международное сотрудничество
	➢ Конвенция о киберпреступности как базовый документ для развития международного сотрудничества ➢ Общие принципы ➢ Временные меры и роль круглосуточных контактных пунктов ➢ Взаимная правовая помощь и роль компетентных органов
Занятие 8	Оценка результатов и выводы
Логистика и материалы	Занятия можно проводить в онлайновом режиме или в аудитории. Если занятия проводятся в аудитории: ➢ Учебной аудитории с компьютером и проектором для презентаций будет достаточно (поскольку курс не включает практических упражнений, т.е. демонстрации программного обеспечения для криминалистической компьютерной экспертизы или методов расследования, то компьютерная

	лаборатория не требуется); ➢ Соответствующие выдержки из национального материального и процессуального законодательства; ➢ Будапештская конвенция о киберпреступности, включая пояснительный доклад; ➢ Папка с глоссарием терминов и другой исходной информацией; ➢ Если лекция читается на иностранном языке, необходимо обеспечить устный перевод и перевод материалов.

4.2 Знания на продвинутом уровне

Иногда для ведения судебного дела о киберпреступлении базовых знаний недостаточно. В таких ситуациях необходимо, чтобы значительное количество судей, судей следственных органов и прокуроров обладали знаниями на продвинутом уровне, чтобы проводить расследование, судебное преследование и выносить решения по сложным делам, связанным в киберпреступлением и электронными доказательствами, или оказать содействия другим прокурорам и судьям.

В одних странах были созданы специализированные судебные подразделения или департаменты (например, в Румынии, Сербии), в других странах более крупные судебные службы имеют в своем распоряжении несколько специально подготовленных прокуроров. В Нидерландах проводится программа «intensiveringsprogramma», которая, среди прочего, призвана обеспечить наличие, по меньшей мере, одного специально подготовленного прокурора по вопросам киберпреступности в каждом из 11 крупных офисов. В Италии в соответствии с новым законодательством о киберпреступности было создано 29 прокурорских служб, которые обладают юрисдикцией по вопросам киберпреступности. В Португалии в Лиссабонской окружной службе судебного преследования имеется специализированный отдел по компьютерным преступлениям, где проводятся такие расследования.

В некоторых странах специальные прокуроры могут контролировать работу полицейских подразделений, занимающихся преступлениями в сфере высоких технологий. В большинстве стран службы судебного преследования организованы по иерархическому принципу, когда старший прокурор может поручить дело специально подготовленному прокурору. Таким образом, можно выявить прокуроров, которые должны обладать знаниями на продвинутом уровне.

Что касается судей, то в некоторых странах дела, связанные с киберпреступностью, можно поручить специально подготовленному судье в суде, который рассматривает конкретные виды преступлений, например, дела, связанные с организованной преступностью. Примером (возможно, единственным в Европе) может служить Сербия, где специальный департамент окружного суда Белграда занимается делами, связанными с киберпреступностью. Однако, учитывая то, что в большинстве судебных систем преобладает принцип естественного права, необходимо избрать иной подход. В Нидерландах, пожалуй, в единственной стране в Европе, было создано пять центров со специально подготовленными судьями, которые оказывают содействие другим судьям. В Испании аналогичное предложение обсуждается в Генеральном судейском совете, согласно которому группа судей, специализирующихся на вопросах киберпреступности и электронных доказательствах, будет оказывать содействие и проводить консультации для других судей. В Бельгии не существует специализации, предусмотренной законом, но большинство судов могут попросить одного или более своих членов пройти специальных курс подготовки. Вместе с тем, тот факт, что эти дела передают специально подготовленным судьям, является лишь вопросом внутренней организации работы суда. Иногда компетенцию по рассмотрению таких дел по закону предоставляют специальным судам страны (Брюссель). Однако в большинстве случаев компетенция определяется по месту совершения преступления, где не всегда имеется специально подготовленный прокурор или судья. Во многих странах суды могут рассматривать преступления, связанные с киберпреступностью, гораздо чаще, чем в других странах, что требует и более высокого уровня специализации.

«Знания на продвинутом уровне» означают, что судьи и прокуроры должны иметь практические знания и уметь применять полученные знания по следующим вопросам:

- Компьютеры и сети:
  - Глоссарий компьютерной лексики и терминов в области киберпреступности;
  - Функционирование Интернета;

- Протоколы и технология;
- Роль поставщиков услуг.

- Киберпреступность:
  - Тенденции в области киберпреступности;
  - Типология: конкретные типы и методы совершения киберпреступлений (например, «фишинг» или Интернет-мошенничество в целях получения личных данных, бот-сети и другие вредоносные программы, детская порнография);
  - Практические примеры и имитационные модели.

- Законодательство о киберпреступности:
  - Национальное законодательство и прецедентное право;
  - Международное сотрудничество: международные и двусторонние договоры, каналы судебного сотрудничества и практические методы оперативного сотрудничества.

- Расследование и электронные доказательства:
  - Юрисдикция и территориальная компетенция;
  - Положения процессуального права и их практическое применение;
  - Методы поиска, изъятия и хранения электронных доказательств;
  - Характеристики компьютерного обеспечения для проведения криминалистической компьютерной экспертизы;
  - Выявление подозреваемых лиц;
  - Отслеживание потоков денежных средств преступного происхождения;
  - Меры и условия обеспечения безопасности;
  - Представление электронных доказательств в суде.

Пример: Подготовка по вопросам киберпреступности и электронным доказательствам – типичный модуль получения знаний на продвинутом уровне [9]

Задача курса	После окончания курса обучения судьи и прокуроры должны обладать и применять на практике знания на продвинутом уровне по следующим вопросам: функционирование компьютеров и сетей, понятие киберпреступности, законодательство о киберпреступности, юрисдикция, методы расследования и электронные доказательства, международное сотрудничество.
Занятие 1	Компьютеры и сети
	➢ Глоссарий компьютерной лексики и терминов в области киберпреступности ➢ Функционирование ИКТ/инфраструктуры Интернета - Протоколы и технология - Как компьютеры обеспечивают коммуникации - Расследование IP и электронные доказательства – количество и названия компьютеров - Роль поставщиков услуг ➢ Информация об Интернете - Сбор информации - Использование (скрытых) баз данных в Интернете ➢ Характеристики социальных групп - Методы коммуникаций ➢ Методы сохранения анонимности ➢ Определение/выявление местонахождения и данных о компьютерах, компаниях или лицах в Интернете
Занятие 2	Киберпреступность и риски для безопасности
	➢ Тенденции в сфере киберпреступности

[9] Основан на ответах на вопросы анкеты и на примере, предоставленном Нидерландами.

