|  |  |
| --- | --- |
|  | **CyberCrime@IPA**  **Совместный проект ЕС/СЕ по укреплению регионального сотрудничества в борьбе с киберпреступностью**    **Подготовка судейского корпуса**  **«Сетевая компьютерная преступность (киберпреступность) и использование доказательств в электронной форме» -вводный курс для работников суда и прокуратуры**  Практическое пособие и руководство для инструкторов – Версия 1.0  Отдел по защите данных  и борьбе с киберпреступностью.  Генеральная дирекция по правам  человека и верховенству права.  г. Страсбург, Франция  5 апреля 2013 г. |
| **www.coe.int/cybercrime**  eu_coe_JP1 |

|  |  |
| --- | --- |
| **Контактная информация:**  Отдел по защите данных  и борьбе с киберпреступностью.  Генеральная дирекция по правам  человека и верховенству права.  Совет Европы,  г. Страсбург, Франция  Тел. : +33-3-9021-4506 Факс: +33-3-9021-5650 Мейл: [alexander.seger@coe.int](mailto:alexander.seger@coe.int) | **Оговорка об ограничении ответственности:**  Настоящий технический отчет необязательно отражает официальную позицию Совета Европы, жертвователей, финансирующих настоящий проект, или же сторон цитируемых в нём договоров. |

**Оглавление**

[1 Введение 4](#_Toc352944220)

[2 Общий обзор содержания 5](#_Toc352944221)

[2.1 Цели курса 5](#_Toc352944222)

[2.2 Зачем необходим настоящий практикум 5](#_Toc352944223)

[2.3 Учебный план 6](#_Toc352944224)

[3 Как использовать руководство для инструкторов 6](#_Toc352944225)

[4 Общий обзор курса 7](#_Toc352944226)

[4.1 Продолжительность курса и его аудитория 7](#_Toc352944227)

[4.2 Кто будет вести занятия? 7](#_Toc352944228)

[4.3 Как будут проводиться занятия? 8](#_Toc352944229)

[4.4 Задачи курса 8](#_Toc352944230)

[4.5 Участники занятий и ведущие их инструктора 8](#_Toc352944231)

[4.5.1 Участники (слушатели) 8](#_Toc352944232)

[4.5.2 Предъявляемые к ним требования 8](#_Toc352944233)

[4.5.3 Ведущие занятия инструктора 8](#_Toc352944234)

[4.5.4 Предъявляемые к ним требования 8](#_Toc352944235)

[4.6 Перечень материалов, необходимых для проведения занятий 9](#_Toc352944236)

[4.7 Оценка уровня знаний 9](#_Toc352944238)

[4.8 Задачи курса и входящих в него занятий 9](#_Toc352944239)

[5 Основные контактные лица 13](#_Toc352944240)

[6 Учебные планы занятий 14](#_Toc352944241)

[6.1 Занятие 1.1.1 Введение в курс 14](#_Toc352944242)

[6.2 Занятие 1.1.2 Введение в киберпреступность 17](#_Toc352944243)

[6.3 Занятие 1.1.3, 1.2.2 & 1.2.5 – Технические средства 29](#_Toc352944244)

[6.4 Занятие 1.3.1 Обзор проделанной работы 55](#_Toc352944245)

[6.5 Занятие 1.2.3 Киберпреступление как уголовно наказуемое деяние в соответствии с положениями национального законодательства 56](#_Toc352944246)

[6.6 Занятие 1.2.4 Процессуальное внутригосударственное законодательство 81](#_Toc352944247)

[6.7 Занятие 1.3.1 Обзор проделанной работы 86](#_Toc352944248)

[6.8 Занятие 1.3.2 & 1.3.3 Доказательства в электронной форме 87](#_Toc352944249)

[6.9 Занятие 1.3.4 Международное сотрудничество 112](#_Toc352944250)

[6.10 Занятие 1.3.5 Заключительное занятие 122](#_Toc352944251)

[7 Оценка слушателями учебного материала и работы инструктора 124](#_Toc352944252)

[8 Оценка уровня знаний, полученных слушателями 124](#_Toc352944253)

# 1 Введение

Принимая во внимание зависимость всемирного сообщества от информационно-коммуникационных технологий, работники суда и прокуратуры должны быть подготовлены к борьбе с сетевой компьютерной преступностью (киберпреступностью) и работе с доказательной базой на электронных носителях. Во многих странах правоохранительным органам уже удалось усилить свой потенциал по расследованию компьютерных преступлений и обеспечению сохранности и доказательной силы улик в электронном виде. Одновременно, представляется, что это в меньшей степени относится к судебному и прокурорскому корпусу. Как нам подсказывает опыт, в большинстве случаев судьи и прокуроры сталкиваются с трудностями, имея дело с новыми реалиями мирового киберпространства. Таким образом, необходимо приложить особые усилия, направленные на то, чтобы позволить им поддерживать обвинение и выносить судебные решения по делам о преступлениях с использованием современной вычислительной и электронной техники, а также пользоваться доказательствами в электронной форме. Этого можно достичь при помощи организации специальных практических занятий (тренингов), формирования сетевых профессиональных сообществ и специализации.

Соответствующая концепция в поддержку подобных усилий была разработана в 2009 г. Советом Европы в рамках проекта «Компьютерная преступность (киберпреступность)» совместно с Лиссабонским сетевым сообществом учебных заведений по подготовке судебных работников и при взаимодействии с другими участниками проекта, выражающими интересы самых различных сторон.

Цель вышеуказанной концепции заключалась в том, чтобы помочь специализированным учебным заведениям в разработке программ ознакомления работников суда и прокуратуры с проблематикой сетевой преступности и использования доказательств в электронной форме, а также в том, чтобы ввести этот предмет на постоянной основе в базисный учебный план их начальной подготовки и во внутриведомственные программы повышения квалификации.

Задачи концепции следующие:

* способствовать тому, чтобы соответствующие учебные заведения могли обеспечивать базовую подготовку и последующее внутриведомственное повышение квалификации по тематике сетевой преступности, основанные на международных стандартах;
* дать как можно большему числу будущих и действующих работников суда и прокуратуры базовые знания о сетевой преступности и о возможностях использования доказательств в электронной форме;
* обеспечить углублённую подготовку по данной тематике критически необходимому количеству работников суда и прокуратуры;
* способствовать непрерывному процессу специализации и повышения технической квалификации работников суда и прокуратуры по данной тематике;
* способствовать углублению приобретённых специальных знаний путём налаживания связей между работниками суда и прокуратуры по данной тематике;
* сделать более доступными разного рода образовательные инициативы и формирование сетевых сообществ.

Кроме того, благодаря совместному региональному проекту Европейского Союза и Совета Европы «Усиление потенциала противодействия сетевой компьютерной преступности (киберпреступности) в рамках регионального сотрудничества в области уголовного правосудия» (CyberCrime@IPA)[[1]](#footnote-1), соответствующие учебные заведения, расположенные в зоне осуществления проекта (в Албании, Боснии и Герцеговине, Хорватии, Черногории, Сербии, «бывшей югославской Республике Македонии», Турции и Косово[[2]](#footnote-2)\*) получают поддержку в реализации вышеуказанной концепции.

В связи с этим разрабатываются учебные материалы, предназначенные для использования в специализированных учебных заведениях. Также было проведено обучение по «Программе подготовки инструкторов». В окончательной редакции данного практического пособия учтены отзывы работников суда и прокуратуры, прошедших курсы по программе подготовки инструкторов и успевших выступить в качестве ведущих практических занятий в своих учебных заведениях. Более того, она была обсуждена на специально созванном с этой целью собрании, в котором приняли участие члены рабочей группы по подготовке работников суда, а также инструктора.

# Общий обзор содержания

## 2.1 Цели курса

Настоящий курс составлен таким образом, чтобы ввести работников суда и прокуратуры в тематику сетевой преступности (киберпреступности) и использования доказательств в электронном виде. В нём содержится как правовая, так и практическая информация об изучаемом предмете. При этом особое внимание уделяется тому, насколько владение этим материалом необходимо судьям и прокурорам в их повседневной работе.

По окончании курса обучающиеся будут владеть базовыми знаниями о том:

* что представляют собой сетевая компьютерная преступность (киберпреступность) и доказательства в электронной форме;
* как использовать таковые доказательства в борьбе с сетевой преступностью;
* какие нормы материального и процессуального права, а также технические средства могут быть при этом применены, и
* какие срочные и эффективные меры должны быть приняты в рамках расширенного международного сотрудничества в борьбе с киберпреступностью.

В данном курсе рассматриваются следующие темы:

* введение в сетевую компьютерную преступность (киберпреступность) – основные направления её развития и используемые преступниками методы;
* технические средства, применяемые преступным элементом в информационном пространстве;
* преступление в сфере компьютерной информации (киберпреступление) как уголовно наказуемое деяние в соответствии с нормами национального законодательства;
* практическое использование доказательств в электронной форме и регламентирующие его нормы процессуального законодательства;
* процессуальное право и следственные меры в национальном законодательстве;
* международное сотрудничество.

## Зачем необходим настоящий практикум?

Судьи и прокуроры играют важную роль при расследовании и вынесении судебных решений по делам в отношении отдельных лиц или же группировок, совершающих преступления. С увеличением доли правонарушений, имеющих признаки киберпреступления или же совершаемых с использованием электронных носителей информации, возрастает спрос на судебных и прокурорских работников, прошедших специализированную профессиональную подготовку и способных выявить характер вышеуказанных противоправных деяний, а также владеющих соответствующей правовой информацией и инструментами международного сотрудничества, предоставленным в их распоряжение для ведения подобных дел.

Как правило, преступники и преступные группировки не ограничиваются пределами своих стран. Сетевая компьютерная преступность (киберпреступность) является одним из видов такой противоправной деятельности, при которой правонарушителю не надо для совершения преступления пересекать государственные границы, что в свою очередь значительно усложняет выявление и судебное преследование правонарушителей. В связи с этим при расследовании преступлений в сфере компьютерной информации (киберпреступлений) возрастает потребность в совершенствовании международного и регионального сотрудничества, а также в укреплении межведомственного взаимодействия.

При расследовании киберпреступлений часто возникает необходимость в оперативном налаживании эффективного регионального или же международного сотрудничества, которое позволило бы своевременно расследовать дело, выявить и преследовать по суду правонарушителей. Таким образом, учебным заведениям необходимо приложить соответствующие усилия для того, чтобы включить в свои учебные планы курсы, содержащие сведения о возможностях, предоставляемых в рамках международного сотрудничества для расследования преступлений в сфере компьютерной информации. В качестве примера здесь можно привести «Сеть 24/7» (международная сеть национальных центров обмена оперативной информацией в сфере компьютерной криминалистики, работающих 24 часа в сутки 7 дней в неделю), систему взаимной юридической помощи, различные мероприятия и центры международно-правового сотрудничества и так далее.

## Учебный план

Учебный план является основным документом при подготовке практических занятий по сетевой преступности (киберпреступности). Он нацелен на то, чтобы обеспечить соблюдение единого образовательного стандарта при разработке курсов или же модулей по данной тематике в странах/регионах, участвующих в осуществлении проекта, а также при проведении базовых практических занятий для судей и прокуроров, поддерживающих обвинение или же выносящих судебные решения по делам о киберпреступлениях.

Предложенный примерный учебный план курса подготовки следует рассматривать лишь как основу при организации практических занятий для работников суда и прокуратуры, а не как её конечный результат. В странах и регионах, участвующих в осуществлении проекта, необходимо сначала обсудить собственные потребности на национальном уровне, а затем сделать запрос о проведении дополнительных занятий со специализацией на тех видах сетевой преступности, где положение представляется наиболее критическим.

В данном пособии учебный материал подаётся в форме занятий, суть которых сжато воспроизводится в соответствующих сериях диапозитивов («презентациях»). В начале каждого занятия/презентации за заголовками следуют краткое изложение их содержания и подробные объяснения, которые должен давать ведущий занятия инструктор. Учебный план был задуман так, чтобы в него можно было вносить поправки с учётом возникающих на местах потребностей, при выполнении поставленных перед курсом целей и задач. Последнее необходимо для обеспечения последовательности и единообразия учебного процесса вне зависимости от страны проведения практических занятий. Инструкторам следует предусмотреть внесение в учебный план определённого количества практических упражнений и обсуждений, которые могли бы способствовать усвоению учебного материала в зависимости от личного профессионального опыта обучающихся в каждой из стран.

Базовый курс обучения построен таким образом, чтобы прошедшие его судьи и прокуроры смогли овладеть основными знаниями о природе сетевой интернет преступности (киберпреступности), об используемых в ней технических средствах и терминологии. Кроме того, в этом курсе содержатся основные сведения о возможностях международного сотрудничества, об использовании доказательств в электронной форме, о применяемых при этом нормах процессуального права, о специфике оперативно-розыскных мероприятий в сфере киберпреступности и т. д.

Предусмотрен также и курс углублённого изучения данной темы, построенный на базовом курсе и являющийся его расширенным вариантом. В нём содержится более подробная информация об изучаемом предмете и проводится анализ конкретных ситуаций для лучшего усвоения материала, изложенного в базовом курсе. Углублённый курс обучения будет разработан с целью предоставления судьям и прокурорам более конкретных сведений, которые можно применить на практике. Таковые будут касаться принципов работы компьютера и интернет сетей, вопросов раскрытия киберпреступлений, законодательства, регламентирующего работу в информационном пространстве, подсудности киберпреступлений, оперативно-розыскных возможностей, использования доказательств в электронной форме и международного сотрудничества.

# 3 Как использовать руководство для инструкторов

Настоящее руководство для инструкторов предназначено для того, чтобы предоставить им сведения о построении и содержании курса. В задачах каждого занятия указывается, какая информация должна быть на нём изложена. Также разработана и методология подачи информации этого курса. Инструктору надо проследить за тем, чтобы к каждому его занятию имелись все необходимые основные наглядные пособия. Целью данного руководства является поддержание образовательного стандарта и обеспечение последовательности изложения.

Кроме того, этим руководством определяются ориентировочные характер и уровень технической осведомлённости, требуемые от судей и прокуроров для эффективного исполнения ими своих профессиональных обязанностей. Его авторы не претендуют на исчерпывающий анализ изучаемого предмета и там, где это им кажется важным, дают ссылки на дополнительные источники информации.

Рекомендуется, чтобы разработчики курса использовали при его подготовке самые современные сведения о последних достижениях науки и техники постольку, поскольку таковые влияют на поведение преступного мира, а также отражаются на правовых нормах, на положениях процессуального права и порядке доказывания вины в рамках той юрисдикции, при которой должны проводиться практические занятия (тренинги). Существуют такие технологические прорывы, которые сказываются на работе всей системы уголовного правосудия. Здесь в качестве примера можно привести появление твёрдотельных устройств хранения данных или же методики проектирования интернет систем по принципу «Веб 2.0.» (Web 2.0.). Таким образом, со временем будет необходимо включить в программы подготовки немало важных тем по мере возрастания их значимости.

Как и любая другая программа, учебный план практических занятий с работниками суда и прокуратуры должен ставить перед ними ясные и понятные задачи, отвечающие следующим требованиям: таковые должны быть конкретными, поддающимися измерению, достижимыми и важными для учащихся. Кроме того, время, выделенное для их решения, должно быть ограниченным. Выполнение этих требований способствует достижению конечной цели. При формулировке задач старайтесь избегать таких слов как «понять» или «изучить», так как нет применительно к ним соответствующей шкалы измерения. Например, как вы оцените, насколько достигнута цель «изучения» рассматриваемого на занятиях предмета? Таким образом, лучше использовать такие поддающиеся измерению понятия как «перечислите» или же «определите».

Подача учебного материала в форме разбора конкретных ситуаций рассматривается как более подходящая для подобного рода практических занятий (тренингов) со взрослой аудиторией нежели, чем чисто дидактический, лекционный стиль обучения.

Ключевая роль организатора практических занятий (тренингов) заключается в том, чтобы обеспечить достижение общей задачи, преследуемой каждым учебным мероприятием, при одновременном осуществлении конкретных поставленных перед ним задач. В этой главе содержится некоторая информация, способствующая этому процессу.

Хотя этот курс и разрабатывался как общий, а не конкретно подогнанный под специфику той или иной страны, важно, чтобы ведущие занятия инструктора придавали личностный характер изложению учебного материала для его лучшего усвоения. Подача такового в форме разбора конкретных ситуаций рассматривается как более подходящая для подобного рода практических занятий (тренингов) со взрослой аудиторией нежели, чем чисто дидактический, лекционный стиль обучения. Использование конкретных образчиков технических средств, упоминаемых на лекциях, а также непосредственная работа в сети также могут повысить эффективность обучения. Кроме того, занятия, посвящённые национальным нормам материального и процессуального права в сфере киберпреступности, готовились как примеры того рода информации, которую следует ввести в программы на национальном уровне. На инструкторов возлагается обязанность по обеспечению учёта положений своего национального законодательства при подготовке занятий у себя в стране.

# Общий обзор курса

## 4.1 Продолжительность курса и его аудитория

Настоящий трёхдневный курс, предназначенный для судей и прокуроров, входит в программу их начальной подготовки.

## Кто будет вести занятия?

Курс задуман таким образом, чтобы занятия могли вести внутриведомственные инструктора, сотрудничающие с национальными учебными центрами по подготовке судей (УЦПС). В случае необходимости, при отсутствии в УЦПС работников требуемой квалификации, целесообразно обратиться к узкому специалисту для освещения сугубо технических аспектов изучаемого предмета. Так как речь идёт о базовом уровне, то предполагается, что этот курс предназначен для всех новых судей и прокуроров.

## Как будут проводиться занятия?

Предполагается, что занятия в их нынешнем виде должны проводиться в учебной аудитории, оборудованной для подготовки инструкторов. В случае необходимости, ничто не мешает конвертировать учебный материал в формат, приемлемый для дистанционного обучения по интернету. Как указывалось выше, в разделе 1, инструкторам следует рассмотреть возможность введения разного рода упражнений и других методов преподавания в программы на национальном уровне.

## Задачи курса

Задачи курса были расписаны вполне традиционно таким образом, чтобы позволить ведущим их инструкторам использовать различные методы обучения для достижения таковых. Все задачи соответствуют так называемым требованиям «СМАРТ» (SMART). SMART – сокращение, составленное из первых букв английских слов:

* **s**pecific – конкретный (в задаче должно быть точно указано, чего нужно достичь);
* **m**easurable – «измеримый» (вы должны иметь возможность оценить, выполнена ли поставленная задача или нет);
* **a**chievable – достижимый – (можно ли в действительности выполнить поставленные вами задачи?);
* **r**ealistic – реальный (можете ли вы реально выполнить поставленные задачи с использованием имеющихся в вашем распоряжении средств?);
* **t**ime - время (к какому сроку вы хотите решить поставленные задачи?).

Задачи курса были сформулированы, отталкиваясь от вышеизложенных требований, и рассматривать их следует в свете общей поставленной перед ним цели.

## Слушатели занятий и ведущие их инструктора

### Слушатели

Настоящий курс предназначен для судей и прокуроров, проходящих начальную подготовку.

### Предъявляемые к ним требования

Не предполагается наличия никаких предварительных познаний по изучаемому предмету.

### Ведущие занятия инструктора

Они должны быть работниками учебных центров по подготовке судей (УЦПС), где предполагается проводить данные практические занятия.

### Предъявляемые к ним требования

Инструктора обязаны владеть на должном уровне тематикой по сетевой преступности и основным тенденциям её развития, а также знаниями законов своей страны происхождения. Кроме того, от них требуется наличие опыта работы в качестве инструктора с хорошей теоретической и практической подготовкой.

## Перечень материалов, необходимых для проведения занятия

Для проведения настоящего курса необходимо предусмотреть наличие в учебной аудитории следующего:

* сама аудитория должна быть достаточных размеров, чтобы вместить с запасом всех потенциальных слушателей;
* ПК/ноутбук с операционной системой Windows 7 и с загруженным офисным пакетом приложений MS Office Professional;
* проектор с экраном;
* доступ в сеть Интернет (при наличии);
* образчики аппаратных средств ЭВМ (при наличии);
* видеоролик «Воины сети» («Warriors of the Net»);
* текст будапештской «Конвенции о компьютерных преступлениях» с объяснительным докладом;
* копия руководства по использованию электронных доказательств, созданного при финансовой поддержке программы Европейского Союза «ОИСИН»;
* «белая классная доска»;
* фломастеры голубого, чёрного, красного и зелёного цветов (по 2 штуки каждого цвета);
* 2 магнитно-маркерных доски («флипчарт») с бумагой;
* блокноты и ручки для слушателей;
* сшиватель («стаплер»), дырокол и ножницы;
* офисный пластилин или его заменители, позволяющие временно развешивать на стенах листы бумаги.