	➢ Типология: конкретные типы и методы совершения киберпреступлений (например, «фишинг» или Интернет-мошенничество в целях получения личных данных, бот-сети и другие вредоносные программы, детская порнография) ➢ Как преступники использую информационные и коммуникационные технологии ➢ Правонарушители ➢ Последствия киберпреступлений ➢ Как повысить безопасность ИКТ ➢ Практические примеры и имитационные модели
Занятие 3	Законодательство о киберпреступности: материальное уголовное право
	➢ Преступление против компьютерных данных и систем ➢ Компьютерное мошенничество и фальсификация ➢ Преступления, связанные с контентом (детская порнография, язык вражды) ➢ Преступления, связанные с правом на интеллектуальную собственность ➢ Судебные постановления/прецедентное право
Занятие 4	Расследование и электронные доказательства
	➢ Электронные доказательства - Следы/отпечатки в компьютерах, Интернете, при цифровых коммуникациях - Меры по поиску, изъятию и хранению электронных доказательств - Характеристики программного обеспечения для криминалистической компьютерной экспертизы - Выявление подозреваемых лиц - Отслеживание потоков денежных средств преступного происхождения - Меры и условия обеспечения безопасности - Ведение/подготовка дела - Представление электронных доказательств в суде ➢ Организация и применение права в отношении киберпреступлений/электронных доказательств ➢ Рассмотрение дел
Занятие 5	Законодательство о киберпреступности: процессуальное право
	➢ Оперативное хранение компьютерных данных ➢ Подготовка приказов ➢ Поиск и изъятие компьютерных данных ➢ Перехват трафика и контента данных ➢ Меры по обеспечению безопасности ➢ Взаимодействие с Интернет-провайдерами/частным сектором ➢ Рассмотрение дел
Занятие 6	Юрисдикция и территориальная компетенция
	➢ Общие принципы ➢ Юрисдикция в сфере киберпреступности – проблемные аспекты ➢ Положения о юрисдикции в Конвенции о киберпреступности ➢ Рассмотрение дел
Занятие 7	Международное сотрудничество
	➢ Конвенция о киберпреступности как базовый документ для развития международного сотрудничества ➢ Общие принципы ➢ Временные меры, роль круглосуточных контактных пунктов, сотрудничество с полицией ➢ Взаимная правовая помощь и роль компетентных органов ➢ Рассмотрение дел

Занятие 8	Оценка результатов и выводы
Логистика и материалы	Занятия можно проводить в онлайновом режиме или в аудитории. При проведении занятий аудитории необходимо следующее: ➢ Учебная аудитория с компьютером и проектором для презентаций ➢ Было бы полезно, если бы у слушателей был компьютер с доступом в Интернет (но это необязательное условие) ➢ Соответствующие выдержки из национального материального и процессуального законодательства ➢ Будапештская конвенция о киберпреступности, включая пояснительный доклад ➢ Папка с глоссарием терминов и другой исходной информацией ➢ Если лекции читаются на иностранном языке, необходимо обеспечить устный перевод и перевод всех материалов.

Судьям и прокурорам, как правило, не требуются такие технические навыки и знания, которые необходимы следователям, занимающимся расследованием преступлений в сфере высоких технологий и криминалистической компьютерной экспертизой. Тем не менее, возможно, было бы полезно напомнить о необходимости усилий, направленных на регулярное проведение программ подготовки для работников правоохранительных органов.

На средства, предоставленные Европейской комиссией (Программа Фальконе, 2002 г.), Ирландская служба полиции (Гарда Сиочана) при участии экспертов из 10 государств-членов ЕС возглавила проект, в рамках которого была разработана стандартизированная базовая программа по киберпреступности (1-ый уровень) для работников правоохранительных органов. С 2004 г. двухнедельный курс подготовки проводился во многих европейских и неевропейских странах. Курс был аккредитован в Университетском колледже Дублина в 2006 г. (University College Dublin).

В ходе реализации дальнейших проектов Ирландской службой полиции в партнерстве с Университетским колледжем Дублина были разработаны дополнительные промежуточные и продвинутые модули для аккредитации программы на получение степени магистра по криминалистической компьютерной экспертизе и расследованию для сотрудников правоохранительных органов во всем мире. Существующие промежуточные модули для сотрудников правоохранительных органов включают следующие компоненты:

- Расследования, связанные с Интернетом;
- Расследования, связанные с использованием компьютерных сетей;
- Криминалистическая экспертиза файловой системы новых технологий (NTFS);
- Криминалистическая экспертиза данных под операционной системой Linux;
- Криминалистическая экспертиза системы мобильной телефонной связи;
- Беспроводные локальные сети и передача голоса через Интернет (LANS и VOIP);
- Скриптинг на продвинутом уровне;
- Криминалистическая экспертиза онлайновых данных;
- Криминалистическая экспертиза данных под операционной системой Microsoft Vista.

Эти модули постоянно обновляются, а также разрабатываются дополнительные модули.[10]

В июле 2007 г. Европол создал Группу по гармонизации подготовки в области киберпреступлений, главной целью которой является координирование усилий по проведению программ подготовки по расследованию преступлений в области высоких

[10] К числу других примеров относятся программы борьбы с преступностью в области высоких технологий, разработанные Службой поддержки национальной полиции Великобритании (UK National Policing Improvement Agency).

технологий в ЕС, чтобы разработать сертифицированную учебную программу для следователей правоохранительных органов Европы и распространить ее за пределами ЕС, чтобы помочь правоохранительным органам других стран, которые заинтересованы в этом. В число партнеров входят Европейская комиссия, Европейское бюро по борьбе с мошенничеством (OLAF), Агентство Евросоюза по координации национальных систем правосудия (Eurojust), Европейский колледж полиции (CEPOL), Интерпол, Совет Европы, ООН, Центр расследования киберпреступлений в Университетском колледже Дублина, Технологический университет в Труа, Кентерберийский университет в Крайстчерче, Болонский университет, а также представители промышленности.

4.3 Специализированные знания

Некоторые судьи и прокуроры могут получить специальные знания в рамках программ для аспирантов, с помощью самообразования, сетевого взаимодействия или на основе профессионального опыта. Эти знания не будут являться частью обычных программ подготовки. Судьи и прокуроры, обладающие такими специализированными знаниями, служат ценным источником информации для других и занимаются преподаванием.

5 Текущая подготовка по вопросам киберпреступности и электронным доказательствам

5.1 Начальная подготовка

«Начальная подготовка» означает подготовку слушателей после получения университетского юридического образования, чтобы они могли стать судьями и прокурорами. Во многих системах начальная подготовка проводится в юридических учебных заведениях в течение 1-3 лет; в некоторых странах такая начальная подготовка включает более или менее формализованные практические занятия на рабочем месте без специального учебного плана.

В большинстве стран вопросы о киберпреступности и электронных доказательствах не рассматривают в ходе начальной подготовки или изучают в крайне ограниченном объеме. Например:

- Во Франции программа подготовки по процессуальному праву в Национальной школе судей (Ecole Nationale de la Magistrature (ENM) включает трехчасовую лекцию специалиста по ИТ по вопросам поиска электронных доказательств и технологии, а вопросы киберпреступности вообще не рассматриваются.
- В Грузии эти вопросы не включены в программу начальной подготовки прокуроров, но при подготовке судей и работников судов на эти вопросы отведено полдня.
- В Германии не существует требования о практической подготовке на рабочем месте.
- В Хорватии, Польше и Румынии эти темы не включены в программы начальной подготовки.

Однако в некоторых странах вопросы киберпреступности и электронных доказательств являются неотъемлемой частью программ начальной подготовки. Например:

- В Нидерландах программа начальной подготовке включает однодневный базовый курс по киберпреступности, который преподается в Институте по подготовке прокуроров и судей (SSR) в Утрехте или в Зютфене и включает учебные пособия и другую исходную информацию. Курс включает интерактивные семинары и рассмотрение дел. Кроме этого, помимо однодневного базового курса и тщательной подготовки в течение четырех дней, программа включает двухдневный мастер-класс.