## Оценка уровня знаний

В рамках этого экспериментального курса никакой оценки уровня знаний слушателей не требуется и не предусмотрено. Страны, на территории которых проводятся практические занятия на национальном уровне, могут изъявить желание ввести у себя соответствующие экзамены. При проведении каждого учебного мероприятия инструкторам следует контролировать усвоение материала слушателями во время самих занятий путём проведения опросов или же иными способами, позволяющими убедиться в том, что задачи проводимого занятия решены.

## Задачи курса и входящих в него занятий

| **№ занятия** | **Тема занятия** | **Поставленные задачи:** |
| --- | --- | --- |
| **1.1.1** | **Вводная часть** | * Провести взаимное представление слушателей и инструкторов. * Изложить программу и содержание курса. * Выполнить основные административно-учётные формальности. * Раздать вспомогательные материалы. * Объяснить порядок работы и месторасположение бытовых удобств, включая аварийный выход и медпункт. |
| **1.1.2** | **Введение в сетевую компьютерную преступность (киберпреступ-ность)** | * Дать определение различным видам преступлений в сфере компьютерной информации (киберпреступлений) и рассказать об их последствиях. * Перечислить угрозы, основные направления развития и технические средства киберпреступности, а также методы борьбы с ней. * Определить понятие сетевой преступности (киберпреступности), являющейся разновидностью преступной деятельности по международным стандартам и в соответствии с положениями большинства законодательств. * Проанализировать необходимость и выгодность гармонизации национальных законодательств и международных правовых документов на основе, прежде всего, «Будапештской конвенции». |
| **1.1.3**  **1.2.2**  **1.2.5** | **Технические средства, введение** | * Перечислить составные части компьютерной системы. * Определить различные типы устройств хранения данных. * Рассмотреть, как отразилось на работе органов уголовного правосудия увеличения в геометрической прогрессии ёмкости запоминающих устройств. * Определить различные компьютерные операционные системы. * Объяснить основные принципы работы интернет сетей. * Описать функции интернета. * Определить как минимум 5 основных интернет приложений (прикладных программ интернета). * Изложить историю развития интернета от его истоков и до наших дней. * Объяснить разницу между различными интернет приложениями. * Рассказать, как киберпреступники используют различные интернет приложения в своих целях. |
| **1.2.3** | **Киберпреступлениекак уголовно наказуемое деяние в соответствии с положениями национального законодательства** | * Руководствуясь положениями «Будапеш-тской конвенции», перечислить материальные нормы уголовного права и выделить некоторые из ключевых признаков, используемых для того, чтобы квалифицировать киберпреступления. * Руководствуясь положениями действую-щего национального законодательства, перечислить материальные нормы уголовного права и выделить некоторые из ключевых признаков, используемых для того, чтобы квалифицировать киберпреступления. * Проанализировать необходимость и выгодность гармонизации национальных законодательств и международных правовых документов на основе, прежде всего, «Будапештской конвенции». * Определить основные нормы материального права, которые можно применить при рассмотрении обсуждаемых конкретных случаев из судебной практики. |
| **1.2.4** | **Процессуальное право и след-ственные меры в национальном законодательстве** | * Объяснить процессуальные нормы, изложенные в «Будапештской конвенции». * Объяснить ныне действующие процессуальные нормы, присутствующие в национальном законодательстве. |
| **1.3.3**  **1.3.4** | **Собирание доказательств в электронном виде (электронных доказательств); процессуальные и следственные меры** | * Рассказать, какие существуют виды электронных доказательств. * Изложить основные наиболее эффективные методы изъятия электронных доказательств и работы с ними. * Определить трудности, возникающие при работе с данными, сохраняющимися на жестком диске компьютера после отключения питания, с данными в оперативной памяти включённого компьютера («короткоживущими данными»), а также с интернет-источниками электронных доказательств. * Выявить проблемы с получением доказательств из другой юрисдикцией. * Обсудить вопросы допустимости использования электронных доказательств в судебном разбирательстве с точки зрения их подлинности, точности и полноты. * Объяснить процессуальные нормы, изложенные в «Будапештской конвенции». |
| **1.3.4** | **Международное сотрудничество** | * Осознать планетарные масштабы интернет сети и международные масштабы сетевой преступности (киберпреступности). * Объяснить важность международного сотрудничества и выявить инструменты международного сотрудничества, имеющиеся в нашем распоряжении в борьбе с киберпреступностью. * Оценить потребность в быстродействующих и эффективных каналах международного сотрудничества и в соответствующих инструментах; определить способы их использования, сроки и действенность. * Описать усилия международных организаций по внедрению новых форм и механизмов международного сотрудничества. * Обсудить будапештскую «Конвенцию о компьютерных преступлениях», определить основные утверждаемые в ней принципы, содержащиеся в конвенции обеспечительные меры, а также работу сети «24/7» по оказанию правовой взаимопомощи. |
| **1.3.5** | **Заключительное занятие** | * Получить отклики слушателей об эффективности курса. * Собрать заполненные вопросники, оценивающие работу ведущих его инструкторов. * Определить на какой следующий уровень владения изучаемым предметом слушатели должны выйти для совершенствования своих теоретических знаний и практических навыков. |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Совет Европы**  **Практические занятия (тренинг) для работников суда и прокуратуры**  **на тему «Сетевая интернет преступность (киберпреступность)»** | | | | | | | | | | | | |
| **Расписание занятий – Модуль 1** | | | | | | | | | | | | |
|  | **09:00 - 10:00** | | **10:00 - 11:00** | | **11:00 - 12:00** | | **12:00 - 13:00** | **13:00 - 14:00** | **14:00 - 15:00** | **15:00 - 16:00** | | **16:00 - 17:00** |
| **День 1** | **1.1.1**  **Начало занятий – вводная часть** | | | **1.1.2**  **Введение в сетевую компьютерную преступность («угрозы, тренды и вызовы»)** | | | | **ОБЕДЕННЫЙ ПЕРЕРЫВ** | **1.1.3 Введение в тему: технические средства**  **Часть 1** | | | |
| **День 2** | **1.2.1**  **Обзор проде-ланной работы** | **1.2.2 Введение в тему: технические средства**  **Часть 2** | | | | **1.2.3**  **Киберпреступление как уголовно наказуемое деяние в соответствии с положениями национального законодательства** | | **ОБЕДЕННЫЙ ПЕРЕРЫВ** | **1.2.4**  **Процессуальное право и следственные меры в национальном законодательстве** | | **1.2.5 Введение в тему: технические средства**  **Часть 3** | |
| **День 3** | **1.3.1**  **Обзор проде-ланной работы** | **1.3.2 Электронные доказательства.**  **«Практика и процедура»** | | | | **1.3.3**  **Электронные доказательства. Процессуальные нормы, регламентирующие их собирание.** | | **ОБЕДЕННЫЙ ПЕРЕРЫВ** | **1.3.4**  **Международное сотрудничество** | | **1.3.5**  **Получение откликов аудитории – заключительное занятие.** | |

NB – Каждый день в установленное время будут делаться также и промежуточные перерывы на принятие кофе и др.

# 5 Основные контактные лица

Просьба направлять вопросы, касающиеся данного курса и его содержания, следующим лицам:

|  |  |
| --- | --- |
| Александр Сегер,  начальник отдела по защите данных и борьбе с киберпреступностью  Генеральной директории по правам человека и верховенству права (ГД-I)  Совета Европы, ФРАНЦИЯ  67075 г. Страсбург Седекс  Тел.: +33 3 90 21 4506  Факс: +33 3 90 21 56 50  [alexander.seger@coe.int](mailto:alexander.seger@coe.int) | Мустафа Ферати,  руководитель программы  отдела по защите данных и борьбе с киберпреступностью  Генеральной директории по правам человека и верховенству права (ГД-I)  Совета Европы 67075 г. Страсбург Седекс, ФРАНЦИЯ Тел.: +33 (0)3 90 21 45 50 Факс: +33 (0)3 90 21 56 50  [Mustafa.Ferati@coe.int](mailto:Mustafa.Ferati@coe.int) |

# Учебные планы занятий

|  |  |  |
| --- | --- | --- |
| 6.1 Занятие 1.1.1 Введение в курс | | **Продолжительность: 90 минут** |
| Перечень материалов, необходимых для проведения занятия:  * ПК/ноутбук с операционной системой Windows 7 и с загруженным офисным пакетом приложений MS Office Professional; * проектор с экраном; * доступ в сеть Интернет (при наличии); * образчики аппаратных средств ЭВМ (при наличии); * белая «классная доска»; * фломастеры голубого, чёрного, красного и зелёного цветов (по 2 штуки каждого цвета); * 2 магнитно-маркерных доски («флипчарт») с бумагой; * блокноты и ручки для слушателей; * сшиватель («стаплер»), дырокол и ножницы; * офисный пластилин или его заменители, позволяющие временно развешивать на стенах листы бумаги. | | |
| **Цель:** Рассказать слушателям, в чём заключается необходимость настоящего практикума, каковы его цели и задачи. В достаточной степени информировать их о программе занятий и расписании на каждый день. Предоставить слушателям информацию по вопросам техники безопасности и охраны труда, а также сведения об административных формальностях, которые необходимо выполнить при прохождении обучения. Провести взаимное представление слушателей и инструкторов. | | |
| **Задачи:**  По окончании занятия слушатели должны быть в состоянии:   * представить инструкторов и своих коллег, участвующих в практикуме; * обсудить общую цель занятия; * объяснить необходимость его проведения; * перечислить занятия, входящие в учебное расписание, и чем слушатели будут на них заниматься; * перечислить правила техники безопасности и охраны труда на месте проведения занятий. | | |
| **№ слайда:** | **Содержание:** | |
| Слайды 1 - 23 | Введение  Это вводное занятие курса. На нём слушатели представляются инструкторам и остальным присутствующим. Цели и задачи подготовки им объясняются одновременно с изложением применяемой методики обучения.  На этом этапе инструктор может попытаться «растопить холодок», то есть применить ряд приёмов для оживления контактов между слушателями с целью активизации их участия в занятиях с самого начала практикума. | |
| Слайд 1 | **Презентация, подготовленная с помощью «ПауерПойнт» (PowerPoint), или же иной программы**  Для проведения настоящего занятия была создана презентация с использованием программы «ПауерПойнт». Это общая презентация, подготовленная без учёта национальной специфики, которую следует принять во внимание при проведении данного курса на национальном уровне. Инструктор должен позаботиться о том, чтобы излагаемые в ней сведения соответствовали месту проведения занятий. | |
| Слайд 2 | На этом слайде речь идёт о вопросах техники безопасности и охраны труда. Их решение может быть различным в зависимости от места проведения занятий. На инструктора возлагается обязанность по предоставлению слушателям соответствующей информации по данной теме. | |
| Слайд 3 | Здесь слушателям излагается предыстория создания настоящего пособия под названием: вводный курс практической подготовки работников суда и прокуратуры на тему «Сетевая интернет преступность (киберпреступность) и использование доказательств в электронной форме». Он стал результатом работы в рамках совместного проекта Европейского Союза и Совета Европы по региональному сотрудничеству в области противодействия сетевой интернет преступности (киберпреступности) в регионе, где реализуется так называемая «программа помощи, предваряющей вступление в ЕС». | |
| Слад 4 | Далее указываются цели настоящего занятия:   * рассказать слушателям, в чём заключается необходимость   практикума (тренинга), каковы его цели и задачи;   * в достаточной степени информировать их о программе занятий и расписании на каждый день; * предоставить слушателям информацию по вопросам техники безопасности и охраны труда, а также сведения об административных формальностях, которые необходимо выполнить при прохождении обучения; * провести взаимное представление слушателей и инструкторов. | |
| Слайд 5 | В личных плановых заданиях перечисляется то, что слушатели должны уметь делать по окончании занятия. Эти задания могут быть использованы для проверки усвоения материала и для оценки слушателями уровня проведения практикума. По окончании этого занятия слушатели должны быть в состоянии:   * представить инструкторов и своих коллег, участвующих в практикуме; * обсудить общую цель всего курса; * объяснить его необходимость; * перечислить, какие занятия входят в учебное расписание, и чем они будут на них заниматься; * перечислить правила техники безопасности и охраны труда в месте проведения занятий. | |
| Слайд 6 | Необходимость этих практических занятий (тренинга) объясняется тем, что судьи и прокуроры играют важную роль при расследовании и вынесении судебных решений по делам в отношении отдельных лиц или же группировок, совершающих преступления. С увеличением доли правонарушений с признаками киберпреступления или же с использованием электронных носителей информации возрастает спрос на судебных и прокурорских работников, прошедших специализированную профессиональную подготовку и способных выявить характер вышеуказанных противоправных деяний, а также владеющих соответствующей правовой информацией и инструментами международного сотрудничества, предоставленными в их распоряжение для ведения подобных дел. | |
| Слайд 7 | Важно, чтобы общая цель настоящего курса была объяснена слушателям в самом начале. Это позволит им лучше понять основную причину того, для чего они здесь находятся. Общая цель практикума следующая: ввести работников суда и прокуратуры в тематику сетевой преступности (киберпреступности) и использования доказательств в электронной форме. Курс содержит как правовую, так и практическую информацию об изучаемом предмете. При этом особое внимание уделяется тому, как владение этим материалом отражается на повседневной работе судебного и прокурорского корпуса. | |
| Слайд 8 | На этом этапе следует представить слушателям расписание, включающее собственно занятия, обеденные и иные перерывы, а также краткое описание каждого занятия. Одновременно следует рассмотреть вопрос о проведении оценки уровня знаний или же отказе от неё. Если экзамен будет, то он должен сопровождаться подробными объяснениями, включая рассмотрение результатов, ожидаемых слушателями от курса. | |
| Слайды 9 - 17 | На этих слайдах представлены конкретные задачи каждого из занятий. Таковые задачи должны быть объяснены слушателям на данном этапе одновременно с изложением основных положений вышеуказанных занятий. | |
| Слайд 20 | Затем следует взаимное представление друг другу инструкторов и слушателей. На этом начальном этапе важно воспользоваться представляющейся возможностью создать атмосферу взаимодействия как между самими слушателями, так и между аудиторией и инструкторами. Можно, например, попросить слушателей разбиться попарно, выбрав себе в наперники незнакомого человека в аудитории, а затем подвести их к тому, чтобы задать своему напарнику следующие вопросы:   * как его зовут и из какой он страны; * где он работает; * чем он занимается; * есть ли у него опыт работы в качестве инструктора; * может ли он рассказать о себе что-нибудь интересное; * ответы на «вопросы по самостоятельному определению оценки своего уровня». | |
| Слайд 21 | «Вопросы по самостоятельному определению оценки своего уровня» задуманы как средство активизации общения между слушателями. Одновременно они позволяют инструкторам больше узнать об их уровне подготовленности и практическом опыте в изучаемой области (виды киберпреступлений и используемые для из совершения технические средства, о которых речь пойдёт далее). По указанной в «вопросах» пронумерованной шкале слушателям надо указать номер уровня, который более всего, с их точки зрения, соответствует их знаниям по каждому из изучаемых разделов.  Напарники должны задать эти же вопросы друг другу, а затем представить своего «нового коллегу» всей аудитории. Инструктору же надо в свою очередь взять на заметку собранную таким образом информацию, чтобы лучше знать свою аудиторию. | |
|  | **Практическое занятие (при наличии необходимых условий)**  Единственное, в чём можно попрактиковаться на этом занятии, так это во взаимном представлении друг другу слушателей и инструкторов. Требования, предъявляемые к ним, изложены в предыдущем разделе. | |
|  | Проверка знаний  На этом занятии проверка знаний не предусмотрена. | |
| Слайд 23 | Подведение итогов занятия/выводы  Инструктору следует подвести промежуточные итоги и проверить знания, чтобы убедиться в том, что слушатели поняли задачи занятия, по ходу которого надо также выделить время и на их вопросы. | |