- В Испанской школе судей проводится курс начальной подготовки по киберпреступности и электронным доказательствам для недавно назначенных судей, который включает вопросы процессуального и материального права. Он является частью обязательной программы подготовки по процессуальному праву и сбору доказательств. Вопросы киберпреступности и электронных доказательств освещаются на семинарах в течение четырех дней, которые включают аспекты национального законодательства, инструменты международного сотрудничества, демонстрацию программы для проведения криминалистической компьютерной экспертизы и методы расследования, изъятия электронных доказательств и рассмотрение конкретных дел. Кроме того, раз в год проводится специальный семинар по электронным доказательствам, а также еще один семинар по материальному праву (преступления, совершенные с помощью электронных средств). Эти семинары проводят специалисты в области права и ИТ. Кроме того, судьи имеют доступ к виртуальной библиотеке по электронной преступности. Целью этого курса начальной подготовки является предоставление базовых знаний.

- В «бывшей югославской Республике Македония» Академия по подготовке судей и прокуроров проводит курс начальной подготовки по киберпреступности и электронным

доказательствам в рамках учебной программы по уголовному праву, ИТ и проведению обысков. Десять часов отводится на киберпреступность и электронные доказательства.

- В Португалии киберпреступность не является специальной и самостоятельной дисциплиной в учебном плане. Однако в разделе, посвященном уголовному расследованию, проводится специальный семинар (полтора часа учебного времени) по киберпреступности и электронным доказательствам. Во время занятий по уголовному праву и уголовно-процессуальному праву 9 часов отводится на компьютерные преступления и процессуальные аспекты получения электронных доказательств, и 9 часов посвящены ИКТ.

Эти занятия проводят штатные преподаватели, судьи, прокуроры или адвокаты, обладающие опытом в этой области, сотрудники специализированных полицейских подразделений, эксперты в области ИТ или специалисты из частных компаний.

Имеющаяся информация позволяет сделать следующие выводы:

- Учитывая задачу по предоставлению всем судьям и прокурорам базовых знаний в области киберпреступности и электронных доказательств, предлагаемые программы подготовки носят весьма ограниченный характер.
- За крайне незначительным исключением, программы начальной подготовки включают лишь базовые знания, и проведение программ подготовки на продвинутом уровне не предусматривается.
- Стандартизированные учебные пособия для тиражирования знаний, как правило, отсутствуют.

5.2 Переподготовка

Программы переподготовки, т.е. дальнейшего профессионального обучения действующих судей и прокуроров, проводятся государственными юридическими учебными заведениями, а также могут проводиться рядом других организаций. Например:

- Во Франции Национальная школа подготовки судей проводит в школе пятидневный семинар на продвинутом уровне, а также предлагает двухдневную стажировку в бюро по борьбе с преступностью в сфере высоких технологий министерства внутренних дел (OLCTIC). Расходы (около 5000 евро за курс) покрываются за счет школы. В качестве преподавателей работают судьи, прокуроры, сотрудники полиции, эксперты в области ИТ или отобранные эксперты из промышленности.

- В Грузии Высшая школа судей является единственным учебным заведением, отвечающим за переподготовку судей. В ней проводятся двухдневный базовый курс по киберпреступности, который финансируется из государственного бюджета. В качестве преподавателей работают члены профессорско-преподавательского состава и судья Верховного и апелляционных судов. Подготовку прокуроров проводит учебное подразделение министерства юстиции, но курсы по киберпреступности и электронным доказательствам пока не были организованы.

- В Германии программы переподготовки судей и прокуроров проводит Академия по подготовке судей Германии, которая организует около 150 мероприятий в год. В 2009 г. два из этих учебных мероприятий посвящены киберпреступности, и каждое из них проводится в течение 4 дней. Как правило, занятия проводят прокуроры и судьи, обладающие опытом в области киберпреступности, а также сотрудники полиции, таможни, налоговых органов и т.п. Расходы на подготовку покрывают федеральные и

местные органы государственного управления. На этих курсах слушатели получают базовые знания и знания на продвинутом уровне.

- В Нидерландах, несмотря на то, что программы переподготовки носят необязательный характер, каждый судья должен ежегодно проходить подготовку в течение определенного количества учебных часов. Каждый судья может решить, какой курс (курсы) ему выбрать. Институт по подготовке судей и прокуроров (SSR), а также несколько других учебных заведений и образовательных центров послевузовской подготовки проводят программы переподготовки по киберпреступности и электронным доказательствам на базовом и продвинутом уровнях. Ежегодно SSR предлагает три базовых курса, три курса углубленного обучения и один мастер-класс. В качестве преподавателей работают специалисты из национальной службы уголовного преследования, а также эксперты из частных компаний и промышленности. Кроме того, SSR также предлагает широкий перечень других курсов подготовки, охватывающих правовые и практические аспекты (всего около 400 курсов). Таким образом, подготовка по вопросам киберпреступности должна конкурировать со всеми этими курсами.

- В Польше Польская национальная школа судей и прокуроров проводит курсы подготовки на базовом и продвинутом уровнях в форме конференции, которая продолжается 4-5 дней. В 2009 г. было организовано два таких мероприятия («Методика преступлений, совершенных с использованием информационных систем», «Электронные доказательства во время слушания дела»).

- В Румынии Национальный институт судей проводит программу переподготовки, но только на базовом уровне. Например, с 2006 по 2009 гг. ежегодно проводилось по два двухдневных семинара, каждый из которых был рассчитан примерно на 25 судей/прокуроров. Они финансировались в основном из бюджета Национального института, частично за счет средств Европейской комиссии (PHARE) и частично за счет поддержки (в 2006 г.) компании *eBay*. В качестве преподавателей работали румынские судьи, специалисты в области ИТ, а также иностранные эксперты, финансирование которых осуществляли такие организации, как Совет Европы. Более того, киберпреступность является обязательным предметом децентрализованных программ подготовки на уровне отделов судебных расследования при апелляционных судах. Эти программы также координирует Национальный институт судей.

- В Испании Испанская школа судей при Генеральном совете судей проводит курсы переподготовки судей по киберпреступности и электронным доказательствам. Для прокуроров эти программы подготовки предлагает Центр правовых исследований при министерстве юстиции. В обоих случаях программы подготовки организованы в сотрудничестве с *CYBEX*, частной компанией, специализирующейся на этих вопросах. Бюджет Школы судей на программы обучения по киберпреступности составляет около 42.000 евро. Также возможно финансовая поддержка со стороны частного сектора. Программы переподготовки проводятся на базовом уровне, продолжаются 3-4 дня и включают лекции и анализ практических дел. Для слушателей издаются учебные пособия, которые, как правило, получает каждый судья. В 2008 и 2009 гг. ежегодно проводилось по два таких семинара. Несмотря на то, что некоторые вопросы изучаются достаточно глубоко, регулярные учебные программы на продвинутом уровне пока не проводятся.

- В Португалии программы переподготовки по киберпреступности проводит Центр исследований судебной системы, который организовывает около 30 мероприятий в год. Два их них регулярно посвящены основным проблемам киберпреступности. Иногда проводятся другие семинары на смежные темы, например, авторское право в онлайновой сети или технология и суды. Занятия проводят судьи и прокуроры, юристы, сотрудники полиции и эксперты из государственного и частного секторов. Семинары пользуются

популярностью и привлекают большое количество участников (в основном, прокуроров, но также адвокатов и судей уголовных судов).

- В Бельгии программа переподготовки до сих пор находится на этапе разработки, что связано с недавним созданием Института подготовки судей. Несомненно, задача заключается в том, чтобы организовать такой процесс обучения, в котором бы учитывались результаты и рекомендации ряда научно-исследовательских институтов и, в том числе, замечания Совета Европы. Институт может профинансировать участие бельгийских судей в программах подготовки за рубежом по их просьбе (например, один судья и один прокурор получили европейский сертификат по киберпреступности и электронным доказательствам, пройдя курс обучения в Париже в феврале 2009 г.).

- В настоящее время в Хорватии не проводятся программы переподготовки по киберпреступности и/или электронным доказательствам. Этот вопрос обсуждался только благодаря программе CARDS, в которой участвует Хорватия.

- В «бывшей югославской Республике Македония» не существует программ переподготовки.

- Программы подготовки предлагает Академия европейского права (ERA). ERA, официально созданная по инициативе Европейского парламента в 1992 г., направляет свою деятельность на предоставление углубленных знаний и проведение анализа европейского права и права Сообщества, организуя практические семинары и курсы для практикующих юристов. Академия также служит форумом для обмена опытом и мнениями о европейском праве и политике. ERA на регулярной основе организует открытые учебные мероприятия по киберпреступности, в которых участвуют слушатели из всех стран ЕС. В 2009-2010 гг. ERA также сотрудничает с Программой TAIEX (Техническое содействие в сфере информационного обмена), в рамках которой проводятся и будут проводиться циклы семинаров в Румынии, Болгарии, странах-кандидатах и странах потенциальных кандидатах на вступление в ЕС, чтобы ознакомить их с основными европейскими и международными инструментами борьбы с киберпреступностью.

  Все семинары предназначены для использования в качестве площадок для дебатов и оценки того, как европейское законодательство в области киберпреступности применяется в разных государствах-членах и странах-кандидатах, а также перспектив для проведения эффективной общеевропейской кампании против незаконного использования Интернета. В настоящее время обсуждаются такие недавно принятые европейские правовые акты, как Конвенция Совета Европы о киберпреступности (2001 г.), Рамочное решение Совета 2005/222/JHA об атаках на информационные системы и Рамочное решение Совета 2004/68/JHA о борьбе против сексуальной эксплуатации детей и детской порнографии. Также рассматриваются вопросы дальнейшего сотрудничества с поставщиками услуг и веб-компаниями *Google, Microsoft и Yahoo*!.

  На каждом семинаре используется программа, включающая комплексные методы обучения: вводные и более углубленные лекции, рассмотрение дел и другие виды интерактивного обучения. Особое внимание уделяется обсуждению в небольших рабочих группах. Курсы лекций и практические занятия проводят эксперты ЕС и национальные эксперты.

- В ряде стран учебные мероприятия финансируются частными компаниями. Например:

  В Германии компания *eBay* финансирует учебный курс «Новые СМИ и уголовное право» для судей и прокуроров, который организован Немецкой академией подготовки судей. Курс ведет преподаватель, который предоставляет информацию о рынке компании *eBay*, связанной с ним уголовной деятельностью, используемых мерах противодействия и взаимодействии компании с правоохранительными органами. Компания *eBay* также

участвовала в нескольких «одноразовых» курсах подготовки, которые были организованы Берлинским сенатом юстиции, в каждом из которых приняли участие около 100 прокуроров.

В Румынии компания *eBay* провела многочисленные учебные мероприятия для судей, прокуроров и сотрудников правоохранительных органов. В частности, компания *eBay* работала с Секретной службой США в Посольстве США, где проводился курс подготовки для 25 прокуроров из разных отделений DIICOT (Директорат по расследованию организованной преступности и терроризма), 15 судей и 20 сотрудников полиции в Сибиу. Кроме того, компания *eBay* принимала участие в организации дополнительных учебных мероприятий для судей в Таргу Жиу, а также для 60 судей из разных судов при апелляционном суде Крайовы.

Как отмечалось выше, практически во всех случаях внесение изменений или дополнений в учебные планы юридических учебных заведений требует проведения формальной оценки и процедур одобрения.[11]

Несмотря на то, что, несомненно, многие инициативы направлены на удовлетворение необходимости в проведении адекватных курсов подготовки по киберпреступности для судей и прокуроров, со всей очевидностью ощущается отсутствие согласованности между описанными выше подходами.

Даже принимая во внимание национальные особенности законодательства и тот факт, что системы образования существенно отличаются друг от друга, проблемы киберпреступности носят международный характер и их решение требует минимального уровня координирования усилий и согласованности действий между странами. Одинаковое понимание проблем киберпреступности в разных странах может только улучшить согласованность судебных постановлений и предотвратить создание «надежных убежищ» для преступников, предоставив учебным заведениям экономически выгодные качественные и содержательные учебные программы.

Имеющаяся информация позволяет сделать следующие выводы:

- Большинство курсов переподготовки предоставляют знания на базовом уровне.
- Проводится крайне мало курсов, которые охватывают лишь очень незначительное количество судей и прокуроров.
- В большинстве случаев базовые курсы не стандартизированы. Таким образом, их тиражирование не представляется возможным, и они не позволяют судье или прокурору пройти системный курс обучения от базового уровня до продвинутого уровня. Судя по всему, исключением являются Нидерланды.
- Учебные пособия носят разрозненный и бессистемный характер.

[11] В этой связи представляет интерес проект «Европейский сертификат по борьбе с киберпреступностью и использованию электронных доказательств ("European Certificate on the fight against cybercrime and the use of electronic evidence"), который осуществляет CYBEX при финансовой поддержки Европейской Комиссии (JPEN). Он включает четырехдневный стандартизированный базовый курс подготовки для судей, прокуроров и юристов. С начала 2009 г и по конец 2010 г. курс будет апробирован в 14 пилотных странах Европы и Латинской Америки. Его участники получат сертификат, свидетельствующий о том, что они получили базовые теоретические и практические, правовые и технические знания по вопросам, связанным с электронными доказательствами и киберпреступностью.
Совет Европы – в рамках Проекта по киберпреступности – также приступил к разработке учебного пособия для судей и прокуроров для использования во время двухдневного базового курса, посвященного законодательству о киберпреступности.

- Учитывая то, что, в конечном счете, всем судьям и прокурорам необходимо получить, по меньшей мере, базовые знания в области киберпреступности и электронных доказательств, предлагаемых программ подготовки явно недостаточно, особенно принимая во внимание то, что нынешнее поколение практикующих судей и прокуроров скорее всего не получили никакой начальной подготовки и не изучали эти темы во время учебы в университете.
- Несмотря на незначительные исключения, программы подготовки судей и прокуроров на продвинутом уровне отсутствуют.
- Принимая во внимание международный характер киберпреступности, необходимо обеспечить минимальный уровень координирования и согласованности действий между разными странами.