|  |  |  |
| --- | --- | --- |
| Занятие 1.1.2 Ввведение в сетевую интернет преступность (киберпреступность) | | **Продолжительность: 120 минут** |
| Перечень материалов, необходимых для проведения занятия:  * ПК/ноутбук с операционной системой Windows 7 и с загруженным офисным пакетом приложений MS Office Professional; * проектор с экраном; * презентация «ПауерПойнт» | | |
| **Цель:**  Целью этого занятия является предоставление участникам общего обзора сетевой компьютерной преступности (киберпреступности), рассматриваемой одновременно как с правовой точки зрения, так и через призму перспективы новых реалий. На нём надо будет осветить предысторию вопроса в различных странах и нормативную базу его решения на международном уровне. | | |
| **Задачи:**   * Во время этого занятия слушателям будет объяснено, что собой представляет сетевая компьютерная преступность (киберпреступность) и почему она вызывает обеспокоенность. Речь пойдёт как об опасности, исходящей от киберпреступности, о её основных направлениях развития и об используемых киберпреступниками технических средствах, так и о том вызове, который они бросили судебному и прокурорскому корпусу. Также в ходе занятия будет дано описание того, как ведётся борьба с этим явлением на национальном и международном уровнях. * По окончании занятия слушатели смогут рассказать, что скрывающиеся за выражением «сетевая компьютерная преступность (киберпреступность)», и выявить компьютерные разработки, квалифицируемые как разновидность киберпреступлений в соответствии с положениями большинства законодательств и с международными нормами права. * На занятии будут освещены материальные нормы уголовного права, связанные с киберпреступлениями, и указаны некоторые из ключевых признаков, используемых для того, чтобы квалифицировать эти преступления, исходя из положений «Будапештской конвенции» и всей совокупности норм правовой системы Европейского союза. * В свете вышеуказанного пункта на занятии будет подчёркнута необходимость и выгодность гармонизации национальных законодательств и международных договоров, прежде всего, на основе «Будапештской конвенции». | | |
| **№ слайдов** | **Содержание:** | |
|  | Введение  Конкретной целью этого занятия является предоставление участникам общего обзора сетевой компьютерной преступности (киберпреступности), рассматриваемой одновременно как с правовой точки зрения, так и через призму перспективы новых реалий. На нём излагается предыстория вопроса в различных странах и освещается нормативная база, используемая для его решения на международном уровне. | |
| Слайд 2 | План занятия  В первой части презентации описываются новые реалии информационного общества и рассматривается процесс зарождения противоправной деятельности в сетях интернета.  Во второй части освещается эволюция подхода ряда международных организаций к проблеме сетевой компьютерной преступности.  В третьей части делается попытка понять, что конкретно скрывается за общим понятием киберпреступности.  В четвёртой части презентации объясняется, что представляет собой будапештская «Конвенция о компьютерных преступлениях», и подчёркивается значимость этого единственного в своём роде обязательного к исполнению международного документа в борьбе с сетевой интернет преступностью (киберпреступностью).  В пятой части рассказывается о некоторых наиболее распространенных на сегодняшний день разновидностях противоправной деятельности в сети.  Шестая часть презентации содержит резюме всех затронутых в ней тем. | |
| Слайд 3 | **Задачи занятия:**  С точки зрения общей перспективы в качестве введения можно сказать, что целью этого занятия является изложение вопросов, относящихся к сетевой компьютерной преступности (киберпреступности).  На нём разъясняется понятие сетевой компьютерной преступности и причины, по которым она должна вызывать нашу обеспокоенность. Далее обсуждаются угрозы, исходящая от киберпреступности, основные направления её развития и используемые киберпреступниками технические средства, а также некоторые ответные меры в отношении этого явления.  Даётся общий обзор того, что скрывается за выражением «сетевая компьютерная преступность (киберпреступность)». Далее идёт описание ряда компьютерных разработок, квалифицируемых как разновидность киберпреступлений в соответствии с положениями большинства законодательств и с международными нормами.  Одна из наиболее важных тем, подлежащих обсуждению, относится к материальным нормам уголовного права и к ряду ключевых признаков, используемых для того, чтобы квалифицировать преступления в сфере компьютерной информации (киберпреступления). Вышеуказанные нормы и признаки основываются на положениях «Будапештской конвенции» и на совокупности норм правовых систем Европейского Союза.  На этом занятии также необходимо подчеркнуть необходимость и выгодность гармонизации национальных законодательств и международных юридических документов, прежде всего, на основе «Будапештской конвенции». | |
| Слайд 4 | Часть первая – Информационное общество и киберпреступность | |
| Слайды 5 - 7 | Информационное общество представляет собой общественно-экономическую модель развития, основанную на сборе и распространении информации с помощью сетей связи (коммуникационных сетей). Оно преобразило повседневную жизнь граждан на работе и дома, а также во многом повлияло и на проведение ими досуга.  При подобном общественно-экономическом устройстве мира физические расстояния уже больше не разделяют людей с разных концов света. Не считая нескольких хорошо известных исключений, в этом новом «открытом мире» потенциально между пользователями интернета политических (государственных) границ не существует. Здесь каждый может вполне демократически получать информацию и знания вне зависимости от места их хранения. В свою очередь, это приводит к соревнованию между всеми хозяйствующими субъектами.  Свободно и открыто выложенная информация доступна любому человеку. Интернет-пользователи чувствуют, что никакая верховная власть не стоит над интернетом. | |
| Слайд 8 | По мере того, как интернет проникает повсеместно и становиться достоянием каждого в мире, для преступного мира открываются новые возможности противоправной деятельности и, соответственно, растёт киберпреступность. Преступления, совершенные с использованием сетей интернет связи, стали наиболее «транснациональным» видом международной преступности.  Сама природа сетевой преступности объясняет особые трудности, возникающие при расследовании этого вида противоправной деятельности: улики, материально находящиеся на другом конце света, могут исчезнуть во мановение ока, если их сразу же не зафиксировать в реальном времени. К тому же, задействованные сотрудники правоохранительных органов должны соблюдать при этом государственные границы и установленный законом порядок работы, используя официальные каналы при обращении за оказанием международной помощи в рамках расследования уголовного правонарушения. | |
| Слайд 9 | В подобных условиях абсолютно необходим международный подход к этому вопросу. Транснациональный и международный подход здесь более эффективен по сравнению мероприятиями на национальном или даже региональном уровнях. Таким образом, глобальное восприятие данного явления предоставляет более широкие оперативные возможности. Международное сотрудничество между правоохранитель-ными органами – на уровне полиции или же прокуратуры – играет основополагающую роль в достижении результатов при расследовании уголовных киберпреступлений. | |
| Слайд 10 | Все наблюдатели согласны в том, что сетевая преступность представляет собой явление, охватившее весь земной шар, и что единственным правильным подходом к международным сетевым преступным сообществам, не ведающим границ, явялется комплексный общий подход, в рамках которого усилия, прилагаемые на национальном уровне, должны дополняться использованием особых форм и каналов международного сотрудничества. Именно таким образом можно противостоять киберпреступности: помогая друг другу глобально, нам легче решать наши проблемы локально в любой части мира.  Абсолютно ясно, что сетевая преступность является всемирным явлением. Как правило, любая противоправная деятельность имеет многочисленные территориальные привязки: обычно исполнители преступления базируются в конкретном месте, подпадающем под юрисдикцию той или иной страны, в то время как их деятельность распространяется на компьютеры и на пострадавших, находящихся на территории многих других стран.  Это является общей характеристикой, присущей и другим формам преступной деятельности. Но применительно к преступлениям в сфере компьютерной информации и доказательствам в электронной форме данная отличительная их особенность представляется как нечто внутренне свойственное природе таковых. Учитывая размах сетей связи и, в особенности, сетей интернета, ни одна страна в мире уже не может в одиночку решить проблему киберпреступности. | |
| Слайд 11 | Современное общество зависит от информационных технологий. В настоящее время государственные органы власти, простые граждане и хозяйствующие субъекты подключены к интернету. Всё это является весьма благодатной почвой для новых зарождающихся видов противоправной деятельности в самих коммуникационных сетях, с использованием таковых сетей или же направленных против них. | |
| Слайд 12 | Повсюду сетевая преступность ассоциируется с таким явлением как *хакерство* или же с распространением *вредоносных программных средств (программ),* существующих главным образом в виде компьютерных вирусов или же компьютернвх «червей» (саморазмножающихся и самораспространяющихся вирусов), а также со «взломом компьютеров» (*DoS* или же *DDos атаки*), ставшему более известным широкому общественному мнению благодаря СМИ. Тем не менее, сегодня даже обычные граждане оповещены о существовании многих других видов противоправной деятельности в сети, осуществляющейся по большей части с целью получения наживы (например, обычное и компьютерное мошенничество). Кроме того, всем известно о широких возможностях использования информационного пространства («киберпространства») для совершения уголовных преступлений. | |
| Слайд 13 | Понятие *«киберпространства»,* даже если ему не дано еще юридического или же академического определения, каждодневно обогащается всё новым содержанием и становится всё сложнее. В результате развития науки и техники происходит увеличение количества и типов разнообразных электронных устройств, способных взаимодействовать друг с другом в сети и передавать данные или же просто регистрировать их. | |
| Слайды 15 - 16 | Часть вторая – Международные организации и сетевая преступность  Многие международные организации вот уже не один год работают над разрешением проблемы киберпреступности и использования доказательств в электронной форме. | |
| Слайды 17 - 20 | Организация Объединённых Наций является одним из форумов, в рамках которых обсуждается проблема сетевой преступности. Начиная с 2000 г. Генеральная Ассамблея ООН приняла рад официальных резолюций по вопросу *о борьбе с преступным использованием информационных технологий* (первая из них под № 55/63 была одобрена на 81-м пленарном заседании Генеральной Ассамблеии ООН 4 декабря 2000 г.).  В этих официальных резолюциях указывается на необходимость принятия государствами – членами ООН законов, предусматривающих введение уголовной ответственности за совершение ряда деяний и отмены территорий, на которых киберпреступники могут чувствовать себя в безопасности (так называемых «*безопасных небес*»).  В принятой в марте 2010 г. Генеральной Ассамблеей ООН Резолюции 64/211 «О создании глобальной культуры кибербезопасности» речь идёт о введении на добровольной основе механизма самооценки усилий, предпринимаемых на национальном уровне с целью защиты критически важной информационной инфраструктуры. Среди всего прочего, в этой резолюции содержатся рекомендации государствам-членам, касающиеся принятия ими уголовного законодательства, учитывающего такие международные правовые документы как будапештская «Конвенция о компьютерных преступлениях».  Каждые пять лет Организация Объединённых Наций проводит Конгресс ООН по предупреждению преступности и уголовному правосудию. На конгрессах, проводившихся в 2005 году в Бангкоке и в 2010 году в г. Салвадор (Бразилия), делегаты согласились с необходимостью оказания технической помощи и укрепления материально технической базы.  Предложения о разработки новых договоров не были поддержаны за отсутствием должного консенсуса. | |
| Слайд 21 | Организация экономического сотрудничества и развития (ОЭСР) разделяет обеспокоенность ООН касательно явления сетевой компьютерной преступности. Тем не менее, её подход к проблеме иной. Начиная с 1983 г. ОЭСР изучала, в каких законах нуждаются входящие в неё государства для борьбы с киберпреступностью, и в результате разработала соответствующие рекомендации. ОЭСР постановляет, что как на международном, так и на национальном уровнях подобные противоправные деяния могут подлежать квалификации, исходя из подобных же норм уголовного права. | |
| Слайд 22 | Государства, входящие в состав «Группы восьми» (или «Большой восьмёрки» - G8), пошли в этом вопросе дальше, выбрав ещё более активный и упреждающий подход. «Большая восьмёрка» создала сеть из контактных центров, ставших опорными пунктами международного сотрудничества в этой сфере. Главным образом, они представлены в форме списка контактных лиц, которые в состоянии способствовать оперативному принятию срочных мер там, где это необходимо.  Если не считать Совета Европы, то «Большая Восьмёрка» стала здесь первопроходцем, внеся сетевую преступность в повестку дня первоочередных проблем. До настоящего времени это самая значительная инициатива по борьбе с киберпреступностью, предпринятая на международном уровне. | |
| Слайды 23 - 24 | Европейский Союз (ЕС) также обеспокоен в связи с ростом сетевой преступности. В 2005 г. им был одобрен обязательный к исполнению документ - Рамочное решение 2005/222/JHA[[3]](#footnote-3), принятое 24 февраля 2005 г. Советом министров ЕС по вопросу о компьютерных атаках на информационные системы. Это рамочное решение обязует все государства – члены Европейского Союза ввести у себя уголовную ответственность за совершение ряда перечисляемых далее правонарушений: незаконный доступ к информации в информационных системах, незаконное вмешательства в информационные системы и базы данных. В это решение также включены положения, относящиеся к подстрекательству, оказанию помощи в совершении, соучастию и к попытке совершения вышеуказанных противоправных деяний.  Кроме того, относительно международного сотрудничества рамочным решением постановляется, что все государства – члены Европейского Союза обязаны обеспечить использование существующей сети постоянно действующих контактных пунктов круглосуточной оперативной связи  В настоящее время, а именно начиная с января 2011 г., Рамочное решение 2005/222/JHA пересматривается – (первый проект этого документа был опубликован в октябре 2011 года). | |
| Слайд 25 | Также немаловажно рассмотреть работу, проделанную Организацией по безопасности и сотрудничеству в Европе (ОБСЕ) в области борьбы с сетевой преступностью.  ОБСЕ даёт рекомендации своим членам. В решении ОБСЕ № 7/06 заявляется, что государствам – членам этой организации следует рассмотреть возможность стать сторонами будапештской Конвенции о компьютерных преступлениях. Этим же решением она побуждает их присоединиться к «Сети 24/7» (круглосуточной постоянно работающей сети по борьбе с киберпреступностью, созданной усилиями государств «Большой Восьмёрки), а также организовать у себя подобные же контактные центры в целях содействия международному сотрудничеству в области применения законов по борьбе с преступным использованием киберпространства. | |
| Слайд 26 | Совет Европы изучает тему сетевой компьютерной преступности начиная с 1980 года. Проделанная подготовительная работа и утверждение рекомендаций из области «мягкого международного права» (то есть, не имеющих обязательной юридической силы), привели к решению обсудить возможность принятия обязательного к исполнению договора: им стала будапештская «Конвенция о компьютерной преступности» (этот документ рассматривается далее).  Подход Совета Европы к этому вопросу основан на трёх следующих пунктах:   1. нормативный документ – «Будапештская конвенция»; 2. «мониторинг» и контроль за исполнением положений вышеуказанной конвенции со стороны Комитета конвенции о киберпреступности (Комитет «T-CY») 3. реализация программ технического сотрудничества по оказанию странам помощи в укреплении материально-технической базы органов уголовного правосудия. | |
| Слайды 28 и 29 | Часть третья - что собой представляет сетевая компьютерная преступность (киберпреступность)? | |
| Слайд 30 | В роли «пострадавшего» выступают компьютерные технические средства (оборудование).  Традиционно принято считать, что мишенью профессионально совершенного «компьютерного преступления» являются технические средства. Сюда входят такие правонарушения как хакерство, атаки с целью нарушения нормального обслуживания пользователей (т.н. «атаки, вызывающие отказ в обслуживании») и распространение компьютерных вирусов. | |
| Слайд 31 | Компьютерные технические средства как вспомогательные при совершении преступления.  В данном случае имеются в виду ситуации, в которых компьютер и другие устройства используются в качестве вспомогательных средств при совершении традиционных противоправных деяний, таких как: изготовление поддельных документов, рассылка мейлов с угрозой смерти, сетевое вымогательство, создание и распространение незаконных материалов, например, изображений со сценами жестокого обращения с детьми. | |
| Слайд 32 | Компьютерное оборудование как средство связи.  Компьютерное оборудование выступает в этом качестве в тех случаях, когда преступные элементы используют его для обеспечения связи друг с другом таким образом, чтобы затруднить возможности перехвата, прибегая для этого, например, к шифровке сообщений (криптографии). | |
| Слайд 33 | Компьютерные оборудование как средство хранения данных.  В данном случае речь идёт об умышленном или же неумышленном сохранении информации с помощью различных запоминающих устройств и, как правило, предполагает наличие сохранённых данных в компьютерных системах пострадавших, свидетелей или же подозреваемых. | |
| Слайд 34 | Компьютерные технические средства как «свидетель» преступления.  В этой роли они выступают в тех случаях, когда улики, содержащиеся в электронных устройствах, могут использоваться в качестве подтверждения доказательств явно неустановленных фактов, например, для установления или же опровержения предоставленного подозреваемым алиби или же заявления, сделанного свидетелем. | |
| Слайд 35 | Виды преступлений, совершаемых с использованием компьютерной техники.  Этот слайд может быть использован для повторения пройденного материала и контроля его усвоения. Инструкторам предлагается начать с перечисления основных положений занятия, вынесенных в заголовки, а потом попросить слушателей определить виды противоправных деяний, определяемых как преступления в сфере компьютерной информации (киберпреступления). Инструктору будет полезно предварительно ознакомиться с различными видами киберпреступлений, подробно изложенных в «Будапештской конвенции», с тем, чтобы в дальнейшем приводить их в качестве примера или же обращаться к ним, отвечая на вопросы слушателей. | |
| Слайд 36 | Начиная с 1984 года, когда писатель Вильям Гибсон ввёл термин *киберпространство*  в своём научно-фантастическом романе «Нейромант», в котором обыгрывалась тема интернета и других коммуникационных сетей, стало возникать всё больше слов с приставкой «кибер». К ним можно причислить, конечно же, и термин *«киберпреступление».* Почти три десятилетия спустя, несмотря на многочисленные публикации о киберпреступности, их авторы так и не пришли к согласию о том, какое конкретное определение можно дать выражениям *киберпреступление* и *киберпреступность.*  Нет также и согласия по вопросу о том, действительно ли сетевая компьютерная преступность является новым и отдельным разделом уголовного права, или же она подпадает под действие отдельных его норм и в каждом конкретном случае достаточно просто сослаться на то, что то или иное конкретное преступление было совершено в киберсреде. | |
| Слайды 37 - 44 | Тем не менее, с социологической точки зрения преступная деятельность в киберсреде сама по себе является самостоятельным и значительным проявлением действительности. Повсюду на Европейском континенте - в полиции, в судах и в органах прокурорского надзора - есть соответствующие специализированные подразделения. Международные общественные организации и частные компании всё более обеспокоены последствиями преступных и вредоносных действий, совершаемых с применением коммуникационных сетей или же в самих сетях.  Исследуя эту новую реальность, юристы не могут прийти к согласию по поводу толкования выражения *киберпреступность.* Некоторые авторы рассматривают её как *компьютерную* или же *сетевую преступность.* Но каждый раз при использовании того или иного термина возникает опасность либо излишне расширительного, либо несправедливо обуженного толкования данного явления.  Преступное деяние, совершенное с использованием компьютера, не обязательно относится к категории «высокотехнологического». Значительная часть преступлений в информационном пространстве совершается с использованием относительно простых средств и при их раскрытии возникает относительно мало чисто технических проблем. Тем не менее, может быть здесь речь идёт о ложной постановке вопроса, так как на сегодняшний день каждый согласится с тем, что существует новая социально-криминальная реальность, возникшая внутри самих компьютерных систем и одновременно с их появлением.  Как правило, сетевую компьютерную преступность (киберпреступность) трактуют одновременно в узком и в расширительном смыслах. Обычно в узком смысле это определение употребляется для обозначения преступной деятельности, в которой использование преступниками компьютеров или же информационных сетей выступает в качестве основного признака этого вида преступности. Тем не менее, термин «киберпреступление» присутствует и в определении преступного деяния, включающего другие виды обычных преступлений, совершение которых стало возможным благодаря использованию компьютеров или же информационных сетей.  Если смотреть на вещи с этой точки зрения, то получается, что мы говорим о сетевом компьютерном преступлении (киберпреступлении) в тех случаях:  - когда компьютер выступает в качестве орудия совершения преступного деяния (например, при рассылке *спама,* при противоправном копировании информации, осуществляемом через так называемые *«пиринговые»,* то есть децентрализованные сети обмена файлами между частными лицами и так далее);  - когда компьютер или информационная сеть становятся мишенью таких преступных атак, как несанкционированных доступ, внедрение вредоносных кодов, и так далее;  - когда компьютер или информационная сеть становятся местом занятия преступной деятельностью (телекоммуникационное мошенничество);  - и наконец, когда совершение преступления облегчается благодаря использованию компьютера или же информационных компьютерных сетей (например, *«письма из Нигерии», хакерство, «фишинг»,*  детская порнография, «кража личности» и так далее.  При этом в первую категорию противоправных деяний попадают преступления, в совершении которых компьютер играет первостепенную роль, а во вторую – преступления, которые могли быть совершены с использованием иных средств, но применение компьютера облегчило их совершение.  Где-то рядом с этими реалиями стоят некоторые преступные деяния *нового поколения.* С одной стороны, они являются лишь новой разновидностью обычных, «традиционных» преступлений, отличительной чертой которых является тот факт, что они могут быть совершены, в том числе, и в киберсреде.  Но, с другой стороны, по своей природе они не могут существовать вне этого виртуального мира и зарождаются они внутри него. В качестве примера можно привести компьютерное мошенничество или же компьютерный подлог.  Некоторые другие уголовные правонарушения также совершаются с использованием компьютерных систем. Хотя в них компьютер и выступает в качестве *способа совершения преступления,* они теоретически не отличаются от того же вида противоправных деяний, реализованных иными способами. Даже будучи сетевыми, они от этого не становятся новым видом преступления. Безусловно, ничего не отличает их от обычных уголовных правонарушений. Здесь в качестве примера можно привести распространение клеветы через электронную версию газеты, угрозы, передаваемые по электронной почте, или же легализация через сетевой банк доходов, полученных преступным путем.  В этом же духе можно привести ещё более элементарный пример обычного *«внесетевого»*  правонарушения, доказываемого, тем не менее, с помощью «электронной» улики: хулиган, заснявших свой «удачный наезд» на прохожего на мобильный телефон и вывесивший этот ролик в сети на *«ютюбе».* Даже если этот инцидент и не может быть квалифицирован как *компьютерное преступление,* методы его расследования и доказывания вины те же, что и в случае с собственно киберпреступлением.  Но по идее, в чистом виде компьютерное преступление (киберпреступление) определяется как вид преступного деяния, характеризующегося тем, что оно направлено против компьютерных средств/среды или же или же компьютерной экосистемы. В качестве классических примеров такого вида преступлений можно привести вмешательство в базы данных, вмешательство в работу компьютерных систем, выражающееся, скажем, в проведении атак с целью нарушения нормального обслуживания пользователей, и даже несанкционированного допуска к информации. Все эти правонарушения направлены против самих компьютерных систем, функционирование которых предполагает обеспечение конфиденциальности, целостности и доступности компьютерных данных или же систем.  Зачастую, на практике при совершении «реального» преступления присутствует целый ряд вышеперечисленных признаков. Преступник может, например, угрожать компании проведением атаки по отказу в обслуживании, направленной против её интернет-сайта (что квалифицируется как преступление против компьютерных систем), если только она не выплатит шантажисту необходимую сумму денег (новая разновидность шантажа с использованием компьютерной техники в качестве орудия совершения преступления). При этом угроза, переданная по электронной почте, могла быть с тем же успехом доведена до получателя и обычным письмом.  В реальной жизни сетевые преступления становятся всё более разнообразными и многочисленными. Растёт количество таких типичных компьютерных преступлений как *«фишинг»* или же создание «бот-сетей» (из "зомбированных" компьютеров). Отмечается наличие обширного ассортимента корыстных киберпреступлений, отличающихся творческим подходом к делу их разработчиков. Широко развито пиратское использование программного обеспечения и посягательство на права интеллектуальной собственности. Констатируется расширение распространения материалов с детской порнографией, а также и объемов отмываемых в интернете денег. В общем и целом можно констатировать, что с каждым днём организованная преступность и незаконные формирования (в том числе и террористические организации) всё активнее используют компьютерные технологии для достижения своих преступных целей. | |
| Слайды 46 - 49 | Часть четвёртая – будапештская Конвенция о компьютерных преступлениях | |
|  | Конвенция о компьютерных преступлениях, известная также как «Будапештская конвенция» (документ ETS 185), была разработана благодаря усилиям Совета Европы и открыта для подписания 23 ноября 2001 года в г. Будапеште. Вступила в силу в июне 2004 года.  К апрелю 2013 г. 39 государств стали сторонами «Будапештской конвенции» (государства Европы, Австралия, Доминиканская республика, Япония и США), 10 государств подписали её (ряд европейских государств, Канада и Южная Африка) и ещё 8 приглашены присоединиться к ней (Аргентина, Чили, Коста-Рика, Мексика, Марокко, Панама, Филиппины и Сенегал). Дополнительно несколько стран находятся в процессе подачи ходатайств о присоединении к ней.  Многие другие государства использовали «Будапештскую конвенцию» в качестве руководства при разработке соответствующих положений своего законодательства.  Договор открыт для присоединения любого другого государства, готового внедрить его положения в своё законодательство и развивать сотрудничество в данной области.  «Будапештская конвенция» обязывает государства:   * ввести уголовную ответственность за совершение правонарушений, направленных против компьютерных систем (несанкционированный доступ к информации, противозаконный перехват данных, вмешательство в базы данных и в работу компьютерных систем и т. д.) и правонарушений, совершаемых с помощью компьютеров (таких как мошенничество, детская порнография и преступления против интеллектуальной собственности). Здесь важно отметить следующее: этот международный документ технологически нейтрален, он не ограничивает развитие технологии или же технических средств. То есть, в нём речь идёт о мошенничестве, а не о техническом способе его реализации в виде «фишинга», о несанкционированном доступе к информации, а не о «хакерстве», о противозаконном вмешательстве в работу компьютерных систем, а не о технических деталях проведения атак с целью нарушения нормального обслуживания пользователей и т. д. * предоставить правоохранительным органам инструменты для обеспечения сохранности доказательств в электронной форме (на этапах их собирания, проведения обыска/выемки, оперативного обеспечения их целостности и т. д.). Здесь важно отметить, что эти меры относятся не только к киберпреступлениям, но и к любым иным противоправным деяниям, доказуемым с помощью улик в электронной форме в компьютерных системах. * осуществлять эффективное международное сотрудничество, выражающееся в принятии оперативных текущих мер, в оказании взаимопомощи на официальном уровне, а также в участии в контактной «Сети 24/7» по борьбе с киберпреступностью.     Все вышеперечисленные меры – прежде всего процессуального характера – направлены на обеспечение соблюдения прав человека и верховенства закона. С этой точки зрения особое значение имеет статья 15 конвенции, в которой речь идёт об обеспечении сохранности хранимых компьютерных данных.  Прежде всего «Будапештская конвенция» позволяет правительствам выполнять свои позитивные обязательства по защите личности от посягательств киберпреступников и одновременно обеспечить соблюдение её прав в борьбе с таковыми.    В настоящее время благодаря принятию «Будапештской конвенции» были достигнуты следующие результаты:   * повсеместно идёт процесс законодательных реформ; * органы уголовного правосудия усиливают меры безопасности; * стороны конвенции с большим доверием относятся к сотрудничеству; * международный отклик/охват: 56 стран ратифицировали, подписали конвенцию или же приглашены присоединиться к ней; налажено сотрудничество с, по меньшей мере, ещё 50 другими государствами; * принятие конвенции ускорило укрепление материально-технической базы органов, противостоящих киберпреступности; * окрепла правовая определённость, усилилось доверие частного сектора; * конвенция легла в основу нормативной базы, регламентирующей поведение в киберпространстве; * конвенция внесла свой вклад в обеспечение соблюдения прав человека и верховенства права; * защитила вас и ваши права. | |