6 Предлагаемый подход

6.1 Цель

Как было продемонстрировано в предыдущем разделе, в целом существующие программы подготовки и переподготовки не дают судьям и прокурорам такого уровня знаний, который необходим для рассмотрения дел, связанных с киберпреступностью и электронными доказательствами.

Таким образом, концепция подготовки судей и прокуроров должна быть направлена на решение следующих задач:

- Предоставить возможность учебным заведениям проводить программы начальной подготовки и переподготовки по вопросам киберпреступности, основанные на международных стандартах;
- Вооружить максимально возможное количество будущих и практикующих судей и прокуроров базовыми знаниями по вопросам киберпреступности и электронных доказательств;
- Предоставить программы подготовки на продвинутом уровне значительному количеству судей и прокуроров;
- Стимулировать дальнейшую специализацию и техническую подготовку судей и прокуроров;
- Содействовать расширению знаний с помощью сетевого взаимодействия между судьями и прокурорами;
- Облегчить доступ к разным учебным инициативам и сетям.

Для достижения этих целей следует принять следующие меры:

6.2 Институционализация начальной подготовки

- Странам, где начальная подготовка представляет собой практическое обучение на рабочем месте (прохождение практики или стажировки) без формально оформленного учебного плана, рекомендуется, чтобы, по меньшей мере, часть этого обучения (например, одна стажировка или аналогичный тренинг) была связана с киберпреступностью и электронными доказательствами.

- Странам, где начальная подготовка проводится в юридических учебных заведениях, необходимо принять следующие меры:
  - Их учебные планы должны включать, как минимум, один базовый модуль по киберпреступности и электронным доказательствам;
  - Эти проблемы следует дополнительно обсуждать при изучении обязательных модулей по материальному и процессуальному праву;
  - Необходимо предлагать факультативные модули для получения знаний о киберпреступности и электронных доказательствах на продвинутом уровне.

Следует стандартизировать специальные учебные модули таким образом, что бы их можно было тиражировать и предоставить возможность слушателям пройти курс обучения с базового уровня до продвинутого уровня. Тиражирование модулей означает, что их можно неоднократно использовать, по меньшей мере, в одной стране для разных слушателей, чтобы участники различных учебных мероприятий получили знания на одинаковом уровне. Это также означает, что обеспечивается стандартизация методов проведения подготовки. В целях обеспечения высокого качества подготовки после окончания каждого курса необходимо проводить оценку знаний.

6.3 Институционализация переподготовки

- Учебные заведения по переподготовке кадров должны предлагать, по меньшей мере, один базовый модуль по киберпреступности и электронным доказательствам, чтобы вооружить практикующих судей и прокуроров базовыми знаниями, если они не получили их во время прохождения курса начальной подготовки.

- Они должны также предлагать курсы подготовки на продвинутом уровне.

- И вновь: следует стандартизировать специальные учебные модули таким образом, чтобы их можно было тиражировать и предоставить возможность слушателям пройти курс обучения с базового уровня до продвинутого уровня. Для этого может возникнуть необходимость в максимально возможной гармонизации модулей программ переподготовки с модулями программ начальной подготовки. Необходимо также стандартизировать методы обучения и обеспечить контроль качества путем оценки знаний после окончания курсов.

- Для подготовки судей и следователей узкой специализации можно было бы способствовать проведению стажировок в подразделениях по борьбе с преступностью в сфере высоких технологий или организовать послевузовские курсы/программы.[12]

6.4 Стандартизация и тиражирование курсов/модулей

- Следует разработать стандартизированные курсы или модули, которые можно было бы эффективно тиражировать в широких масштабах, чтобы предоставить возможность слушателям и практикующим судьям и прокурорам пройти курс обучения с базового уровня до продвинутого уровня.

- Необходимо провести оценку существующих базовых курсов[13], которые можно было бы включить в учебные планы программ начальной подготовки и переподготовки. Стандартный курс впоследствии можно было бы рекомендовать учебным заведениям, проводящим программы начальной подготовки и переподготовки.

- Аналогичной оценке можно было бы подвергнуть курсы подготовки на продвинутом уровне и затем рекомендовать учебным заведениям стандартные курсы на продвинутом уровне.

- И, наконец, необходимо провести подготовку преподавателей, чтобы они могли вести такие курсы, чтобы занятия проводили местные преподаватели на местных языках при ограниченном участии международных тренеров.[14]

6.5 Доступ к учебным пособиям и материалам для самообучения

- Необходимо разработать учебные пособия, отражающие общие международные стандарты и передовую практику. Они должны быть предоставлены учебным заведениям по конкурентным ценам для распространения на местах. Несомненно, несмотря на то, что высокий уровень стандартизации возможен при разработке программ подготовки для

[12] Например, двухнедельный базовый курс, разработанный Ирландской службой полиции и Университетским колледжем Дублина (UCD), должен также представлять интерес для судей и прокуроров.

[13] Например, курс ECCE, разработанный и в настоящее время апробируемый CYBEX.

[14] Курс подготовки преподавателей был разработан UCD и ИНТЕРПОЛОМ, и его можно было бы использовать. Курс включает навыки преподавания, разработку курса и т.п. Этот курс НЕ предназначен исключительно для правоохранительных органов и может проводиться для всех.

сотрудников правоохранительных органов, в которых особый акцент делается на технологии и криминалистической экспертизе, это в меньшей степени относится к подготовке судей и прокуроров, которых, в первую очередь, необходимо научить применять национальное законодательство. Тем не менее, разработка стандартизированных учебных пособий возможна таким образом, чтобы осталось достаточно места для того, чтобы включить в них национальные системы и законодательство.

- В некоторых странах учебные пособия для судей и прокуроров имеются в онлайновом режиме.[15] Другие страны должны последовать этой практике.

- Необходимо разрабатывать и предоставлять онлайновые курсы.[16]

- Следует максимально облегчить доступ к учебным курсам (национальным и международным) с помощью упрощенных процедур одобрения.

6.6 Пилотные центры подготовки на базовом и продвинутом уровнях

- Следует создать ряд пилотных центров подготовки судей и прокуроров по вопросам киберпреступности и электронным доказательствам на базовом и продвинутом уровнях. Эти центры могли бы:
  - Апробировать и осуществлять дальнейшую разработку стандартизированных курсов и материалов;
  - Распространять передовую практику;
  - Проводить исследования в области обучения;
  - Вести учет преподавателей;
  - Проводить подготовку преподавателей;
  - Предоставлять программы подготовки другим странам с аналогичными системами и языками.

- Пилотные центры должны координировать свою работу друг с другом при поддержке Совета Европы.

- Судья и прокуроры, которые готовы стать специалистами, должны подумать об участии в учебных программах в центрах повышения квалификации для правоохранительных органов и промышленности.[17]

---

[15] Примерами служат Нидерланды и библиотека электронных доказательств CYBEX. В рамках проекта «2 центра», UCD будет разрабатывать онлайновые ресурсы для предоставления некоторых учебных пособий AGIS/ISEC.

[16] Например, в настоящее время UCD предлагает две программы MS, отдельные разделы которых полностью представлены в онлайновом режиме. В Португалии Центр подготовки судей намерен создать онлайновый курс «Суды и информационные и коммуникационные технологии», включающий модули по киберпреступности и электронным доказательствам. Курс будет подготовлен на португальском языке, и уже рассматривается возможность его использования в других странах, говорящих на португальском языке (например, в Бразилии, Кабо-Верде, Анголе, Мозамбике, Гвинеи-Биссау, Сан-Томе и Тиморе).