| Слайд 51 | Часть пятая – некоторые виды противозаконной деятельности в сети.  Цель пятой части курса заключается в том, чтобы весьма коротко описать некоторые виды преступной деятельности, имеющей место в информационных компьютерных сетях. | |
| Слайд 52 | Фишинг («выуживание паролей») – это техника, заключающаяся в том, чтобы попытаться убедить пользователя выслать постороннему лицу свою конфиденциальную информацию, которая, затем, может быть использована для кражи или мошенничества. Обычно преступники используют для обмана своих жертв электронные сообщения, пытаясь получить их личную информацию, включая пароли или другие учетные данные для доступа. Иногда, используется техника перенаправления пользователей на вредоносный и фальшивый сайт. | |
| Слайд 53 | СПАМ (от англ. сокращения «тухлое мясо») является очень большой проблемой. Он состоит в распространении нежелательных сообщений по электронной почте, рассылаемых миллионными тиражами. Получатель этих сообщений не может избежать этого. Иногда, сообщения имеют просто рекламные цели. Но, зачастую, они являются проверкой канала связи для распространения вредоносных программ и заражения компьютеров.   Как правило, жертва не знает отправителя сообщений, не запрашивала, и не давала разрешения на их отправку. | |
| Слайд 54 | От слияния слов “*malicious*" ("злонамеренный") и "*software*” ("программное обеспечение") происходит термин “malware” ("вредоносные программы", «мальвеар»)​​, который относится к программному обеспечению, разработанному с целью проникновения в компьютерную систему без согласия собственника или пользователя, или с целью нарушить его работу. Пострадавший может получить вредоносную программу, не замечая этого, через вложения электронной почты или через изображения в сообщениях.  Это, как правило, враждебное программное обеспечение. Оно устанавливается на компьютере жертвы без её согласия для выполнения враждебной функции или деятельности. | |
| Слайд 55 | Вирусы – это конкретный пример вредоносного ПО. Как правило, вирус – это программа, способная воспроизводить/копировать своё тело из одного файла пользователя в другой, и «обитающая» в определенной системе – на жестком диске или на другом носителе данных. Как правило, вирус распространяется только когда зараженный файл копируется или выполняется. Конечно, все это осуществляется без согласия или даже без уведомления жертвы с целью причинения ущерба компьютерной системе. | |
| Слайд 56 | Компьютерный червь очень похож на вирус. Как и вирус, червь - это программное обеспечение, которое имеет способность копировать себя и устанавливаться в определенной системе, потребляя ее ресурсы. Но он отличается от вируса, поскольку распространяет себя через сеть и не должен встраиваться в какой-либо файл. | |
| Слайд 57 | Рекламное ПО (англ. adware = «advertising» + « software» ) также является разновидностью вредоносных программ. Это программное обеспечение, которое автоматически отображает или загружает коммерческую рекламу, без согласия и вмешательства пользователя. Иногда оно распространяется вместе с другим программным обеспечением, или при загрузке бесплатных файлов из Интернета.  Некоторые виды рекламного ПО более опасны, потому что следят за тем, какие сайты в Интернете посещал пользователь, и собирают другие пользовательские настройки и предпочтения. | |
| Слайд 58 | Одной из самых навязчивых форм вредоносных программ являются программы-шпионы (англ. spyware = «spy» + « software» ) – программное обеспечение, установленное в системе без ведома пользователя, с целью сбора информации о пользователе системы и об использования системы пользователем. После этого программа автоматически отправляет эту информацию третьим лицам. Конкретная цель шпиона – скрыться в компьютере жертвы, и сообщить о нём информацию кому-то в сети. | |
| Слайд 59 | Название «Трояны» (Троянские кони) происходит от имени знаменитого коня, построенного Одиссеем – примера греческой военной хитрости. Конь был подарен осаждённым жителям Трои для того, чтобы открыть ворота города изнутри. Таким образом, это название вредоносного программного обеспечения, которое выполняет нежелательные для пользователя функции без его ведома. Этот вид вредоносного ПО может привести к разрушению данных и отключению программ обеспечения безопасности. Троян содействует несанкционированному удаленному доступу к компьютеру третьим лицам, или загрузке и инсталляции других вредоносных программы.  Как и в случае оригинального знаменитого коня времён Троянской войны, эти программы предназначены для того, чтобы тайно открыть компьютер для проникновения извне. | |
| Слайд 60 | «Бот-сеть» также является аббревиатурой от англ. «*robot networks»* (сеть роботов), используемая для наименования сети зараженных компьютеров (зомби), контролируемых одним лицом или организацией, с целью их использования для незаконной деятельности.   Бот-сеть основана на заражении компьютера вредоносной программой, рассылаемой владельцем бот-сети. Все зараженные компьютеры управляются одним программным обеспечением, позволяющим автоматизировать операции по сети. Владелец сети контролирует свою деятельность и может дать ей указание оставаться неактивной, пока в ней нет необходимости.  Бот-сеть может состоять из миллионов компьютеров-зомби, которым может быть дана команда для рассылки спама или вредоносного ПО частным лицам, а также для атаки инфраструктурных объектов. Бот-сети могут быть использованы для различных преступных целей и их, поэтому, иногда называют «швейцарским армейским ножом» киберпреступников. | |
| Слайд 62 | Часть шестая – Подведение итогов занятия | |
| Слайд 63 | Что собой представляет киберпреступность и почему она должна вызывать нашу обеспокоенность?  Угрозы, основные направления развития и технические средства киберпреступности; ответные меры.  Реалии, скрывающиеся за выражением сетевая компьютерная преступность (киберпреступность); виды киберпреступлений в соответствии с положениями большинства законодательств и с международными нормами.  Необходимость и выгодность гармонизации национальных законодательств и международных юридических документов на основе, прежде всего, «Будапештской конвенции». | |
|  | Практические занятия (проводятся при наличии необходимых условий).В рамках этого занятия они не предусмотрены за отсутствием гарантий того, что во всех местах его проведения будут в наличии технические средства должного уровня и доступ в интернет, необходимый для их проведения.  На будущее инструктора могут добавочно ввести практические занятия в учебный план в том случае, если на месте их проведения будут соблюдены все необходимые технические условия. | |
|  | **Проверка знаний**  На этом занятии никакой дополнительной проверки в дополнение к вышеперечисленным требованиям в настоящее время не предусмотрено. Также, не требуется проводить никакого официального зачёта. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Занятие 1.1.3, 1.2.2 & 1.2.5 – Техническиесредства | | | | **Продолжительность: 330 минут** |
| Перечень материалов, необходимых для проведения занятия:  * Ноутбук или ПК с операционной системой Windows 7 и с загруженным офисным пакетом приложений MS Office 2010; * проектор с экраном; * доступ в сеть Интернет (при наличии); * презентация «ПауерПойнт»; * образчики аппаратных средств ЭВМ (при наличии); * видеоролик «Воины сети» («Warriors of the Net») | | | | |
| **Цель:** на этом занятии слушатели будут ознакомлены с техническими средствами, используемыми преступниками для совершения противоправных деяний, а также правоохранительными органами для раскрытия таковых. Соответственно, работники суда и прокуратуры будут сталкиваться с вышеуказанным компьютерным оборудованием в своей работе. Таким образом, полученные на этом занятии знания позволят им более эффективно выполнять свои обязанности, что и является его конечной целью. | | | | |
| **Задачи:**  По окончании занятия слушатели должны быть в состоянии:   * Объяснить, как развитие технических средств отражается на характере преступности * Перечислить составные части компьютерной системы * Определить/распознать различные типы устройств хранения данных. * Рассмотреть, как отразилось на работе органов уголовного правосудия увеличение в геометрической прогрессии ёмкости запоминающих устройств. * Определить/распознать различные компьютерные операционные системы. * Объяснить основные принципы работы интернет сетей. * Описать функции интернета. * Определить/распознать как минимум 5 основных интернет приложений (прикладных программ интернета). * Изложить историю развития интернета от его истоков и до наших дней. * Объяснить разницу между различными интернет приложениями. * Рассказать, как киберпреступники используют различные интернет приложения в своих целях. | | | | |
| **Продолжительность** | **Содержание:** | | | |
| 30 минут  60 минут  60 минут  60 минут  60 минут  30 минут  30 минут | * Введение и открытие (план работы и задачи занятия) * Часть 1 – Как работает компьютер * Часть 2 – Как работает интернет * Часть 3 – Службы интернета * Часть 4 – Другие важные интернет приложения * Часть 5 – Интернет преступления * Часть 6 – Подведение итогов занятия | | | |
| **Слайд №** | **Содержание:** | | | |
|  | Вводное занятие для работников суда и прокуратуры на тему: компьютерные технические средства  Для ведения этого занятия инструкторам даётся лишь его общая структура, на основе которой они выстраивают учебный материал, подаваемый как часть более обширной программы. По своему содержанию она не может быть исчерпывающей и окончательной, так как наука и техника развиваются столь стремительно, что любой более или менее подробный с технической точки зрения отчёт устаревает уже к моменту своей публикации. В данном случае принципиально важно для обеспечения должного отправления правосудия добиться того, чтобы присутствующие на нём работники суда и прокуратуры в достаточной степени овладели технической стороной изучаемого предмета в тех пределах, которые им необходимы по работе. Таким образом, на этом занятии даётся общий обзор основных компьютерных технических средств и объясняется, какой интерес они представляют с точки зрения уголовного правосудия. В качестве наглядного материала прилагается презентация «ПауерПоинт», использование которой оставляется на усмотрение инструкторов.  Кроме того, предоставляется ещё одно, дополнительное наглядное пособие в форме видеоролика «Воины сети», с помощью которого слушатели получат ясное и чёткое представление о том, как работают интернет сети. Этот ролик выложен на сайте www.warriorsofthe.net на следующих языках: английском, немецком, французском, иврите, датском, шведском, итальянском, португальском, датском, норвежском, венгерском, чешском, испанском и украинском.  На этом занятии слушатели будут ознакомлены с техническими средствами, используемыми преступниками для совершения противоправных деяний, а также правоохранительными органами для раскрытия таковых. Соответственно, работники суда и прокуратуры будут сталкиваться с вышеуказанным компьютерным оборудованием в своей работе. | | | |
|  | Презентация «ПауерПоЙнт»  В дополнение к этому занятию была подготовлена с помощью программы «ПауерПойнт» презентация. Для инструкторов она служит примером того, как они могут самостоятельно разрабатывать свои собственные наглядные пособия для реализации поставленных задач. Здесь важно напомнить, что именно инструктора отвечают за своевременную подготовку учебных материалов. Таковые должны быть актуальными и представлять конкретный интерес для аудитории, а не просто основываться на документации, составленной их коллегами раньше. | | | |
| Слайды 2 и 3 | План занятия  На слайде показано, как в плане занятие разбито на части. Инструктор должен тщательно, попунктно разобрать их, останавливаясь при необходимости на тех специфических аспектах изучаемого предмета, которые представляют особый интерес для той или иной части аудитории. Кроме того, ему необходимо объяснить, в какой форме будет осуществляться подача материала и когда предусмотрено время для взаимного обмена мнениями и вопросов. Инструктору следует подчеркнуть, что этот практикум (тренинг) задумывался как мероприятие, ведущееся в режиме взаимного диалога, и что поэтому он ожидает от слушателей активного участия. Кроме того, он должен объяснить, предусмотрен ли экзамен, в какой форме и будет ли какой-нибудь «проходной балл». (для этой экспериментальной программы проведение экзамена не предусмотрено). | | | |
| Слайд 4 | Задачи занятия  Важно, чтобы слушатели уяснили себе задачи занятия, которые должны соответствовать требованиям «SMART ». Их надо подробно объяснить аудитории с самого начала с помощью наглядной информации на соответствующем слайде. | | | |
| Слайды 5 - 54 | Часть первая – как работает компьютер   * Перечислить составные части компьютерной системы * Определить/распознать различные типы устройств хранения данных. * Рассмотреть, как отразилось на работе органов уголовного правосудия увеличение в геометрической прогрессии ёмкости запоминающих устройств. * Определить/распознать различные компьютерные операционные системы. | | | |
| Слайд 5 | Для того, чтобы судьи и прокуроры представили во всей полноте роль технических средств в современных правонарушениях, необходимо, чтобы они поняли основные функции этого оборудования и этих технологий. В случаях, когда сбор доказательств производится методами электронной криминалистики, в самом широком смысле этого термина, понимание контекста позволит им принимать решения, наполненные содержанием. На этом занятии слушатели получат общее представление о компьютерах, их компонентах, хранении данных и возможных последствиях наличия большого количества данных на персональных устройствах. Подчеркнём ещё раз, что инструктор должен пытаться сделать это занятие максимально интерактивным и использовать изложение материала так, чтобы слушатели осознали необходимость учёта возможностей технических средств в своей профессиональной деятельности, ознакомились с методами управления таким большим количеством данных и их эффективного использования в системе уголовного правосудия.  Если это представляется возможным, инструктор должен принести образцы оборудования, о котором пойдёт речь на этом занятии, для демонстрации его слушателям и создания предметной опоры изложения.  Существует большое количество компьютерных компонентов, которые на этом занятии не рассматриваются, однако наиболее важные для целей курса группы оборудования в него включены. Рекомендуется включать в программы обучения слушателей компоненты, не охваченные здесь, но соответствующие уровню знаний и квалификации аудитории. Можно было бы ожидать, что большинство слушателей понимают, что такое клавиатура и мышь, но инструкторам не следует переоценивать уровень знаний аудитории. Список устройств, которые могут быть добавлены к приведённым выше, может включать: принтеры, сканеры, веб-камеры, модемы, звуковые колонки, компьютерные и видеофоны, различные устройства хранения данных и организации сетевых подключений, а также внешние порты, такие как Firewire и USB.  В частности, обратитесь к ресурсу <http://computer.howstuffworks.com/computer-hardware-channel.htm>, который содержит подробную информацию о компьютерных аппаратных средствах. Ресурс предоставляет фотоизображения, которые смогут существенно увеличить легкость усвоения эти понятий. Не забудьте получить разрешение от владельцев информации, если она предлагается для использования в программах обучения. | | | |
| Слайд 6 | Этот слайд демонстрирует, что даже самый технически грамотный человек не может в полной мере оценить те изменения, которые привносят новые технические средства. Слушатели не одиноки в возможном непонимании последствий, которые оказывает технология на их профессиональные роли, и отсылка к этому слайду может побудить их к принятию того, что в системе уголовного правосудия не нужно бояться технических средств, но использовать их возможности, с обеспечением всех необходимых гарантий. | | | |
| Слайд 7 | В качестве введения к описанию компьютерных компонентов, инструктор должен привести краткое объяснение развития компьютеров от автономных систем, через терминалы мэйнфреймов, в мир компьютерных сетей. | | | |
| Слайд 8 | Компьютерные компоненты  Инструктор должен объяснить, что компьютер состоит из большого количества компонентов, и для судей и прокуроров важно знать названия и понимать функции этих компонентов, поскольку они будут использованы в заявлениях и доказательствах.  Краткое объяснение каждого компонента даётся на следующих слайдах: | | | |
| Слайды 9 и 10 | * Материнская плата – известная, как основная плата или системная плата. Материнская плата является центральной платой компьютера. Все остальные компоненты и периферийные устройства подключаются к ней. Работа материнской платы заключается в передаче информации между прочими компонентами. На материнской плате работает базовая система ввода-вывода БСВВ (англ. «Basic Input Output System», BIOS, «БИОС»), которая является довольно простой программой, запускаемой на компьютере при начальном загрузке. Напрямую к материнской плате подключаются такие компоненты, как память, центральный процессор (англ. «Central Processing Unit», CPU, «ЦэПэУ»), видеокарта, звуковая карта, жесткий диск, дисководы, а также, различные внешние порты и периферийные устройства. * Порты расширения/Слоты - это разъёмы на задней панели компьютера, где вы можете подключить звуковые карты, видеокарты, беспроводные адаптеры и т.д. | | | |
| Слайды 11 - 13 | * КМОП и БСВВ (англ. CMOS и BIOS) - часто используются как синонимы. КМОП является аббревиатурой технологии изготовления микросхем – комплементарная структура металл-оксид-полупроводник (англ. CMOS произносится как "Си-МОС", complementary metal-oxide-semiconductor). Вы можете думать о BIOS как о программном обеспечении, и о CMOS как об аппаратном устройстве, исполняющем его. В данном контексте речь идёт о микросхеме, расположенной на материнской плате, то есть об аппаратным устройстве, которое выполняет функции BIOS очень низкого уровня – простые пусковые подпрограммы, – а также хранит их данные. Для того, чтобы BIOS мог выполнять свою работу, CMOS выполняет такие задачи как, хранение часов компьютера и обеспечение интерфейса с остальной частью компьютерного оборудования. Это требует очень мало мощности. * БСВВ это аббревиатурой от «базовая система ввода-вывода» (англ. BIOS произносится как «БИОС», Basic Input/Output System). BIOS представляет собой интерфейс, который позволяет пользователю выполнять низкоуровневые изменения на материнской плате, в процессоре, в памяти и на других устройствах. Заводские настройки BIOS, настройки «по умолчанию», обеспечивают, как правило, наиболее удобные для повседневной работы условия. Одно из наиболее распространенных изменений, вносимых в BIOS в процессе сбора доказательств в электронной форме, это изменение порядка, в котором компьютер будет использовать устройства для начальной загрузки. Обычно, судебный эксперт, использующий программное обеспечение на компакт-диске (CD), изменяет BIOS так, чтобы компьютер загружался с компакт-диска, а не с жесткого диска, так как такая загрузка сама по себе приводит к изменению данных. | | | |
| Слайд 14 | * Блок питания - Блок питания (БП) в компьютере регулирует и поставляет электрическую мощность к компонентам, расположенным в общем корпусе. Стандартные источники питания преобразуют входное переменное напряжение 110В или 220В в различные постоянные напряжения, подходящие для питания компонентов компьютера. Блоки питания имеют определенную мощность, указываемую в ваттах. Стандартный блок питания, как правило, в состоянии обеспечить около 350 Вт мощности. Чем больше компонентов в ПК, тем больше мощность, требуемая от источника питания. | | | |
| Слайд 15 | * Центральный процессор (англ. CPU, произносится «Си-Пи-Ю» – central process unit). Полностью – центральный процессор вычислительной системы. Многие часто принимают корпус или шасси компьютера за его центральный процессор. Однако, процессор является внутренним компонентом компьютера и находится на материнской плате. Как правило, его не видно снаружи системы. Первые процессоры появились в начале 1960-х годов. С введением интегральных схем в конце 1970-х, стало возможным производить процессоры малых размеров. Это способствовало тому, что компьютеры из больших, громоздких устройств, которые занимали целые комнаты превратились в более управляемые настольные, а затем и в портативные устройства. Независимо от типа компьютера, процессор выполняет последовательность введённых в него команд, известную, как программу. Большинство процессоров соответствует архитектуре фон Неймана, в которой процессор должен передавать, декодировать, обрабатывать и выводить данные в довольно быстрой последовательности. Для неспециалиста, центральный процессор, не что иное, как мозг компьютера. То, что компьютер фактически выполняет, в основном делается с помощью его процессора. | | | |
| Слайд 16 | * Память - Памятью компьютера технически может быть любая форма хранения электронной информации, хотя этот термин в узком смысле чаще всего используется для описания тех временных форм хранения, которые могут обеспечить быстрый доступ к данным. Работа компьютера была бы значительно более медленным процессом, если бы процессор должен был получать данные с жесткого диска при каждом обращении к памяти, поэтому большое количество данных временно сохраняется в оперативной памяти для того, чтобы уменьшить время доступна к ним. Этот тип памяти известен как оперативное запоминающее устройство (ОЗУ, англ. RAM – random acess memory). Процессор запрашивает данные из оперативной памяти, обрабатывает их и записывает обратно в ОЗУ. Это происходит миллионы раз в секунду. Понимание концепции временной памяти важно в случае изъятия данных из компьютера, так как эти данные не сохраняется при выключении компьютера, что может произойти при обыске и изъятия компьютерных систем. В настоящее время в практике правоохранительных органов более распространены попытки захватить данные, находящиеся как раз, в оперативной памяти, до отключения питания во время компьютерных обысков. Эта методика широко известна как "криминалистика короткоживущих данных" (англ. Live Data Forensics). Эти мероприятия проводят наиболее часто, так как объем данных, которые могут быть потеряны, превосходит размер самого большого жесткого диска, выпущенного всего несколько лет назад. | | | |
| Слайд 17 | * Универсальная последовательная шина (англ. USB – Universal Serial Bus, «ЮЭсБэ») – разъемы USB, имеющиеся на большинстве современных компьютеров, позволяют легко подключать к компьютеру большое количество разнообразных устройств, как-то, мыши, принтеры, внешние устройства хранения данных и мобильные телефоны. В настоящее время это наиболее распространенный способ подключения внешних устройств к компьютерам. Исторически сложилось так, что другие способы соединения, такие как параллельные или последовательные порты, имели ограничение на количество одновременно подключаемых устройств, а скорость передачи данных у них была гораздо меньше, чем у USB. С помощью USB к компьютеру можно подключить до 127 устройств. Легкость подключения и использования USB устройств ставит их на видное место во многих случаях сбора доказательств в электронной форме. | | | |
| Слайды 18 - 20 | * Жесткие диски - Большинство компьютеров имеют по крайней мере один жесткий диск; многие имеют два и более. Большие компьютеры, такие как мэйнфреймы, как правило, имеют множество жестких дисков. Другие современные устройства, такие как системы видеонаблюдения и музыкальные плееры также имеют жесткие диски, которые могут вместить огромные объемы данных. Эти диски состоят из жестких пластин, на поверхности которых хранится информация и данные могут быть легко записаны и удалены, что делает их жизнеспособными в течение длительного периода времени. Данные хранятся на поверхности пластин в секторах и дорожках. Дорожки представляют собой концентрические окружности, а секторы – дуговые сегменты на дорожках. Данные хранятся на жестких дисках в виде файлов, являющихся просто совокупностью "байтов". Исполняемые программы также являются файлами на диске. Все эти данные использует центральный процессор. | | | |
| Слайд 21 | * Твердотельные накопители (англ. Solid State Disk, SSD, произносится «ЭсЭсДе») – это такие устройства для хранения данных (их иногда называют «твердотельный диск» или «электронный диск»), ячейки памяти которых способны долговременно хранить данные. Доступ к этой памяти организован посредством той же системы ввода-вывода, как и у традиционный жестких дисков. Традиционные магнитные диски – жесткие диски HDD или дискеты – являются электромеханическими устройствами с вращающимися дисками и подвижными головками чтения-записи. В отличие от них, SSD-накопители используют микросхемы, которые сохраняют данные в энергонезависимых ячейках памяти [1] и не содержат движущихся частей. [1] В следствие этого, SSD-накопители, как правило, менее восприимчивы к ударам, не шумят, имеют меньшее время доступа и более высокое быстродействие, но стоят дороже в расчёте на 1 гигабайт памяти. SSD-накопители используют тот же интерфейс, что и жесткие диски, и поэтому могут легко заменять их в большинстве приложений. | | | |
| Слайд 22 | * CD / DVD / Blu-Ray-диски (англ. Compact Disk – компактный диск, «СиДи»; Digital Versatile Disk – цифровой универсальный диск, «ДиВиДи»; blue ray – синий луч, «БлюРэй»). Эти диски могут вмещать различный объем данных и, как правило, используется для хранения музыки, видео или компьютерных файлов для коммерческого распространения. DVD, например, имеет тот же размер, что и компакт-диск, но содержит приблизительно в 7 раз больше данных. Blu-Ray диск, который может быть использован для хранения видео контента высокой четкости, вмещает в настоящее время в 10 раз больше, чем DVD. Другими словами, эти диски могут хранить больше данных, чем это было возможно на жестком диске, произведённом всего лишь несколько лет назад. Принципы устройства памяти у всех этих дисков различны, и они отличается от принципа хранения данных на жестких диски. Данные, содержащиеся на этих носителях не так часто изменяются, как хранящиеся на жестких дисках. | | | |
| Слайд 23 | Хранение данных  Получение электронных доказательств, связанных с использованием компьютеров и других электронных устройств, например, мобильных телефонов, является повседневной практикой в уголовном и гражданском судопроизводстве. Поскольку технические средства продолжают проникать в общество, неизбежно станет нормой, что элементы электронных доказательств могут быть получены из все большего и большего количества устройств. Мы уже видим домашние устройства, проверяемые для извлечения таких доказательств.  Поэтому очень важно, чтобы судьи и прокуроры ориентировались в вопросах, которые влияют на целостность и допустимость электронных доказательств. Для начала, им будет полезно понять, как следователи хранят и восстанавливают данные.  Электронные или цифровые данные хранятся в различных формах. Наиболее известным и во многих случаях наиболее доступным для проверки является хранение данных на жестких дисках компьютеров. Типовой подход к сохранению и извлечению электронных доказательств состоит в проверке устройства в статическом состоянии. Другими словами, в состоянии, когда компьютер выключен и данные изменяются не очень интенсивно. Судебные эксперты хорошо знакомы с требованиями международных и национальных инструкций, регламентирующих обращение с такими доказательствами. Одно из таких руководств под названием «Выемка E-доказательства» было разработано при финансовой поддержке программы Ойсин (Oisin) Европейской комиссии. Его можно найти по адресу: <http://www.e-evidence.info>. Это руководство выдвигает общие принципы, по которым работает большинство правоохранительных органов. Важно, чтобы судьи имели четкое представление о том, каким образом хранятся данные и как представляются доказательства, то есть о том, что появляется перед ними. Это требует базового понимания концепции цифровых данных, их хранения, выемки, а также знания инструментов и процедур, используемых для представления этих данных в системе уголовного правосудия. В рамках программы обучения слушателей можно использовать множество открытых ресурсов для разработчиков программного обеспечения по сбору информации о хранении данных на жестком диске. Один из таких источников находится по адресу: <http://www.storagereview.com/hard_disk_drive_reference_guide>. Как правило, речь там идёт об энергонезависимой памяти, такой как магнитные носители, оптические носители, флэш-память и т.д.  В современной кибер криминалистике стало обычной практикой выявление электронных доказательств в энергозависимых устройствах хранения данных, таких как оперативные запоминающие устройства (ОЗУ/RAM) или мобильные телефоны. Судьи должны понимать это отличие в способе получения данных, а также все факторы, влияющие на их целостность. Важность восстановления энергозависимых данных в том, что при выключении устройства они, как правило, утрачиваются, а с ними утрачивается и возможность восстановить большое количество информации, которая может оказаться ценным свидетельством. Методы, используемые для восстановления этой информации должны соответствовать общим принципам сохранения и восстановления таких данных. Характерным примером извлечения энергозависимых данных является выявление электронных доказательств из сетевых компьютерных систем, которые не могут быть выключены для проведения статического анализа. | | | |
| Слайд 24 | Память и хранение данных – На этом слайде даётся обзор терминов, используемых для описания данных, и представление об их объёмах. Слайд предлагает необходимое слушателям введение, для уяснения основных понятий последней части занятия, которая касается различных устройств хранения данных и обсуждения их масштабов. | | | |
| Слайд 25 | Операционные системы  Для того, чтобы компьютеры и другие цифровые устройства выполняли свои функции, необходима операционная система. Операционная система представляет собой программу, которая позволяет аппаратным устройствам взаимодействовать с различными приложениями. Без операционной системы компьютер функционировать не может. Существуют различные типы операционных систем в зависимости от типа компьютера или другого электронного устройства, в котором они применяются.  Широко известны распространенные сегодня операционные системы Windows, Unix/Linux и Apple Mac. Существуют и другие операционные системы, созданные для использования в других типах устройств, таких как смартфоны и мобильные телефоны. Зачастую, это усеченные версии основных систем, хотя для некоторых небольших устройств их производители сейчас заказывают специальные операционные системы.  Большинство программных приложений, разработанных для компьютеров, написаны для конкретных операционных систем, хотя для большинства из них сейчас доступны версии и для других платформ.  Важно, чтобы судьи и прокуроры оценили важность операционных систем и знали, что разные операционные системы ведут себя по-разному. Существует масса ресурсов, дающих возможность инструктору найти достаточно информации об операционных системах для иллюстрации целей учебной программы, изложенных в этом разделе. Среди этих ресурсов отметим следующий:  http://en.wikipedia.org/wiki/Operating\_systems | | | |
| Слайды 26 - 28 | Операционные системы - Cлайды рассказывают о назначении операционных систем, указывают наиболее популярные из них, используемые сегодня, и предоставляют статистическую информацию об их распространенности. Инструкторы должны позаботиться о поддержании этой информации в актуальном состоянии. В частности, информация на Слайде 38 должна обновляться не реже одного раза в год. | | | |
| Слайд 29 | Прочие электронные устройства  Обзорное занятие, посвященное электронным устройствам, позволит слушателям – судьям и прокурорам – оценить разнообразие типов устройств, которые могут потенциально содержать доказательства. Занятие продолжает обсуждение того, сколько данных может содержаться на устройствах, и касается определённых проблем, которые эти объемы данных ставят перед системой уголовного правосудия. | | | |
| Слайды 30 - 38 | Слайды, которые включены в этот раздел достаточно пространны, и инструкторы должны сами определить какой объём информации необходим для достижения цели.  Этот раздел, однако, не описывает различиями между такими устройствами, как мобильные телефоны, флэш-накопители или компьютеры в рамках проблем выявления, выемки и исследования доказательств на этих устройствах. Инструкторы должны рассмотреть возможность использования на занятиях примеров или образцов для поддержки целей обучения.  На этом этапе слушателям будут представлены большое количество технических аспектов. Предполагается, что некоторые из слайдов предоставят им точку зрения, которую можно будет легко усвоить, а также привлекут их внимание к некоторым интересным примерам.  Важно осветить здесь различие характеристик устройств, на которых могут храниться данные и степень проблемы, которую это вносит в систему уголовного правосудия. Инструкторы должны рассмотреть возможность использования примеров, в которых необычные технические устройства предоставили важные источники доказательств по уголовным делам. | | | |
| Слайд 39 | Несколько необычных компьютерных устройств  Этот короткий раздел следует сразу за предыдущим и является продолжением обсуждения характеристик электронных устройств. Снова подчеркнём, что количество относящихся к теме и представляемых слайдов определяет инструктор, руководствуясь, при этом, соображениями достаточности для формирования у слушателей представления о возможности обнаружения доказательств на широком спектре устройств. Следует подчеркнуть, что не все устройства, с которыми можно столкнуться в реальной жизни это то, чем они кажутся на первый взгляд.  Важной особенностью раздела является демонстрация простоты доступа к устройствам, которые могут вмещать многие сотни тысяч страниц документов – потенциальных источников доказательств. | | | |
| Слайды 40 - 45 | Важно осветить здесь различие характеристик устройств, на которых могут храниться данные и степень проблемы, которую это вносит в систему уголовного правосудия. Инструкторы должны рассмотреть возможность использования примеров, в которых необычные технические устройства предоставили важные источники доказательств по уголовным делам. | | | |
| Слайды 46 - 54 | Проблема большого количества данных.  Данный раздел освещает существенный практический аспект, проистекающий из технических возможностей устройств, описанных выше. В частности, вопрос о количестве информации который они могут содержать, и что это означает с точки зрения объёма получаемой документации. Это введение к обсуждению целостности и допустимости электронных доказательств, и их производных, о которых пойдёт речь в дальнейшем.  Фотография на слайде предоставляет слушателям шкалу, позволяющую оценить объем данных, который может поместиться на различных устройствах. Инструкторам рекомендуется использовать другие примеры, которые могут быть более актуальность в их собственной стране.  Еще один важный момент, который необходимо донести, это то, что устройства хранения данных больше не являются дорогостоящим оборудованием, но позволяют вмещать огромные объемы данных на устройствах самых разных типов.  Инструкторы должны также обсудить вопрос о принятия судьями и прокурорами таких решений, которые позволяли бы с разумными затратами времени производить эффективную обработку больших объемов данных или печатных материалов. | | | |
| Слайды 55 - 81 | Часть 2 - Как работает Интернет  К концу занятия слушатели должны быть в состоянии:   * Изложить историю развития интернета от его истоков и до наших дней. * Описывать функции интернета. * Объяснять разницу между различными интернет- приложениями. * Определять/распознавать как минимум 5 основных интернет-приложений. * Определить, как преступники могут использовать различные интернет-приложения. | | | |
| Слайд 55 | На этом занятии слушателям предоставляется основная информация об истории Интернета, его функционировании и услугах, доступных в Интернете. На занятии слушатели узнают, как отличать и четко определять компоненты Интернета, и поймут, как он влияет на систему уголовного правосудия. Инструктора должны приготовить к занятию такие примеры практического характера, которые послужат увеличению ценности технических данных, включенных в презентацию. | | | |
| Слайды 56 - 57 | Термин ИНТЕРНЕТ происходит от сокращения английских слов INTERconnected NETwork - взаимосвязанная сеть. Многие преступные действия предполагают использование Интернета. К ним относятся такие виды преступлений, как взлом, распространение вирусов и фишинг-атаки, а также более традиционные преступления, например, мошенничество. Для того, чтобы судьи эффективно справлялись с рассмотрением подобных случаев, им необходимо понять основы Интернета и его приложений, таких как Всемирная паутина и электронная почта. Ниже приводится введение в этот предмет и предоставляет шаблон для создания успешного учебного модуля. | | | |
| Слайды 58 и 59 | История Интернета  Интернет начал свою жизнь как ARPANET в 1960-х годах. Хотя это и неочевидно на первый взгляд, но при разработке Интернета, он никогда не задумывался, как абсолютно безлопастная среда, что может объяснить сравнительную легкость, с которой преступники могут злоупотреблять этой системой. Первая физическая компьютерная сеть была создана в 1969 году между узлами, находившимся в 4-х различных университетах. Первое письмо было отправлено в 1972 году, а в следующем году был создан новый протокол связи TCP/IP (англ. Transmission Control Protocol, «ТиСиПиАйПи»), который в настоящее время является основным протоколом связи в Интернете. В начале своего развития Интернет, как мы теперь знаем, представлял собой довольно скромные разрозненные локальные сети, имевшие небольшое количество соединений между ними. Это привело к разработке протокола, с разбиением потока информации на небольшие пакеты, для соединения множества различных сетей в рамках одной супер сети.  В дальнейшем, такой подход позволил наладить всё увеличивающуюся по скорости взаимосвязь передовых сетей западного мира. Затем эта технология начала проникать в остальные части света. Несоответствие роста Сети между развитыми странами и развивающимися странами привели к образованию «цифрового барьера», который все еще существует и сегодня.  Затем последовала коммерциализация Интернета, и появление в 1980-х годах частных компаний – Интернет-провайдеров. В 1990-х годах они сделали возможным доступ к Сети огромного количества пользователей. Интернет оказал колоссальное влияние на торговлю, а также на культуру. В настоящее время с его помощью устанавливается практически мгновенная связь между корреспондентами по электронной почте, в нём существуют сайты социальных сетей, текстовые дискуссионные форумы, и Всемирная паутина (англ. World Wide Web). Интернет продолжает расти, что обусловлено развитием электронной сетевой торговли, наличием большого количества онлайн-информации и баз знаний. Мы переживаем появление концепции Web 2.0. | | | |
| Слайд 60 | Инструктор должен постараться сделать так, чтобы сообщаемая слушателям информация позволила им в полной мере понять основы работы в сети и существующие в ней ограничения. Они должны быть в состоянии различать локальные и глобальные типы сетей. Этот слайд предоставляет лишь основную информацию. Инструкторам следует рассмотреть несколько характерных примеров и побудить слушателей к обсуждению различных типов сетей и вопросов устройства Интернета. На данном этапе должно быть предоставлено ​​объяснение некоторых общих, относящихся к теме терминов, таких как порты и пропускная способность. Слушателей необходимо попросить поделиться своим личным опытом использования доступа в интернет, например, дома или на работе. | | | |
| Слайд 61 | Локальная сеть (англ. LAN – Local area network) - это компьютерная сеть, охватывающую небольшую географическую область, например дом, офис или группу зданий, например, школу. Определяющими характеристиками локальных сетей являются высокая скорость передачи данных, малый географический размер, и отсутствие необходимости в арендованных линиях связи.    Глобальная сеть (англ. WAN – wide area network) - это компьютерная сеть, которая охватывает широкую область (то есть любая сеть, чьи звенья пересекают границы города, региона, или государства). Определяя менее формально, это сеть, которая использует маршрутизаторы и коллективные линии связи.  Существуют варианты сетей других типов: личные сети (англ. PAN – personal area network), Кампус сети (англ. CAN – Campus area network), или городские сети (англ. MAN – metropolitan area network), которые, соответственно, ограничены одной комнатой, зданием, учебным заведением, или некоторой агломерацией (например, город). Самый большой и самый известный пример глобальной сети – это ИНТЕРНЕТ. | | | |
| Слайд 62 | Порты - это конечная точка или "канал" для сетевого маршрута. Нумерация портов позволяет различным приложениям на одном и том же компьютере одновременно использовать сетевые ресурсы, не мешая друг другу. В контексте сетевого маршрута данных, порт является виртуальным понятием – это адрес в памяти компьютера. Не следует его смешивать с портом, к которому вы подключаете периферийные устройства.  Пропускная способность компьютерной сети характеризует интенсивность информационного обмена, который может быть осуществлен с помощью телефонной линии, кабельной линии, спутникового канала, и так далее. Чем больше пропускная способность, тем больше скорость вашего соединения и тем больше загрузка Интернет-страниц напоминает «мгновенную» загрузку, в стиле телевизионной передачи. | | | |
| Слайд 63 | Сетевой адаптер (англ. NIC - Network Interface Controller) - это плата или карта установленная ​​в компьютер, что позволяет ему подключиться к сети.  Адрес доступа к управлению медиа (англ. MAC address - Media Access Control) – это уникальный идентификатор, присвоенный производителем большинству сетевых адаптеров или сетевых карт (NIC). Однозначная идентификация сетевого устройства обеспечивается уникальным значением адреса.  Сетевой концентратор (англ. Hub, «Хаб»), или просто концентратор, представляет собой разветвитель для соединения между собой нескольких устройств по кабелю типа витая пара или оптоволоконному Ethernet, что позволяет им работать, как единому сегменту локальной сети. Концентраторы работают на физическом уровне (уровень 1) сетевой модели ЭМВОС (англ. OSI - open systems interconnection), и термин «коммутатор уровня 1» часто используется наравне с термином «концентратор». Концентратор, таким образом, является разновидностью повторителя с несколькими физическими портами. Сетевые концентраторы также ответственны за передачу всем портам служебного сигнала временного наложения сетевых пакетов (jam signal), если обнаруживается такой конфликт. | | | |
| Слайд 64 | Сетевой коммутатор (Network switch) - это компьютерное сетевое устройство, которое связывает между собой различные локальные сегменты сети. В прошлом, для установления быстрого соединения использовались коммутаторы уровня 2, когда в содержимом ассоциативной памяти (англ. CAM - content addressable memory) нужно было искать только MAC-адрес. С появлением троичной ассоциативной памяти (ternary CAM - TCAM), оказалось, что искать IP-адрес или MAC-адрес можно с одинаковой скоростью.  Маршрутизатор (Router) - это устройство, которое определяет следующую точку сети, в которую пакет должен быть передан по направлению к месту назначения. Он должен быть подключен, по крайней мере, к двум сетевым сегментам. Устройство имеет процессор и работает с составлением таблицы маршрутизации. Оно расположено на входном узле сегмента сети. Термин «коммутатор уровня 3» часто используется наряду с термином «маршрутизатор», но «коммутатор» - это очень общий термин, без точного технического определения.  Сервер (Server) – это компьютер или устройство, которое предоставляет информацию или услуги (сервисы) другим компьютерам в сети. При использовании соответствующего программного обеспечения, любой компьютер, подключённый к сети, может быть настроен в качестве сервера. В большинстве случаев, в сетевом сегменте выделяется мощный компьютер, который должен работать в круглосуточном режиме. Один компьютер может одновременно предоставлять несколько сервисов - например, веб-сервер, почтовый сервер, файловый сервер, сервер печати и т.д. В бизнес-реальности часто имеет смысл запускать различные сервисы на разных машинах по соображениям безопасности и чтобы свести к минимуму воздействие любого отказа. | | | |
| Слайды 65 и 66 | **Основы Интернета**  Интернет можно рассматривать как систему информационных организационных структур, обеспечивающую функционирование множества различных приложений, которые могут выполняться одновременно. Если даже часть интернета окажется неисправна или разрушена, то передача данных всё равно сможет продолжаться. Никто не владеет Интернетом – ни какая-либо организация, ни корпорация, ни правительство. Эта система в значительной степени регулируется сама. Все её пользователи используют одну и ту же технологию подключения.  Большинство современных сетей передачи данных, как и Интернет, описываются формулой "без установления соединения" или "с коммутацией пакетов". Трафик делится на небольшие пакеты, каждый из которых находит свой ​​путь от отправителя к получателю. Не все пакеты одного отправителя следуют одинаковым маршрутом. Они соединяются вместе только когда достигнут места назначения. | | | |
| Слайды 67 и 68 | Инструктора должны четко объяснить, как работают различные приложения, использующие Интернет, приводя примеры и объясняя, что эти приложения из себя представляют. В дополнение к обзору, представленному на этом слайде, следует уделить время для показа рабочих примеров каждого из выбранных приложений.  Наиболее важным, из довольно большого числа интернет-протоколов, является Internet Protocol (IP-протокол). Каждый компьютер, подключенный к сети Интернет должен его использовать. IP-адрес – это «телефонный номер» вашего устройства в Интернете. Более того, не имея IP-адреса, устройство не смогло бы использовать Интернет. Различные приложения и службы используют для связи в сети множество разнообразных протоколов. Вот некоторые из них: HTTP - протокол передачи гипертекста; SMTP - простой протокол передачи почты; FTP - протокол передачи файлов; NNTP – Протокол передачи сетевых новостей. Все эти протоколы действуют на основе IP-протокола (не вместо него). | | | |
| Слайды 69 и 70 | Большинство пользователей подключается к Интернету через Интернет провайдеров (англ. ISP - Internet Service Provider). Эти коммерческие организации сдают пользователю в аренду место на дисках своих компьютеров. Они ведут учёт пользователей ... но как долго хранятся пользовательские данные? Существуют национальные и международные законы, защищающие данные и конфиденциальность пользователей. Эти нормы определяют, как долго данные могут быть сохранены на диске провайдера. Это, конечно, ограничивает возможности сотрудников системы уголовного правосудия по извлечению доказательств из этих источников. Подключение, как правило, производится одним из следующих способов: по телефонной линии, широкополосный доступ по телефонной линии (ADSL), многоканальная передача данных (ISDN), кабельное соединение (Cable), беспроводной доступ или спутниковая связь.  Необходимо рассказать слушателям о том, какие бывают подключения к Интернету. Нужно поощрять слушателей к обсуждению их собственных способов подключения. Следует пояснить, что провайдеры ведут учет данных пользователей, но законодательство о защите пользовательских данных ограничивает время хранения данных.  Роль провайдера и его правовой статус должны быть объяснены слушателям. Это хорошая возможность обсудить важность отношений с провайдерами в связи с вопросами доступа к данным и проведения санкционированного перехвата.  Для простоты можно сказать, что провайдеры сдают пользователям доступ к Интернету в аренду, являются ли их клиенты частными лицами или организациями.  Каждый провайдер хранит определенную информацию о своих клиентах. Детали и количество этой информации зависит от провайдера, а продолжительность хранения данных составляет от несколько часов до нескольких дней.  Данные, которые можно получить от провайдеров:  Имя, адрес и другая информация используемая для регистрации  Дата регистрации и способ регистрации пользователя  Адреса электронной почты или уникальные для пользователя названия экранов  Финансовые детали: кредитные карты, используемые для оплаты услуг провайдера  Возможно, некоторые детали используемых пользователем программ  Самое главное: детали истории пользовательской онлайн активности - даты, время и продолжительность  Информация о времени доступа чрезвычайно важна (вопросы часовых поясов рассматриваются далее в этом разделе). Следует отметить, что создавая учетную запись, пользователь может ввести неверные данные о себе.  Может ли провайдер перехватить подозрительный интернет-трафик? Да, но такая возможность зависит от наличия специального оборудования для записи активности и мониторинга того, что происходит, т.е. нужен штат сотрудников, что генерирует дополнительные расходы. Кроме того, для выполнения перехвата, необходимо рассмотреть вопрос о полномочиях. В любом случае, связаться с провайдером необходимо в самом начале расследования.  Преобразование сетевых адресов (англ. Network Address Translation) – это техника, позволяющая изменить IP-адрес источника и/или назначения в пакете данных, когда он проходит через сетевой экран (брандмауэр) или маршрутизатор. Наиболее часто она используется, чтобы организовать доступ в Интернет для нескольких компьютеров в локальной сети через один IP адрес.  Можно рекомендовать, чтобы любой учебный курс включал в себя объяснение некоторых деталей работы сети и, в частности, тот факт, что начиная с IP версии 4, IP-адреса представляют собой 4 группы по 3 цифры (32-разрядная адресация). В каждой группе – 256 значений от 0 до 255. Каждая группа называется октета (28), а некоторые значения защищены. Следует объяснить, как составляются IP-адреса. Этого можно легко достичь с помощью визуального представления двоичной нумерации, из которых они получены. В дальнейшем следует объяснить разницу между статическими и динамическими IP-адресами и влияние этого факта на расследование. Должны быть даны объяснения изменений в IP версии 6, связанные с тем, что в Интернете начинают заканчиваются IP-адреса. | | | |
| Слайды 71 и 72 | Использование Интернета в глобальном масштабе является его важной особенностью. Два данных слайда показывают, во-первых, два различных метода подачи информации, и во-вторых, процесс проникновения разных языков в систему Интернета, и изменения возникающие в нём за достаточно короткий период времени. Как и в случае прочего, зависящего от времени содержимого занятия, инструктор должен будет убедиться, что информация является актуальной и происходит из надёжных источников. | | | |
| Слайд 73 | Как работает интернет?  Этот раздел занятия позволит слушателям получить представление о том, как данные передаются по Интернету. Приводятся только основные факты, что вполне оправдано для данной аудитории. | | | |
| Слайд 74 | В случае IP-протокола, пакеты имеют переменный размер. Любые два пакета могут проходить от источника к получателю по разным маршрутам. Компьютер-получатель собирает весь трафик, и если отсутствуют какие-нибудь пакеты, запрашивает их повторную передачу.  Преимуществом такой схемы является то, что сеть является общим ресурсом, который может быть динамически распределён в зависимости от потребностей данного момента времени. Недостатком является то, что становится трудно гарантировать качество передачи, так как нет выделенного соединения. Эта проблема сейчас решается, и некоторые приложения IP-телефонии, например, предлагают отличное качество звука. | | | |
| Слайды 75 и 76 | Две иллюстрации на этих слайдах позволяют инструктору легко объяснить, как организован Интернета трафик. | | | |
| Слайд 77 | Фильм под названием «Войны Сети» это отличный ресурс для иллюстрации концепции Интернета. Это идеальный инструмент-введение в Интернет для начинающих пользователей. Он помогает новичкам «увидеть», как работает Сеть. Продолжительность фильма составляет 12 минут. Речь идет о путешествии IP-пакета через сетевые маршрутизаторы, межсетевые экраны и трансатлантические кабели. Он доступен для бесплатной загрузки и для некоммерческого использования с www.warriorsofthe.net и в настоящее время (янв. 2012) доступен на следующих языках: английском, немецком, испанском, иврите, голландском, шведском, французском, итальянском, португальском, датском, норвежском, венгерском, и чешском. Еще один полезный ресурс для оценки уровня проникновения Интернета и роста количества пользователей в различных странах или регионах, можно найти на http://www.internetworldstats.com/ Элементы статистической информации рекомендуется вводить в обучение для того, чтобы слушатели могли оценить влияние Интернета в их собственной стране. | | | |
| Слайд 78 | Важно, чтобы слушателя получили представление об IP-адресах и ограничениях IP версии 4. Мы будем опираться на это в последующем, при обсуждении динамической и статической IP-адресации. Эта небольшая ремарка подводит нас к следующему разделу – о будущем Интернета. | | | |
| Слайд 79 | Большинство провайдеров имеют меньше IP-адресов, чем клиентов, рассчитывая на то, что не все клиенты будет подключен в одно и то же время. Использование динамического распределение IP-адресов позволяет сократить потребность в IP-адресах.  Поскольку вполне вероятно, что данный IP-адрес, может использоваться разными людьми в один и тот же день, то становится ясно, что проверка времени и даты доступа (с учётом часового пояса) имеет решающее значение при расследовании в отношении подозреваемых.  Интернет-провайдеры могут предлагать и статические IP-адреса (например, для размещения веб-сайта), но по более высокой цене. | | | |
| Слайды 80 - 81 | Будущее Интернета – это постоянно изменяющееся празднество, однако появление IP версии 6 принесет много изменений, как в нашу жизнь, так и в систему уголовного правосудия. Инструктор должен объяснить, что IPv6 позволит почти каждому отдельному устройству иметь свой ​​собственный IP-адрес, а это прямой способ отслеживания, который будут использовать в будущем.  Должны быть приведены примеры того, как Интернет, изменяясь, влияет на эти способы расследования и контроля. Изложение должно быть адаптировано к конкретной аудитории. В качестве таких примеров можно привести воздействие на пропускную способность, интернет торговлю и беспроводные системы. | | | |
| Слайды 83 - 111 | Часть третья - Интернет услуги | | | |
| Слайд 83 | На этом занятии будет более подробно рассказано об услугах, которые доступны в Интернете, в частности о Всемирной паутине и об электронной почте. | | | |
| Слайд 84 | Прежде, чем перейти к подробностям описания услуг, доступных в Интернете, стоит поразмыслить о том, в какой степени страны на национальном уровне полагаются на эти услуги в настоящее время. Инструкторы должны представить обзор существенных элементов национальной инфраструктуры в своих странах, чтобы слушатели усвоили, насколько важным стал Интернет в вопросах национальной безопасности за сравнительно короткий промежуток времени. | | | |
| Слайд 85 | **Всемирная паутина (англ. World Wide Web или WWW)**  Термин Всемирная паутина фактически родился в 1991 году, когда сэр Тим Бернерс-Ли изобрёл язык гипертекстовой разметки HTML (англ. Hypertext Markup Language, «АшТиЭмЭль»). HTML предоставил платформу для объединения на веб-страницах текстов, картинок и звуков. Веб-стандарты создаются Консорциумом Всемирной паутины (англ. World Wide Web Consortium, W3C). Следующая цитата даёт объяснение происхождению названия «паутина». "Документы в WWW-мире ссылаются друг на друга с помощью ссылок. Этот мир подобен сооружениям паука, поэтому называется «паутина»" *(Тим Бернерс-Ли, Роберт Кайо;. Всемирная паутина; сентябрь 1992)*. | | | |
| Слайды 86 и 87 | Доступ к паутине, как правило, осуществляется с помощью браузера – программы, разработанной для поиска и отображения веб-страниц. Наиболее распространенными, по состоянию на январь 2012, являются: ​​Mozilla Firefox, Google Chrome, Internet Explorer, Safari и Opera. Инструкторы должны помнить, что любые статистические данные, подобные приведённым здесь, подлежат систематическому обновлению. | | | |
| Слайды 88 и 89 | Протокол передачи гипертекста (англ. Hyper-Text Transfer Protocol, HTTP, «ЭйчТиТиПи») – это общий язык обмена в Интернете между веб-браузерами и веб-серверами.  Хотя WWW браузеры поддерживают различные протоколы, например, FTP, NNTP, SMTP и т.д., HTTP является средством передачи, который используется наиболее часто. HTTP выполняет простые запросы/ответы по базовому Интернет протоколу связи TCP.  Многие ошибочно думают, что WWW это и есть Интернет, вероятно, потому, что WWW – это одно из широко распространённых приложений. Зачастую преступники эксплуатируют это популярное приложение.  При разработке учебной программы, следует включить в неё примеры преступной деятельности с использованием WWW, постольку поскольку это имеет отношение к стране, в которой производится обучение. | | | |
| Слайд 90 | Доменные имена и IP-адреса  Данный раздел предназначен для ознакомления слушателей с базовыми принципами построения IP-адресов и их назначением без объяснения технических подробностей соотношения IP-адреса и доменного имени, которые выходят за рамки этого курса. Важно, чтобы инструктор объяснил этот аспект настолько просто, насколько это возможно. Представленные материалы показывают, каким образом этого можно достичь. | | | |
| Слайды 91 - 93 | В данном разделе должны быть представлены три основные понятия:  1. Во-первых, объясняется понятие унифицированного указателя ресурса (англ. «Uniform resource locator», URL, «ЮЭрЭл») и его состав;  2. Затем, даётся объяснение статической IP адресации – статический IP-адрес выделяется на постоянной основе и, таким образом, всегда соотносится с одним и тем же устройством.  Динамические IP-адреса выделяются каждый раз, когда вы подключаетесь к интернету, но в течение нескольких секунд после отключения вашего устройства, его IP-адрес может быть вновь перераспределён.  Именно по этой причине, важное значение имеет точное время доступа в Интернет.  3. Наконец, объясняется взаимосвязь между IP-адресом и URL именем. Доменные имена и IP-адреса взаимозаменяемы, если известен IP-адрес, то его можно набрать вместо имени домена в адресной строке браузера. Произойдёт подключение к тому же сайту.  На практике обычно происходит наоборот: вы вводите удобное доменное имя, например www.open.gov.uk, и сервера, в рамках интернет-системы, переводят его в IP-адрес и отправляют вас на нужный сайт.  В Интернете доменное имя преобразуется в уникальное 32-х разрядное число (IP-адрес), как правило, написанное в нотации Dotted Quad – серия из четырех 8 битных чисел, в десятичной записи, разделенных точками. Как и в примере, приведённом выше (212.140.189.10), все числа в этой последовательности должны находиться в диапазоне между 0 и 255 (т.е. имеется всего 256 вариантов). Очевидно, что в приведенном примере последний номер нужно читать как 010, однако, соглашение позволяет сокращать незначащие нули и читать 10. | | | |