[17] Проект «2 Центра» (Центры повышения квалификации по вопросам киберпреступности сети аналитических исследований и образования) (2Centre initiative (Cybercrime Centres of Excellence Network for Training Research and Education) был запущен в марте 2009 г. (во время Конференции Совета Европы, «Октопус»). В рамках проекта *2Centre* «изучаются существующие методы подготовки правоохранительных органов и промышленности по вопросам криминалистической экспертизы ИТ и расследования киберпреступлений. Проект посвящен рассмотрению деятельности сотрудников правоохранительных органов и соответствующего персонала в промышленности, направленной на получение знаний и навыков в области, в которой в настоящее время существует разнообразные уровни

6.7 Расширение знаний за счет сетевого взаимодействия

Несмотря на то, что программы начальной подготовки и переподготовки позволяют судьям и прокурорам закладывать основы отношений, обмениваться мнениями между коллегами и налаживать сетевое взаимодействие, важнейшую роль также играет взаимодействие с широким кругом других заинтересованных сторон.

Таким образом:

- Судья и прокуроры должны использовать существующие сети для судей[18] или прокуроров (например, GPEN).[19]
- Совет Европы должен обсудить создание международной сети по киберпреступности или сети судей, занимающихся рассмотрением дел об электронных преступлениях (аналогичной сети GPEN для прокуроров).
- Взаимодействие между европейскими институтами, проводящими программы подготовки по вопросам киберпреступности и электронным доказательствам, должно опираться на поддержку Совета Европы и Европейской сети по подготовке судей.
- Чтобы облегчить судьям и прокурорам доступ к этим и многим другим сетям, связанным с киберпреступностью, Совет Европы - на своем сайте www.coe.int/cybercrime - должен составить список инициатив и сетей и создать портал с указанием ссылок, краткой информацией и контактными данными различных сетей. Это также будет способствовать координированию работы сетей. В дальнейшем это облегчит доступ к существующим учебным материалам и инициативам.

6.8 Государственно-частное сотрудничество

Структурированное и регулируемое сотрудничество между правоохранительными органами и частным сектором (отраслью ИКТ, включая Интернет-провайдеров) жизненно важно для расследования киберпреступлений и получения электронных доказательств[20], и частный сектор передает правоохранительным органам свои опыт и знания и оказывает другую поддержку их инициативам в области обучения.

Поддержка частного сектора в подготовке судей и прокуроров была бы полезной, учитывая то, что частный сектор обладает соответствующим опытом в области знания предмета. В то же время, судьи и прокуроры должны оставаться независимыми и беспристрастными.

профессиональной подготовки, обучения в собственном учреждении, перекрестного обучения и обучения на рабочем месте». Университетский колледж Дублина стал первым центром повышения квалификации, в 2010 г. вторым центром станет Университет в городе Труа.

[18] Складывается впечатление, что международной сети судей, охватывающей проблемы киберпреступности и электронных доказательств, пока не существует. Примером инициативы на национальном уровне могут служить Нидерланды, где был создан внутренний ресурс Интранет типа «вики».

[19] Глобальная сеть для прокуроров, занимающихся электронными преступлениями (GPEN), была создана в 2008 г. и поддерживается Международной ассоциацией прокуроров (IAP). Сеть облегчает информационный обмен и сотрудничество между прокурорами по делам, связанным с электронными преступлениями или киберпреступностью, принимая во внимание Конвенцию о киберпреступности, и способствует разработке и проведению учебных программ, предоставлению прокурорам онлайновых ресурсов. GPEN – это сеть для прокуроров, специализирующихся на электронных преступлениях, и каждый член IAP получает приглашение назначить, по меньшей мере, одного прокурора для регистрации в GPEN в качестве национального контактного лица. Работой сети руководит Правление развития GPEN, которое состоит из членов IAP.

[20] См. в качестве примера Руководящие принципы сотрудничества правоохранительных органов и Интернет-провайдеров, принятые на Конференции Совета Европы «Октопус» в апреле 2008 г.

Таким образом:

- Юридические учебные заведения могут использовать опыт и знания частного сектора при разработке учебных программ, подготовке учебных пособий и проведении курсов обучения.

- Поддержка учебных заведений со стороны промышленности не должна сводиться к принятию потенциально выгодных решений в суде или стимулировать развитие бизнеса, а призвана обеспечивать судей и прокуроров адекватной информацией, позволяющей им принимать информированные решения.

- Частный сектор мог бы оказывать прозрачную поддержку международным или национальным организациям, научному сообществу, инициативам в области образования и другим третьим сторонам, которые в свою очередь поддерживают учебные заведения.

- Судьи и прокуроры должны иметь общее представление об Интернете и киберпреступности, но не менее важно предоставить им платформу для специализированной информации. Промышленность могла бы предоставить материалы для конкретных модулей (а не для полного курса), посвященных функционированию соответствующих платформ.

7 Оказание поддержки в реализации настоящей концепции

Реализация настоящей концепции, в первую очередь, является ответственностью юридических учебных заведений, но также нуждается в поддержке государственных и частных институтов и партнеров, в том числе международных организаций. Принимая во внимание значение для общества информационных и коммуникационных технологий, финансирование таких мер по проведению подготовки станет ценным вложением наряду с усилиями, которые следует приложить, чтобы предоставить учебным заведениям необходимые ресурсы.

Совет Европы и Европейская сеть по подготовке судей, а также другие организации должны способствовать реализации настоящей концепции во всей Европе и за ее пределами.

Европейская сеть по подготовке судей и Совет Европы могли бы в ближайшем будущем организовать совместную конференцию для обсуждения этой концепции.

Совет Европы и Европейская сеть по подготовке судей должны регулярно проводить оценку достигнутых результатов.

Реализация концепции на практике также должна опираться на поддержку донорских организаций. Заинтересованные доноры и организации могли бы стать партнерами в разработке проектов оказания содействия учебным заведениям и другим заинтересованным сторонам, которые готовы взять на себя ответственность за принятие мер, предусмотренных концепцией.

Для снижения риска возникновения конфликта интересов или дискредитации беспристрастности судей и прокуроров, доноры не должны оказывать прямую поддержку, а могли бы предоставлять ресурсы через нейтральные третьи стороны, например, международные организации, которые затем взаимодействовали бы с учебными заведениями.

8 Приложение

8.1 Лиссабонская сеть: связи с юридическими учебными заведениями

В Лиссабонской сети представлены 44 из 47 государств-членов Совета Европы. Членами Лиссабонской сети являются соответствующие национальные институты, отвечающие за начальную и дальнейшую подготовку судей и прокуроров. В зависимости от обстоятельств, членами сети могут быть Школы по подготовке судей, Центры юридической подготовки или подразделения по подготовке судей при министерствах юстиции.