| Слайд 94 | Следы  Важным аспектом работы с киберпреступлением является понимание того, что следы могут быть оставлены самими следователями при использовании Интернета для проведения расследований. Это относится не только к следователю, но и к прокурору, который может вынести распоряжение о расследовании, и к судьям в свете перспективы допустимости доказательств. В этом разделе следует предоставить слушателям базовые знания, которые позволят им понять риски, которые могут привнести в расследование онлайн подключения. | | | |
| Слайды 95 - 98 | На этих слайдах презентации слушателям представлена основная информация о том, какие сведения оставляются любым пользователем, в том числе самим следователем, посещающим веб-сайты. Это нужно связать с важностью обеспечения защиты идентичности следователя в этих условиях, и с указанием, что в некоторых юрисдикциях, существуют юридические условия, которые должны быть выполнены для того, чтобы такие расследования могли иметь место. | | | |
| Слайды 101 - 104 | Электронная почта  Электронная почта (англ. E-mail, «И-мейл») представляет собой способ обмена сообщениями (текст, изображения, документы, архивы).  Для пользователя процесс выглядит так, будто электронная почта передается непосредственно от машины отправителя к машине получателя; однако каждое сообщение проходит за время передачи через, по меньшей мере, четыре компьютера.  1. Сообщение составляется на компьютере пользователя, а затем отправляется на SMTP почтовый сервер\* Интернет-провайдера (англ. Simple Mail Transfer Protocol - простой протокол передачи почты, «ЭсЭмТиПи»)  2. SMTP сервер\* Интернет-провайдера пересылает исходящую электронную почту на SMTP сервер\* Интернет-провайдера получателя (SMTP – SMTP передача)  3. Почтовый сервер получателя находит входящий POP3 сервер получателя (англ. Post Office Protocol или POP3 – протокол почтовой службы) и доставляет сообщение в «почтовый ящик» получателя.  4. Получатель входит в систему, и сообщения переправляются в почтовый ящик на его компьютере и, как правило, удаляются из его почтового ящика на почтовом сервере.  \* Почтовый сервер – выделенный компьютер, который используется для обработки почты | | | |
| Слайд 105 | Существуют различные виды электронной почты.  Традиционная электронная почта, типа приложения Outlook, отправляется по SMTP, извлекается через POP3 и, после загрузки, остаётся на вашей машине.  Веб-почта.  Разновидность почты POP3. Например, с помощью приложения Outlook Express, вы входите в систему и скачиваете все новые письма в папку Входящие, находящуюся на вашем компьютере.  Разновидность почты IMAP – "истинной" веб-почты, которую вы можете просмотреть через вашу машину, но письма, при этом, остаются на удаленном сервере. Они могут быть организованы в папки, и т.д., но доступны для чтения только при онлайн подключении. | | | |
| Слайды 106 - 109 | Заголовки электронных писем  При рассказе об электронной почте, удобно сравнивать её с обычным письмом. Сообщение в электронной почте имеет заголовок (конверт), и основную часть (само письмо) с вложениями. Заголовок сообщения содержит важнейшую для следователей информацию, поскольку он содержит сведения об отправителе, получателе, IP-адресах, почтовых серверах, временных метках и т.д. Информация из заголовка используется для того, чтобы отследить отправителя сообщения, в случаях, когда это не очевидно, например, в случае требования выкупа, присланного по электронной почте. Полный или расширенный заголовок критически важен для отслеживания источника сообщения, и поэтому существенно, чтобы судьи оценили разницу между заголовком, видимым при доставке сообщения, и расширенным, который содержит полную информацию. Электронная почта является одним из самых распространенных приложений, с которыми будут сталкиваются судьи, и инструкторы должны постараться включить в курс обучения наиболее актуальную информацию о различных видах электронной почты. Необходимо рассказать о том, как правильно получать доказательства из самих сообщений, а также от Интернет-провайдеров, через которых эти сообщения проходят. Дополнительную информацию о почтовых службах, которая может быть использована обучающими инструкторами, можно найти на сайте  http://www.learnthenet.com/english/html/20how.htm | | | |
| Слайдs 112 to 159 | Часть четвёртая - Другие важные интернет приложения.  В этом разделе курса слушателям даётся обзор Интернет-приложений, которые не вошли в предыдущие разделы. Их необходимо представить, поскольку они будут встречаться в процессе обычной деятельности целевой аудитории. Эта информация будет способствовать достижению целей курса. Уровень детализации считается подходящим для необходимого уровня преподавания. Инструкторы не должны предоставлять слишком глубоких знаний, так как эти сведения будут включены в курс усовершенствования, который разрабатывается в настоящее время. | | | |
| Слайды 113 - 114 | Онлайн хранилища  «Облачные» вычисления  «Облачные» вычисления, это маркетинговый термин для технологий, которые предоставляют вычислительные ресурсы, программное обеспечение, доступ к данным, услуги хранения данных, и которые не требуют от конечного пользователя знания о физическом местоположении и конфигурации системы, предоставляющей услуги. Можно провести параллель между этой концепцией и электросетями, где конечные пользователи потребляют мощность не имея представления о компонентах устройств или инфраструктуры, необходимых для предоставления энергии. Термин «облачные вычисления» описывает новую модель потребления и поставки ИТ-услуг на основе интернет-протоколов, и, как правило, включает в себя предоставление динамически масштабируемых и часто виртуализированных ресурсов. Это является побочным продуктом Интернета и следствием простоты доступа к удаленным вычислительным узлам. Облачные услуги могут принимать форму веб-инструментов и приложений. Пользователи, получив доступ, могут использовать их через веб-браузер, как будто эти программы были локально установлены на их компьютерах. Поставщики облачных вычислений доставляют результаты работы приложений по Интернету, через веб-браузеры, настольные и мобильные приложения, в то время как программное обеспечение и данные для предприятий хранятся на удаленном сервере. В некоторых случаях, обычные приложения доставляются пользователю по технологии общего экрана, в то время как вычислительные ресурсы объединяются в удаленном центре обработки данных; в других случаях, целые бизнес-приложения программируются с использованием технических средств Интернета, таких как AjX. В основе облачных вычислений лежит более широкое представление об инфраструктуре и общих услугах. Этот тип среды для обработки данных позволяет предприятиям быстрее включать свои приложения и быстрее работать на них, имея повышенную управляемость этими техническими средствами, и сокращая расходы на их обслуживание. Предприятие быстрее оптимизирует IT-ресурсы (например, сервера, хранилища данных и конфигурацию сети), чтобы учесть непредсказуемые колебания спроса. Большинство инфраструктур облачных вычислений базируются на общих дата-центрах, и выглядят для потребителей вычислительных потребностей как единая точка доступа к необходимым ему услугам. Для удовлетворения некоторых запросов на особый уровень обслуживания могут потребоваться специальные коммерческие предложения, но более мелкие компании реже вступают в переговоры о конкретных условиях. Огромное влияние облачных вычислений на бизнес побудило федеральное правительство США рассмотреть «облака» в качестве средства для реорганизации своей IT-инфраструктуры, и снижения IT-бюджетов. (Источник www.wikipedia.com)  Вопросы, связанные с идентификацией и сбором данных из облака, и c правовыми последствиями таких действий, рассматриваются в другом месте этого курса. | | | |
| Слайды 115 и 116 | Инструктор может рассказать о распространенности хранения данных в сети, и в качестве примера привести количество поисковых запросов Гугл и увеличение их количества в течение определенного периода времени, что дает представление о том, что в таком хранении есть большой интерес. Необходимо познакомить слушателей с различными типами интернет-хранилищ, различая бесплатные и платные услуги. Должен быть четко представлен тот факт, что преступники могут использовать этот тип хранения. | | | |
| Слайды 117 и 118 | Для слушателей должны представлять интерес различные способы, которыми преступники используют Интернет услуги. Например, способ связанный с использованием тайников. Инструктор может объяснить эти способы простыми словами, дав понять, что этот метод общения может быть использован с минимальным риском перехвата. | | | |
| Слайды 119 и 120 | Одноранговая сетевая структура (англ. Peer to Peer, P2P)  Одноранговые сети уже на протяжении многих лет использовались для передачи между пользователями файлов с незаконной информацией, а также файлов, содержание которых защищено правом на интеллектуальную собственность. Одноранговая сеть равных клиентов были популярны среди преступных групп, занимающихся этой деятельностью. Первое поколение одноранговой архитектуры работало по принципу использования централизованного сервера, к которому люди подключались с тем, чтобы загрузить файлы. Это делало идентификацию и закрытие тех, кто предлагал незаконные услуги довольно простым делом. Второе поколение сетей одноранговых клиентов использует различные методы подключения к сети, от таких, которые содержат списки доступных файлов, чтобы сделать их поиск проще, до таких, которые действуют как суперузлы и идентифицируют, где, на каких ресурсах есть доступные файлы.  Судьи должны быть осведомлены об одноранговой (пиринговой) деятельности, так как это может относиться ко многим случаям, которые подлежат рассмотрению в уголовном и гражданском суде. Слушатели не обязаны иметь по этой теме глубокие знания. Инструкторы могут найти актуальную информацию и необходимые материалы для своих презентаций на таких сайтах, как http://ezinearticles.com/?How-Peer-to-Peer-(P2P)-Works&id=60126. | | | |
| Слайды 121 и 122 | Группы новостей  Принятый термин «группы новостей» вводит в заблуждение, поскольку эти группы предназначены, как правило, для размещения дискуссий. Хотя технически они и отличаются от других дискуссионных форумов, размещенных во Всемирной паутине, но функционируют они сходным образом. Новостные группы размещаются различными организациями, которые согласовали с другим сетевыми ресурсами, что они будут синхронизировать свою информацию на регулярной основе. Это позволяет пользователям отправлять сообщения лишь на один сервер, и оно становится видимым более широкой аудитории. | | | |
| Слайды 123 и 124 | Протокол передачи файлов (англ. File Transfer Protocol, FTP, «ЭфТиПи»)  FTP – это мощный протокол, который позволяет передавать файлы с одного компьютера на другой. Он работает на основе технологии клиент/сервер, при этом программа-клиент FTP, установленная на компьютере пользователя, позволяет ему взаимодействовать с сервером, и получать доступ к услугам и информации, расположенным на нём. Когда пользователь желает передать файл, то его FTP-клиент устанавливает TCP-соединение с целевым компьютером, с помощью которого могут быть переданы ID пользователя и пароль доступа. Пользователь может выбрать файлы и требуемое действие. После получения подтверждения запроса на передачу файлов, создается другое TCP-соединение для передачи самих данных. Почему судьи должны знать о существовании услуги FTP? Ответ заключается в том, что они могут столкнуться с тем, что преступники обмениваются файлами друг с другом, или, когда FTP используется в качестве метода передачи при работе по другим протоколам, таким как Internet Relay Chat (IRC). | | | |
| Слайды 125 и 126 | Internet Relay Chat (IRC) — протокол для обмена сообщениями в режиме реального времени.  Internet Relay Chat (IRC) это, в сущности, система телеконференций, хотя и несколько устаревшая, но все еще используемая преступниками для общения и обмена файлами. Он работает за счет последовательности серверов, соединённых друг с другом и обменивающихся сообщениями, которые размещаются в "каналах" – текстовых виртуальных конференц-залах. Темы для обсуждения перечислены в публичном пространстве, и пользователи, имеющие клиент IRC, могут подключаться к одному или нескольким каналам в любое время, чтобы принять участие в обсуждении с единомышленниками. IRC не самый удобный сервис в сети Интернет и в основном используется теми, кто имеет большой опыт работы и, потенциально, относится к пользователям старшего возраста. Это протокол, используемый преступниками, поэтому судьям и прокурорам требуется элементарное знакомство с его свойствами. | | | |
| Слайды 127 - 132 | Система мгновенных сообщений (англ. Instant messaging, IM, «АйЭм») и социальные сети  Система мгновенных сообщений и социальные сети выдвинулись в последние годы на передний план в качестве инструмента коммуникации, обеспечивающего мгновенный и удобный доступ к общению для пользователей во всем мире. Главными особенностями этих сайтов являются возможность создания личного профиля и распространение информации о себе, знакомства с новыми людьми. Можно обмениваться фотографиями, музыкой и видео. Размещение на сайте большого количества персональной информации может сделать его мишенью для преступников, например, тех, кто участвует в краже личных данных или тех, кто желает ухаживать за малолетним ребёнком с сексуальными намерениями. Дополнительную информацию, которая может помочь в разработке учебных материалов можно найти на сайте http://communication.howstuffworks.com/how-social-networks- work.htm.  Мгновенный обмен сообщениями является одной из форм чата в реальном времени между двумя или большим количеством лиц, использующим общие клиенты. Этот тип чата предполагает контакт между известными людьми, в отличие от других видов чата, которые допускают контакты между неизвестными лицами. Известно, что преступники используют мгновенный обмен сообщениями в качестве метода связи.  Инструктор может предоставить дополнительную информацию в виде статистических данных о росте числа пользователей, использующих социальные сети. В качестве примеров приводятся данные о росте числа пользователей конкретных сайтов и о глобальном воздействии социальных сетей.  Инструктор должен предоставить примеры типовых сведений о пользователях, которые доступны для следователей. Могут быть использованы некоторые примеры из презентации, хотя инструкторы должны попытаться найти примеры, приближенные к географическому положению слушателей. | | | |
| Слайды 133 - 136 | Онлайн-игры  Онлайн-игра – это игра, разворачивающаяся в той или иной форме компьютерной сети. Это почти всегда означает, Интернет или эквивалентную технологию, но игры всегда использовали современную им сетевую технологию; до Интернета использовались модемы, а до модемов использовались кабельные терминалы.  Развитие онлайн-игр отразило общее развитие компьютерных сетей: от небольших локальных сетей к Интернету, и рост доступа в сам Интернет. Онлайн-игры могут варьироваться от простых текстовых игр до игр, включающих сложную графику и виртуальные миры, населенные многими игроками одновременно.  Многие онлайн-игры имеют присоединённые интернет-сообщества, делая онлайн-игру формой социальной активности за пределами игры с одним игроком.    Инструктор должен стремиться привести примеры преступлений, связанных с играми. Они становятся все более распространенными, и слушателям было бы полезно рассмотреть правовые последствия игровой активности в их странах. | | | |
| Слайды 137 - 146 | Интернет анонимность и прослеживаемость  Интернет анонимность является важным предметом, который должен на базовом уровне обсуждаться в рамках этого курса. Эти термины будут встречаться судьям и прокурорам в их повседневной работе. Примеры анонимных услуг должны сопровождаться объяснением того, как они работают. Должна быть объяснена разница между анонимной и прослеживаемой передачей данных. Слайды, предусмотренные в презентации, могут помочь инструкторам в разработке собственных материалов. Инструктор должен привести примеры веб-анонимных услуг и анонимной электронной почты. | | | |
| Слайдs 147 to 159 | Часть пятая - Интернет преступления  Заканчивая основную часть занятия, инструктор должен стремиться показать способы использования технических средств, о которых шла речь выше, при совершении уголовных преступлений. Действительно, единственной страной в мире, которая собирает жалобы на Интернет-преступления, являются Соединенные Штаты. Статистические данные, предоставленные Центром Интернет-преступности, по крайней мере, дают некоторое представление о масштабах проблемы. Они могут быть использованы в курсе и должны систематически обновляться инструктором. | | | |
|  | ***Инвестиционные схемы***  Использование Интернета для запроса финансовой поддержки высокотехнологичных схем, таких как виртуальные торговые сайты, или поставщики новых услуг.  ***Схемы кредитных карт***  Использование незаконно полученных данных кредитной карты для покупки дорогостоящих товаров через Интернет.  ***Возможности для бизнеса / Схемы работы на дому***  Интернет используется для рекламы возможностей для бизнеса, в результате чего, потерпевший производит оплату информации до оказания услуги.  ***Махинации 419***  Западноафриканские мошенники. Изменились средства доставки запросов – теперь, это электронная почта, вместо традиционных запросов по почте или по факсу, в остальном ничего не переменилось. Преобладающий тип доступа к жертве – через спам.  ***Интернет-банкинг***  Просто копируют веб-сайт банка, немного изменяют веб-адрес, дают ссылки на легальные услуги банка и только одну или две ссылки на предложение инвестиций высокой доходности, которые требуют перечисление значительных сумм в обмен на включение в проект с действительно невероятными возможностями для инвестиций.  ***Стихийные бедствия / Благотворительность / Призывы***  В течение одного часа после Дальневосточного цунами, в Сети появились сайты, призывающие оказать помощь пострадавшим, многие из них (если не все в это время) были фиктивными.  ***Травы / Виагра***  В области альтернативных методов лечения онлайн, предлагаемых "клиентам" в виде спама, большинство продуктов не оказывают лечебного воздействия (если, вообще, доставляются). Некоторые из них просто откровенно опасны.  ***«Невесты из России»***  Брачные агентства в сети, предлагающие контакты с красивыми женщинами из Восточной Европы и дешевые туры в Россию, а также в прилегающие государства.  ***Выигрыш в лотерею***  Запрос на оплату за требование на лотерейные выигрыши или за оказание помощи для выигрыша (часто иностранные лотереи).  ***Фишинг***  Сообщения электронной почты под видом сообщения от хорошо известного источника (например, от банка или от Интернет-провайдера) с просьбой подтвердить личные данные.    Инструктор должен стремиться выявлять соответствующие случаи в регионе, в котором проводится занятие, и использовать их в качестве примеров. В конце занятия, инструктор должен поощрять участников поделиться своими знаниями и опытом по поводу интернет-преступлений. | | | |
|  | Практические занятия (проводятся при наличии необходимых условий).  В рамках этого занятия они не предусмотрены за отсутствием гарантий того, что во всех местах его проведения будут в наличии технические средства должного уровня и доступ в интернет, необходимый для их проведения.  На будущее инструктора могут добавочно ввести практические занятия в учебный план в том случае, если на месте их проведения будут соблюдены все необходимые технические условия. | | | |
|  | **Проверка знаний**  На этом занятии никакой дополнительной проверки в дополнение к вышеперечисленным требованиям в настоящее время не предусмотрено. Также, не требуется проводить никакого официального зачёта. | | | |
| Слайды 160 - 162 | Часть шестая - Подведение итогов занятия/выводы | | | |
|  | Инструктору необходимо подвести итоги / проверить знания слушателей, которые должны быть в состоянии:   * Объяснить, как развитие технических средств отражается на характере преступности * Перечислить составные части компьютерной системы * Определить/распознать различные типы устройств хранения данных. * Рассмотреть, как отразилось на работе органов уголовного правосудия увеличение в геометрической прогрессии ёмкости запоминающих устройств. * Определить/распознать различные компьютерные операционные системы. * Объяснить основные принципы работы интернет сетей. * Описать функции интернета. * Определить/распознать как минимум 5 основных интернет приложений (прикладных программ интернета). * Изложить историю развития интернета от его истоков и до наших дней. * Объяснить разницу между различными интернет приложениями. * Рассказать, как киберпреступники используют различные интернет приложения в своих целях.   Задачи занятия могут быть достигнуты путём проведения коллективного обсуждения изучаемого материала, опроса слушателей, заполнения контрольных вопросников или же с помощью других общепризнанных методов.  Это занятие задумывалось таким образом, чтобы задать ориентировочные характер и уровень технической осведомлённости, требуемые от судей и прокуроров для эффективного исполнения ими своих профессиональных обязанностей. Его авторы не претендуют на исчерпывающий анализ изучаемого предмета и там, где это им кажется важным, дают ссылки на дополнительные источники информации.  Рекомендуется, чтобы разработчики практических занятий при их подготовке использовали самые современные сведения о последних достижениях науки и техники постольку, поскольку таковые влияют на поведение преступного мира, а также отражаются на правовых нормах, на положениях процессуального права и порядке доказывания вины в рамках той юрисдикции, при которой должны проводиться практические занятия (тренинги). Существуют такие технологические прорывы, которые сказываются на работе всей системы уголовного правосудия. Здесь в качестве примера можно привести появление твёрдотельных устройств хранения данных или же методики проектирования интернет систем по принципу «Веб 2.0.» (Web 2.0.). Таким образом, будет необходимо включить в программы подготовки немало важных тем по мере возрастания их значимости.  Как и любая другая программа, учебный план практических занятий с работниками суда и прокуратуры должен ставить перед ними ясные и понятные задачи, отвечающие следующим требованиям: таковые должны быть конкретными, поддающимися измерению, достижимыми и важными для учащихся. Кроме того, время, выделенное для их решения, должно быть ограниченным. Выполнение этих требований способствует достижению конечной цели. При формулировке задач старайтесь избегать таких слов как «понять» или «изучить», так как нет применительно к ним соответствующей шкалы измерения. Например, как вы оцените, насколько достигнута цель «изучения» рассматриваемого на занятиях предмета? Следовательно, лучше использовать такие поддающиеся измерению понятия как «перечислите» или же «определите». Практические объяснения того, как надо ставить задачи, отвечающие стандарту «СМАРТ», даются по адресу:  [www.sheffield.ac.uk/.../Guide%20to%20setting%20objectives.doc](http://www.sheffield.ac.uk/.../Guide%20to%20setting%20objectives.doc)  Подача учебного материала в форме разбора конкретных ситуаций рассматривается как более подходящая для подобного рода практических занятий (тренингов) со взрослой аудиторией нежели, чем чисто дидактический, лекционный стиль обучения.  Ключевая роль организатора практических занятий (тренингов) заключается в том, чтобы обеспечить достижение общей задачи, преследуемой каждым учебным мероприятием, при одновременном осуществлении конкретных поставленных перед ним задач. В этой главе содержится некоторая информация, способствующая этому процессу. | | | |
| **Дополнительные источники**  Ниже приведен список документов, опубликованных различными организациями из ряда стран. Они могут пригодиться инструкторам при подготовке учебных материалов для этого курса. | | | | |
| **Организвция** | | **Страна происхождения** | **Документы** | |
| Международная организация по стандартизации (ИСО) и Международная электротехническая комиссия (МЭК) | | международная организация | ИСО/МЭК (ISO/IEC) 17025: 2005 Общие требования к компетентности испытательных и калибровочных лабораторий (18.10 Класс электронных доказательств, 01 обеспечение сохранности данных, .02 Анализ данных)  ИСО/МЭК (ISO / IEC CD) 27037 Информационные технологии - Методы обеспечения безопасности - Руководящие принципы при выявлении, сборе, получении и сохранении целостности электронных доказательств  ИСО/МЕК (ISO/IEC 9797-2: 2011) Информационные технологии - Методы обеспечения безопасности - Коды аутентификации сообщений (MAC) - Часть 2: Механизмы, использующие специальные хеш-функции | |
| Европейская сеть институтов судебной экспертизы (англ. сокращение ENFSI) | | ЕС | Руководство по внедрению стандарта ИСО/МЕК (ISO/IEC) 17020 в области производства следственных действий на месте преступления (код документа - EA-5/03) | |
| Ассоциация начальников управлений полиции Англии, Уэльса и Северной Ирландии,  Центральный отдел полиции по раскрытию компьютерных преступлений.  Полиция Уэльса  «Уэльс против электронной преступности» - партнёрское объединение организаций и учреждений по информированию бизнеса для защиты от киберпреступности | | Англия, Уэльс и Северная Ирландия  Уэльс | Рекомендуемые правила работы с электронными доказательствами, хранящимися в компьютере.  Руководство по оперативному реагированию для следователей: неотложные меры, принимаемые при расследовании инцидентов, связанных с использованием компьютерной техники. | |
| Ассоциация начальников управлений полиции Англии, Уэльса и Северной Ирландии (англ. сокращение – ACPO) | | Англия, Уэльс и Северная Ирландия | Советы и практическое руководство для начальников отделов по борьбе с преступлениями в сфере высоких технологий | |
| Ассоциация начальников управлений полиции Англии, Уэльса и Северной Ирландии  (англ. сокращение – ACPO) | | Англия, Уэльс и Северная Ирландия | Советы и практическое руководство для сотрудников, уполномоченных вести расследование компьютерного преступления. | |
| Британский институт стандартов | | Соединенное Королевство Великобритании и Северной Ирландии | Стандарт ASTM E1732 – 11: стандарт по терминологии в области судебной экспертизы.  Стандарт ASTM E1492 – 11: стандартный порядок действий при приёмке, регистрации, хранении и извлечении доказательств в лаборатории судебной экспертизы. | |
| Служба аккредитации Соединенного королевства (англ. сокращение – UKAS) | | Соединенное Королевство Великобритании и Северной Ирландии | Публикации, касающиеся аккредитации органов по сертификации. | |
| Регулятор судебной экспертизы (англ. сокращение - FSR) | | Соединенное Королевство Великобритании и Северной Ирландии  (Головной офис) | Нормы и правила, регламентирующие работу поставщиков услуг в области научно-исследовательской судебной экспертизы, и практикующих специалистов в системе уголовного правосудия  Протоколы группа специалистов в области судебной компьютерно-технической экспертизы | |
| Инженерно-технологическое общество (англ. сокращение - IET) | | Международная организация, объединяющая общество инженеров- электромехаников и общество объединённых инженеров | Разработка стандартов в зарождающихся и традиционных областях развития науки и техники | |
| Европейская группа по распространению знаний и практических навыков по борьбе с киберпреступностью (англ. сокращение - ECTEG) | | ЕС («Европол») | Протоколы заседаний группы | |
| Британское компьютерное общество, группа специалистов в области судебной компьютерно-технической экспертизы | | Соединенное Королевство Великобритании и Северной Ирландии | Программные документы | |
| Департамент (министерство) юстиции США | | США | «Судебная экспертиза электронных доказательств» - руководство для правоохранительных органов | |
| ФБР / Научная группа по электронным доказательствам | | США | Электронные доказательства: стандарты и принципы | |
| Департамент (министерство) торговли США | | США | Руководство по электронной криминалистике мобильной связи | |
| Международная организация по электронным доказательствам | | международная организация | Рекомендации по использованию электронных доказательств | |
| Совет Европы | | EC | Законодательные и процессуальные требования, предъявляемые странам, желающим ратифицировать Конвенцию о компьютерных преступлениях | |
| «Интерпол» | | международная организация | Учебник по киберпреступности | |
| «Умения, знания и навыки для юстиции» - организация по повышению квалификации работников правосудия | | Соединенное Королевство Великобритании и Северной Ирландии | Национальные профессиональные стандарты в сфере борьбы с электронной преступностью, устанавливающие требуемые уровни знаний, умений и навыков в области обращения с электронными доказательствами, компьютерной криминалистики и расследования киберпреступлений | |
| Спец. службы США, Департамент (министерство) внутренней безопасности Соединённых Штатов Америки | | США | «Методические рекомендации по производству выемки электронных доказательств» - карманный справочник для групп быстрого реагирования | |
| Европейская комиссия | | EС | «Методические рекомендации по производству выемки электронных доказательств» - справочник, подготовленный в рамках проекта ЕС «ОИСИН» 2002/OIS/014 | |
| Национальный институт юстиции  (Национальный институт стандартов в технологии) | | США | «Следственные действия на месте совершения электронного преступления» - руководство для групп быстрого реагирования (2-е издание) | |