См. ниже более подробную информацию о каждой стране-члене сети (включая в некоторых случаях ассоциированные учебные программы):

- Албания Albania
- Андорра Andorra
- Армения Armenia
- Австрия Austria
- Азербайджан Azerbaijan
- Бельгия Belgium
- Босния и Герцеговина Bosnia and Herzegovina
- Болгария Bulgaria
- Хорватия Croatia
- Кипр Cyprus
- Чешская РеспубликаCzech Republic
- Дания Denmark
- Эстония Estonia
- Финляндия Finland
- Франция France
- Грузия Georgia
- Германия Germany
- Греция Greece
- Венгрия Hungary
- Исландия Iceland
- Ирландия Ireland
- Италия Italy
- Латвия Latvia
- Литва Lithuania
- Люксембург Luxembourg
- Мальта Malta
- Молдова Moldova
- Черногория Montenegro
- Нидерланды Netherlands
- Норвегия Norway
- Польша Poland
- Португалия Portugal
- Румыния Romania
- Российская Федерация Russian Federation
- Сербия Serbia
- Словакия Slovakia
- Словения Slovenia
- Испания Spain
- Швеция Sweden
- Швейцария Switzerland
- бывшая югославская Республика Македония "the former Yugoslav Republic of Macedonia"
- Турция Turkey
- Украина Ukraine
- Соединенное Королевство
  - Англия и Уэльс England and Wales
  - Шотландия Scotland

Наблюдатель

- Миссия ООН в Косово UNMIK

8.2 Примеры базовых учебных курсов: структура и тематика

8.2.1 Пример Нидерландов

Базовая подготовка – 1 день
Программа:

1 Общая ориентация:
- Что представляет собой киберпреступность?
- Проявление киберпреступности
- Законодательно-правовые рамки для правоприменения и судебного преследования

2 Правоприменение:
- Цифровое правоприменение как повседневная практика
- Методы правоприменения

3 Правоприменение (часть 2):
- Интернет и правоприменение в соответствии с Актом о специальных привилегиях правоприменения

Выводы + оценка

8.2.2 Пример Германии (Академия по подготовке судей Германии)

Базовая подготовка: ***«Формы проявления и стратегия борьбы с киберпреступностью»*** **– 4 дня**
Программа:

День 1:
- Уголовный кодекс Германии
- Использование Уголовного кодекса Германии в контексте компьютерной и Интернет-преступности
- Проблемы повседневного опыта работы в прокуратуре и суде

Лектор – судья Мюнхенского суда, специализирующийся на финансовых и экономических преступлениях, несколько лет назад был прокурором и занимался делами, связанными с киберпреступностью, шпионажем, коррупцией и т.п.

- Проблемы в повседневном опыте работы в прокуратуре и суде в Нидерландах
- Раскрытие и борьба с киберпреступностью в Европе
- Проблемы с провайдерами в Нидерландах и других европейских странах
- Конвенция Совета Европы о киберпреступности
- Важность и значение Конвенции о киберпреступности для Европы и остальных стран мира (Китай, США, Россия)

Лектор – профессор д-р Хенрик Касперсен, Нидерланды

День 2:
- Саботаж компьютерных систем
- Деятельность хакеров в Интернете
- Ловушки заказов в Интернете
- Шпионаж данных
- Компьютерное мошенничество с кредитными картами
- Атаки на банковские данные
- Фишинг- мошенничество и новые виды преступлений в Интернет
- Бот-сети
- Мошенничество в компании *eBay* или других платформ продаж

Лектор – сотрудник полиции из Немецкого штаба полиции (BKA), Висбаден

- Превентивные поиски в Интернет случаев организованной преступности, терроризма, жестоких преступлений, отмывания денежных средств и т.п.

- Поиск в Интернете объявлений лиц с приступнообразным сознанием (школы и т.п.)
- Поиск в Интернете детской порнографии
- Международное сотрудничество в сфере поиска в Интернете
- Онлайновый поиск (проблемы, связанные с конституцией)

Лектор – руководитель специального департамента Штаба баварской полиции (LKA), Мюнхен

День 3:

- Хранение и оценка данных в Германии и других странах
- Поиск данных в Интернет и отслеживание данных в сети
- Возможности криминалистической экспертизы ИТ и ограниченность анализа данных
- Системы размещения анонимных данных в Интернет
- Использование преступниками криптографии

Лектор – специалист Мюнхенского штаба полиции

- Новые правовые проблемы, связанные с хранением и оценкой Интернет-данных
- Компетенция по применению всех правовых мер поиска
- Компетенция по получению доказательств для расследования и суда
- Новые факторы в сфере правоприменения

Лектор – судья Баварского высшего уголовного суда в Бамберге

День 4:

- Российская предпринимательская сеть
- Интеркейдж
- Защита от диверсий в отношении компьютеров или данных
- Позитивное «хакерство»
- Значение и фальсификации при использовании машин для голосования
- Политическое влияние новых законов
- Население, которое сидит в стеклянном доме

Лектор – член известного *Chaos Computer Club* (CCC) в Гамбурге, члены клуба пытаются проникнуть в компьютеры правительства, Белого дома, ЦРУ. Клуб демонстрирует, как можно манипулировать водоснабжением в городе и т.п.

8.2.3 Примеры Совета Европы

1. Практический семинар по киберпреступности для прокуроров, Белу-Оризонти, Бразилия, 26 августа 2008 г. (организован *Ministério Publico Estadual Minas Gerais* совместно с Советом Европы)

Базовая подготовка – 1 день
Программа:

1 Открытие семинара
- Вступительное слово
- Текущие законодательные реформы

2 Киберпреступность: новое явление
- Обзор существующих угроз
- Конкретные угрозы и дела, расследованные в Бразилии

3 Материальное право: каков характер правонарушений?
- Международные стандарты
  - Типология, правовые концепции
  - Конвенция о киберпреступности

- Положения бразильского законодательства
  - Действующие положения
  - Проведение правовых реформ

4 Расследования и международное сотрудничество
- Роль прокуроров в расследовании киберпреступлений
- Национальное процессуальное право
- Процессуальные меры и международное сотрудничество в рамках Конвенции о киберпреступности

5 Государственно-частное партнерство
- Примеры государственно-частного партнерства в Бразилии
- Правоприменение – сотрудничество Интернет-провайдера при расследовании киберпреступлений: руководящие принципы
- Обсуждение: сотрудничество между правоохранительными органами и Интернет-провайдерами: опыт Бразилии

2. Киберпреступность: курс подготовки для судей, Каир, Египет, 9-10 июня 2008 г. (организован компанией *Microsoft* при содействии Совета Европы)
Настоящий кур проводился дважды для разных групп судей из коммерческих судов (они также отвечали за вопросы, связанные с электронными преступлениями)

Базовая подготовка – 1 день

Программы:

1 Открытие семинара

2 Киберпреступность: новое явление
- Обзор существующих угроз
- Конкретные угрозы
  - Мошенническое использование онлайновой идентификации и информации: примеры
  - Кредитные карты и другие виды мошенничества

3 Материальное право: каков характер правонарушений?
- Международные стандарты (эксперт Совета Европы)
  - Типология, правовые концепции
  - Конвенция о киберпреступности
  - Криминализация хищения персональных данных
- Положения национального законодательства
  - Действующие положения
  - Проведение правовых реформ

Часть 2 Доказательства в ходе судебного разбирательства дел, связанных с киберпреступностью

4 Расследование и уголовное преследование
- Процессуальные меры, предусмотренные Конвенцией о киберпреступности
- Роль полиции, прокуроров, судей, специализированных служб
- Национальное процессуальное право

5 Международное сотрудничество

- Конвенция о киберпреступности
- Положения национального законодательства и двусторонних договоров
- Круглосуточные контактные пункты
- Роль судей

6 Получение, сохранение, использование электронных доказательств

- Доказательства, находящиеся в компьютере обвиняемого: наличие цифровых файлов, использованных для киберпреступления
- Доказательства, идентифицирующие местонахождения сети: IP адреса
- Доказательства, полученные от Интернет-провайдеров

7 Судебное разбирательство и прецедентное право: примеры

8.3 Примеры курсов подготовки на продвинутом уровне: структура и тематика

8.3.1 Пример Нидерландов

Углубленная подготовка – 4 дня
Программа:

1-ый и 2-ой дни

Инфраструктура Интернета

- Представление о том, как работает Интернет
- Как связаны компьютеры?
- Что представляют собой IP-номера и компьютерные имена?