|  |  |  |
| --- | --- | --- |
| Занятие 1.3.1 - Обзор проделанной работы | | **Продолжительность: 30 минут** |
| **Перечень материалов, необходимых для проведения занятия:**   * ноутбук или ПК с операционной системой Windows 7 и с загруженным офисным пакетом приложений MS Office 2010; * проектор с экраном; * презентация «ПауерПойнт»; | | |
| **Цель** этого занятия заключается в том, чтобы проанализировать проделанную за предыдущие дни работу, получить отклики аудитории и убедиться в том, что поставленные на этом занятии задачи были решены. | | |
| **Задачи:**  По окончании занятия слушатели должны быть в состоянии:   * определить, насколько хорошо они усвоили учебный материал, преподнесённый им в предыдущие дни; * выявить те области, к которым они должны вернуться ещё раз, чтобы довести свои знания до необходимого уровня. | | |
| **Введение**  Это занятие было подготовлено таким образом, чтобы позволить слушателям проверить, насколько хорошо они поняли материал, преподнесённый им в предыдущие дни, и оценить, насколько каждый из них готов самостоятельно ответить на все вопросы, вытекающие из задач пройденных занятий. Кроме того, для инструктора представляется возможность проконтролировать уровень знаний слушателей и выявить те области, которые нуждаются в углублённой проработке. | | |
| **Слайды №** | **Содержание:** | |
| Слайды  1 - 12 | **Презентация «ПауерПойт»** (или же подготовленная с помощью другой программы)  Слайды этой презентации составлены с таким расчётом, чтобы помочь инструктору и слушателям провести обзор работы, проделанной за предыдущие дни. Со своей стороны, инструктор должен подвести её промежуточный итог, используя в качестве критерия оценки пункты учебной программы и задачи предыдущих занятий. | |
|  | **Практические занятия** (проводятся при наличии необходимых условий)  Не предусмотрено. | |
|  | **Проверка знаний**  Тренер должен проверить знания слушателей, задавая им конкретные вопросы по каждой из пройденных на занятиях тем. | |
|  | **Подведение итогов занятия/выводы**  Всё занятие построено таким образом, чтобы слушатели смогли проанализировать на нём работу, проделанную за предыдущие дни. Соответственно, никакого отдельного подведения итогов по каждой из пройденных тем проводить не требуется. | |