Информация об Интернете

- Как осуществлять сбор информации в Интернете
- Поиск (скрытых) баз данных в Интернете

Характеристики социальных сетей

- коммуникации
- анонимность
- определение местонахождения и идентификация компьютеров, компаний и лиц в Интернете

Цифровые следы

- Что представляют собой «следы»?
- Какие следы остаются в компьютере?
- Какие следы остаются в Интернете?
- Какие следы можно обнаружить в цифровых коммуникациях?

Безопасность

- Риски, связанные с Интернетом
- Важность надежной цифровой безопасности
- Безопасное хранение информации
- Безопасность электронной почты

В течение этих двух дней каждый участник получает доступ к компьютеру, подсоединенному к Интернет, и получает практический опыт по обсуждаемым темам. Участникам сообщают имя определенного лица и просят собрать о нем как можно больше информации из открытых источников в Интернет. Их также просят отследить отправителей электронных писем (с помощью заголовков электронных писем) или найти следы цифровых коммуникаций.

3-ий и 4-ый дни

Законодательно-правовая база

- Какой компетенцией обладают полиция и прокуроры при расследования дел, связанных с киберпреступностью
- Рассмотрение дела группой по преступлениям в сфере высоких технологий

Организация расследования и судебного преследования киберпреступности в Нидерландах;

Перехват (это не будет включено в новый курс, поскольку является частью базовой программы);

Цифровые встречные иски

- Какие встречные иски известны
- Прецедентное право в отношении встречных исков

- Какие встречные иски можно ожидать в будущем и какой будет реакция на них
- Рассмотрение дел

Каждый участник получает учебные пособия, папку, которая включает все темы, обсуждаемые во время семинара, и которую можно использовать как справочное пособие, а также распечатки всех презентаций преподавателей и книгу Аржана Дасселаара (*Arjan Dasselaar*) *Handboek Digitale Criminaliteit* .

8.3.2 Предложение Нидерландов по проведению мастер класса

Разработка нового курса по киберпреступности

«Интенсивная программа подготовки по киберпреступности» ('Intensiveringsprogramma Cybercrime'), Национальный прокурор по киберпреступности и Институт по подготовке прокуроров и судей в Нидерландах (SSR) занимаются разработкой нового курса по киберпреступности, который охватывает широкий перечень тем: начиная с вопросов «перехвата» и кончая мастер-классами по киберпреступности в конкретных областях (бот-неты).

Пока работа над программой не завершена, но первый день будет посвящен основам перехвата (несанкционированное подключение к проводной связи и Интернету), на второй день слушатели пройдут базовый курс по киберпреступности. Оба эти курса будут обязательными для *всех* прокуроров Нидерландов и станут частью их обязательного образования. Вторая часть курса предназначена исключительно для специалистов в области киберпреступности (будут введены строгие условия приема на эти курсы), включает курс углубленной подготовки (2 - 4 дня) и двухдневный мастер-класс (ежегодно). Эти курсы будут проводиться совместно с внешними партнерами, например, *Fox-IT*, *Digital Intelligence Training* и *Hoffman Bedrijfsrecherche*.

Причиной разработки курса стало не разочарование в содержании проводимых программ подготовки, а стремление добиться того, чтобы части курса были более структурированы и лучше согласованы друг с другом, чтобы избежать дублирования в процессе преподавания. Назначение прокуроров по вопросам киберпреступности в 11 самых крупных отделениях Прокурорской службы Нидерландов в рамках 'Intensiveringsprogramma' также стало важным стимулом для разработки/пересмотра программ подготовки. Важным аспектом курса является принцип последовательного повышения уровня знаний; каждый участник должен сначала пройти два базовых курса, прежде чем его зачислят на курс углубленный подготовки и на прохождение мастер-классов.

Одной из возможных новых составляющих курса станет информационное графическое отображение работы и рисков, связанных с Интернетом. В настоящее время работа над графическим отображением находится на завершающих этапах и может также использоваться во время проведения пробных презентаций. Ниже приводится несколько примеров графических материалов.

Последующие мероприятия

Для того чтобы прокуроры, которые занимаются киберпреступностью на повседневной основе, могли следить за последними достижениями в быстро развивающемся мире киберпреступности, в настоящее время проводятся две дополнительные программы по этой тематике.

Первая программа предусматривает создание Центра знаний и повышения квалификации при Национальной прокуратуре в Роттердаме. Этот центр будет отвечать на вопросы технического и юридического характера, следить за последними изменениями в прецедентном праве и распространять эту и другую необходимую информацию среди всех профессиональных

сотрудников в области киберпреступности в полиции и в прокурорской службе (центр является совместным предприятием двух организаций).

Во-вторых, в качестве приложения к данному проекту идет создание «комнаты цифрового сотрудничества», которую можно сравнить с функционированием службы Share Point. В этой виртуальной комнате киберпрофессионалы смогут обсуждать вопросы, связанные с их работой, и заниматься поиском любой информации, необходимой для их деятельности. Перечень того, что будет входить в контент и какими (техническими) возможностями будет обладать эта комната, появится в октябре этого года. Ниже приводится пример одного из возможных вариантов домашней странички цифровой комнаты.

Создание чувства неотложной необходимости: подготовка на управленческом уровне

Принимая во внимание относительно ограниченные возможности полиции Нидерландов, ей приходится делать выбор между тем, какие преступления следует или не следует расследовать (примечание: правовая система Нидерландов позволяет Прокурорской службе не расследовать и не вести судебного преследования в связи с преступлениями, что называется opportuniteitsbeginsel). Как правило, это выбор делается на уровне управленческих кадров.

По признанию полиции и Прокурорской службы на этом уровне отсутствуют знания, касающиеся последствий киберпреступлений и важности борьбы с киберпреступностью, что создает опасность того, что эти важные дела не будут рассмотрены, поскольку более важными будут признаны другие (обычные) преступления. В связи с этим, в настоящее время разрабатывается учебный курс для руководителей полиции и Прокурорской службы. В соответствии с графиком, пилотная программа подготовки будет представлена в конце этого года. Этот учебный курс будет нацелен на создание чувства неотложной необходимости и, в основном, будет направлен на ознакомление участников с реалиями киберпреступности в

современном обществе. Он будет включать изучение тем не на уровне контента (как это происходит в процессе углубленного изучения предметов), а на стратегическом, управленческом уровне.