|  |  |  |
| --- | --- | --- |
| Занятие 1.2.3 Киберпреступление как уголовно наказуемое деяние в соответствии с положениями национального законода-тельства | | **Продолжительность: 90 минут** |
| **Перечень материалов, необходимых для проведения занятия:**   * Ноутбук или ПК с операционной системой Windows 7 и с загруженным офисным пакетом приложений MS Office 2010; * проектор с экраном; * презентация «ПауерПойнт»; | | |
| **Цель:**  Цель этого занятия заключается в том, чтобы ввести слушателей в следующую тему: национальные нормативные акты в сфере противодействия сетевой компьютерной преступности (киберпреступности), перечисляемые в них виды уголовно наказуемых правонарушений и соответствующие положения международного законодательства, которые могут быть применены на национальном уровне. | | |
| **Задачи:**  По окончании занятия слушатели должны быть в состоянии:   * выделить национальные нормативные акты в сфере противодействия киберпреступности; * выделить перечисляемые в них виды уголовно наказуемых правонарушений; * определить, в чём заключается специфика национальных нормативных актов в сфере противодействия киберпреступности по сравнению с положениями международного законодательства, регламентирующего эту область. | | |
| **Введение**  Настоящее занятие направлено на то, чтобы предоставить работникам суда и прокуратуры всю необходимую информацию по сути вопроса и его предыстории. Таким образом, они смогут более эффективно использовать соответствующие положения национального законодательства на этапах поддержки обвинения и вынесения судебных решений по делам о киберпреступности. По окончании занятия слушатели будут в состоянии выделить те нормы национального права, которые относятся к:   * преступлениям против конфиденциальности,целостности и доступности компьютерных данных и систем; * преступлениям, совершенным с использованием компьютерных данных и систем; * правонарушениям, связанным с содержанием данных.   На занятии приводится пример того, как положения «Будапештской конвенции» были внедрены в национальное законодательство одной страны – в данном случае, Португалии. Инструкторам надо будет заменить представленные здесь сведения о Португалии соответствующей информацией о своей стране. | | |
| **Слайды №** | **Содержание:** | |
| Слайды 1 - 66 | Презентация «ПауерПойнт» (или же подготовленная с помощью другой программы)  Содержание слайдов в этом разделе приводится лишь в качестве примера того, о чём может идти в данном случае речь на каждом их местных практикумов (тренингов).  В идеальном варианте на занятии, посвящённом национальному материальному праву, должны упоминаться международные юридические документы, подписанные или же ратифицированные тем или иным государством, и результаты переноса их норм во внутригосударственное право этой страны.  Кроме того, необходимо дать описание признаков различных видов преступлений в сфере компьютерной информации (киберпреступлений) в соответствии с национальным законодательством, и ближе к концу занятия, если только это представляется возможным, выделить специфические особенности, присущие национальным нормам материального права. | |
| Слайд 2 | План занятия  Занятие разбито на четыре части:   1. в первой части внимание слушателей будет сосредоточено на материальных нормах уголовного права в том виде, в котором они изложены в будапештской Конвенции о компьютерных преступлениях; 2. национальное материальное уголовное право является предметом второй части занятия; 3. в третьей части проанализированы конкретные случаи из практики; 4. и наконец, в четвёртой части, проводится подведение итогов занятия. | |
| Слайд 3 | Инструктор должен раскрыть следующие темы:   * материальные нормы уголовного права, связанные с киберпреступлениями, и некоторые из ключевых признаков, используемых для того, чтобы квалифицировать таковые, исходя из положений «Будапештской конвенции» * материальные нормы уголовного права, связанные с киберпреступлениями, и некоторые из ключевых признаков, используемых для того, чтобы квалифицировать таковые, исходя их положений действующего национального законодательства; * Необходимость и выгодность гармонизации между национальными законодательствами и международными документами на основе, прежде всего, «Будапештской конвенции». | |
| Слайд 4 | * Обсуждение представленного на рассмотрение слушателей конкретного случая из судебной практики и определение норм материального права, которые можно к нему применить. | |
| Слайды 5 и 6 | Часть первая – будапештская Конвенция о компьютерных преступлениях – материальное уголовное право  Будучи первым международным договором о сетевой компьютерной преступности (киберпреступности), «Будапештская конвенция» направлена на содействие развитию международного сотрудничества в области расследования преступлений в сфере компьютерной информации.  Основной её целью является обеспечение гармонизации норм материального права сторон конвенции, что способствовало бы укреплению взаимодействия между ними. Соответственно, в «Будапештской конвенции» даются определения:   * преступлений против конфиденциальности, целостности и доступности компьютерных данных и систем; * преступлений, совершенных с использованием компьютерных средств. | |
| Слайд 7 | В этом разделе рассматривается один из наиболее распространенных видов сетевых компьютерных правонарушений: преступлений против конфиденциальности, целостности и доступности компьютерных данных и систем. В данном случае, речь может идти о киберпреступности в узком понимании этого слова. | |
| Слайды 8 и 9 | Преступление в виде противозаконного (несанкционированного) доступа совершается теми, кто умышленно осуществляет доступ к компьютерной системе в целом или к любой ее части без права на то. Оно описывается в статье 2 «Будапештской конвенции».  Данный вид противоправной деятельности очень часто определяется как *хакерство* в отношении компьютерных систем и является одним из наиболее распространённых компьютерных преступлений. Тем не менее, наряду с *хакерством* существует и ряд других деяний, которые могут подпадать под квалификацию противозаконного доступа. Действительно, термин *хакерство* обычно употребляется для обозначения действий по противозаконному доступу к компьютерной системе с использованием компьютерных технологий. Но понятие противозаконного доступа также включает в себя и несанкционированное проникновение в систему вне зависимости от типа используемых технических средств или даже вне зависимости от того, применялись таковые или нет. В качестве примера такого преступного деяния можно привести противозаконное получение преступником пароля. При его совершении имеет место покушение на конфиденциальность данных, хранящихся в компьютерной системе. | |
| Слайды 10 - 11 | В статье 3 «Будапештской конвенции» речь идёт другом виде умышленного компьютерного правонарушения, а именно, о неправомерном (несанкционированном) перехвате. Он совершается тем, кто – не имея на то права – перехватывает не предназначенную для общего пользования передачу входящих, исходящих и межсистемных компьютерных данных, используя для этого технические средства.  Настоящее положение «Будапештской конвенции» защищает неприкосновенность не предназначенной для общего пользования передачи цифровых данных, вводя уголовную ответственность за их неправомерный перехват.  Сегодня передача входящих, исходящих, меж и внутрисистемных цифровых данных стала неотъемлемой частью нашей повседневной жизни в информационном пространстве.  С технической точки зрения перехват осуществляется очень легко при отсутствии должной защиты сети связи и передаваемых по ней данных. Благодаря их перехвату можно выяснить, скажем, какие сайты посетило то или иное лицо, а также какие электронные письма оно получило или отправило.  Таким образом, преступление, квалифицируемое как неправомерный перехват, выявляет уязвимость коммуникационных технологий, призванных обеспечивать конфиденциальность передачи цифровых данных, не предназначенных для общего пользования. | |
| Слайды 12 и 13 | Лица, которые – действуя преднамеренно и не имея на то права – вызывают повреждение, удаление, ухудшение качества (порчу), изменение или блокирование компьютерных данных, совершают преступление, квалифицируемое как воздействие на данные (другие определения этого вида компьютерного преступления: «нарушение целостности данных», «вмешательство в базу данных» - примечание переводчика) и описанное в статье 4 «Будапештской конвенции».  Настоящее положение защищает целостность данных от несанкционированного воздействия на них. Владелец данных вправе хранить их в первоначальном виде точно так же, как в повседневной жизни собственник того или иного имущества вправе сохранять его в целости и сохранности и защищать от постороннего посягательства. В соответствии с правовыми нормами ряда стан, классические правила возмещения причинённого ущерба распространяются и на нарушение целостности данных; в других государствах ущерб, нанесённый компьютерным данным или же причинённый им в результате нарушения их целостности, законодательно выделен отдельно.  Существование этого преступления ярко свидетельствует о возрастающей важности обмена компьютерными данными в современной жизни. Цифровые данные очень уязвимы и легко поддаются уничтожению (удалению, стиранию) или же изменению (манипулированию). Настоящая уголовно-правовая норма призвана защитить их целостность и доступность.  Одним из наиболее распространённых случаев воздействия на базы данных является результат «работы» компьютерных вирусов, самовольно и противоправно проникающих в компьютер пострадавшего лица и уничтожающих записанные на нём данные. | |
| Слайды 14 и 15 | В соответствии со статьей 5 «Будапештской конвенции», воздействие на функционирование компьютерной системы (другое определение этого вида компьютерного преступления: «вмешательство в работу автоматизированных/компьютерных систем» - примечание переводчика) заключается в создании препятствий работе компьютерных систем (при этом, в «Будапештской конвенции» имеются в виду серьёзные препятствия - на незначительные она не распространяется) путём ввода, передачи, повреждения, удаления (стирания), ухудшения качества (порчи), изменения или уничтожения компьютерных данных, если таковые действия совершаются намеренно и несанкционированно. Как правило, последний аспект выводит из сферы действия этой статьи, скажем, тестирование защищённости сети её системным администратором. Эта квалификация охватывает широкий круг деяний, которые могут препятствовать нормальной работе сети на должном уровне. Действительно, в «Будапештской конвенции» признаётся значительная роль, которую играют в нашей повседневной жизни коммуникационные системы и компьютерные технологии. Доступность обрабатываемой ими информации крайне важна для обеспечения нормальной жизнедеятельности в общественной, экономической и социальной сферах. Но этот вид преступлений распространяется не только на широкомасштабные деяния по вмешательству в работу автоматизированных/компьютерных систем, типа атак на отказ в обслуживании. Даже незначительные правонарушения в отношении отдельного компьютера могут квалифицироваться как «воздействие на функционирование компьютерной системы». В качестве примера можно привести *«бомбардировку электронной почтой»* того или иного электронного адреса. В жизни мы всегда имеем дело с воздействием на функционирование компьютерной системы (вмешательством в её работу) в тех случаях, когда преступник перегружает её большим количеством запросов, нежели чем она может технически обработать.  Статья 5 «Будапештской конвенции», квалифицирующая это компьютерное преступление, защищает доступ к сетям связи, системных операторов и пользователей. | |
| Слайды 16 - 19 | Одной из наиболее сложных с юридической точки зрения является статья 6 «Будапештской конвенции», где речь идёт о «противозаконном использовании устройств».  Как и в случае с другими вышеописанными преступлениями, деятельность правонарушителя в данном случае должна быть преднамеренной и несанкционированной. Под действие этой нормы подпадает широкий круг деяний, связанных с противозаконным использованием компьютерных устройств/программ/данных.  Речь здесь идёт о весьма «инновационном» преступлении, которое не фигурировало в Рекомендации 1989 года. Описывающая его признаки статья «Будапештской конвенции» также весьма новаторская: перечисляемые в ней деяния ранее не квалифицировались как преступления в соответствии с положениями национальных законодательств многих стран.  Главным образом, этой нормой запрещается производство, продажа, приобретение для использования, импорт, оптовая продажа или иные формы предоставления в пользование перечисленных в конвенции устройств (в том числе, компьютерных программ, разработанных или адаптированных, прежде всего, с целью совершения преступлений).  Равно, ею вводится уголовная ответственность за торговлю компьютерными паролями, кодами доступа или иными аналогичными данными, с помощью которых может быть получен доступ к компьютерной системе в целом или к любой ее части.  Этим положением «Будапештской конвенции» признаётся необходимость преследовать по уголовной линии процветающий, доходный и разрастающийся «вторичный рынок» компьютерных средств, делающих возможным совершение преступлений. На нём хакеры торгуют в сети своим «рабочим инструментом» и наборами самодельных компьютерных вирусов. Здесь же предлагается обширный ассортимент паролей, выкраденных с помощью вирусов «троянов», и других программ. Это значит, что отныне хакерское проникновение в компьютерные системы более не остаётся уделом лишь программистов высокой квалификации. Отныне любой «обычный» преступник может легко купить необходимый ему инструментарий или же просто выкраденные пароли. Доходит до того, что преступные торговцы предлагают покупателям также и «послепродажное обслуживание» с установкой на их компьютеры программ, используемых для совершения преступлений.  Одним из наиболее спорных положений статьи шестой является пункт 1(б), которым вводится уголовная ответственность за преднамеренное и несанкционированное обладание одним из вышеперечисленных устройств/программ/кодов с намерением использовать его для совершения каких - либо правонарушений, предусмотренных статьями 2 – 5 «Будапештской конвенции» (несанкционированный доступ, неправомерный перехват, вмешательство в базу данных и в работу компьютерных систем).  Этот пункт подобен тому, что в законодательствах некоторых стран называется «превентивной нормой», которой применительно к данному случаю сразу же и отдельно вводится уголовная ответственность. | |
| Слайд 20 | Компьютерное правонарушение это преступление, совершенное с применением компьютерной системы. Оно является новой разновидностью традиционных преступных деяний, но совершено может быть лишь в киберсреде. Вне этого виртуального мира ему нет места. | |
| Слайд 21 | Подлог с использованием компьютерных технологий, описанный в статье 7 «Будапештской конвенции», является особой разновидностью подлога. В большинстве стран подлог представляет собой обычное уголовное правонарушение. В таком случае объект подлога материален и осязаем. При введении уголовной ответственности за компьютерный подлог или же подлог компьютерных данных такие материальные объекты отсутствуют. Вот почему в «будапештскую конвенцию» была введена седьмая статья.  Иными словами, конвенция направлена на введение вида правонарушения аналогичного традиционному подлогу документов (материальных и осязаемых), в котором объектом преступления становятся компьютерные данные. Это преступное деяние совершается теми, кто вводит, изменяет, стирает или блокирует компьютерные данные, нарушая их подлинность, с тем намерением, чтобы они рассматривались или использовались с юридической точки зрения в качестве подлинных.  Естественно, все вышеперечисленные действия совершаются умышленно и несанкционированно. | |
| Слайд 22 | Мошенничество с использованием компьютерных технологий, описываемое в статье 8 «Будапештской конвенции», является тем видом преступления, который, с догматической точки зрения, трудно отличить от обычного мошенничества, как уголовного правонарушения. Тем не менее, в действительности речь идёт о новой, самостоятельной разновидности этого преступления, которая может совершаться лишь в киберсреде.  В соответствии с законами большинства стран, традиционное мошенничество является уголовно наказуемым преступлением. Но, как правило, они не могут быть применены в ситуациях, возникающих в киберпространстве. Мошенничество предполагает наличие обмана или же ошибки, умышленно совершенных конкретным лицом. Но в большинстве случаев в компьютерном мошенничестве отсутствует прямое вмешательство конкретного лица, так как таковое мошенничество является лишь результатом манипуляции с компьютерной системой. Вот почему в описании признаков такого вида преступления как компьютерное мошенничество вмешательство конкретного лица, выступающего в качестве его автора, заменено на понятие «незаконной манипуляции данными», совершаемой с намерением незаконного извлечения экономической выгоды. Таким образом, нет больше необходимости огорчать постороннее третье лицо, чье наличие выступало бы в качестве признака мошенничества. | |
| Слайд 23 | Правонарушения, связанные с содержанием данных, относятся к тому разряду преступлений, совершение которых облегчается благодаря использованию компьютеров и сетей. Этого рода правонарушения могут совершаться с использованием и других средств, но компьютерные технологии облегчают их осуществление. | |
| Слайды 24 - 26 | В статье 9 «Будапештской конвенции» содержится одна из основных новаторских норм этого договора: ею вводится уголовная ответственность за ряд деяний, связанных с детской порнографией и совершаемых с применением компьютерных систем, за которые ранее таковая ответственность предусмотрена не была.  С появлением интернета торговля детской порнографической продукцией возросла в гигантских масштабах. Информационно-коммуникационные сети очень удобны для тех, кто ищет «контент» подобного рода. Кроме того, в интернете пользователи могут сохранять анонимность при получении доступа к материалам со сценами насилия над детьми.  Что касается правонарушений, связанных с детской порнографией, то у этой темы есть один аспект, который следует обсудить особо, так как он широко затрагивается в конвенции. Речь идёт об уголовной ответственности просто за хранение материалов с детской порнографией. Пунктом 1 статьи 9 конвенции квалифицируется как уголовно наказуемое деяние факт простого хранения такого рода продукции в своей компьютерной системе, а также её приобретение сугубо для личного пользования. Такой подход является общепринятым и на других международных *форумах,* на которых эта тема рассматривалась.  Другим предметом обсуждения является и введение уголовной ответственности за продукцию со «псевдоизображениями». Иными словами, положения «Будапештской конвенции» распространяются не только на материалы, на которых фигурирует реальный ребёнок, сфотографированный в момент совершения действий сексуального характера, но также и на искусственно созданные изображения детей в подобных ситуациях. Здесь в качестве примера можно привести изображения детей, полностью созданные с помощью компьютерной графики (скажем, коллаж детской головы на взрослом теле, совершающем действия сексуального характера), или же изображения установлено взрослых лиц, играющих роль детей или же переодетых под них.  Введение уголовной ответственности просто за хранение материалов с детской порнографией значительно облегчает уголовное расследование дел, относящихся к этой категории. Действительно, в соответствии с этим положением, любое лицо, хранящее у себя подобного рода материалы, подлежит преследованию в уголовном порядке, и нет более необходимости доказывать наличие у него особого умысла использовать их определённым образом (скажем, с целью продажи) или же устанавливать факт участия такового лица в их изготовлении. Это также значит, что лицо, подозреваемое в совершении действий сексуального характера в отношении несовершеннолетних (педофилии), может быть подвергнуто наказанию без предъявления каких бы то ни было доказательств того, что оно совершило их, испытывая острое влечение к ребёнку. И, конечно же, полиция может проводить следственные действия в отношении лиц, подозреваемых в распространении детской порнографии (даже если у них таковая просто хранилась), а судебные органы привлекать их к суду и выносить соответствующие судебные решения вне зависимости от того, есть ли доказательства наличия факта продажи этих материалов или нет.  С этой точки зрения представляется необходимым также рассмотреть позицию, занятую по данному вопросу Европейским Союзом. Начиная с принятия Советом министров ЕС соответствующего решения от 29 марта 2000 года, Европейский Союз постановил ввести уголовную ответственность за простое хранение материалов с детской порнографией. Недавно Директивой 2011/92/EU Европейского парламента и Совета Евросоюза от 13 декабря 2011 г. «О борьбе с сексуальным насилием в отношении детей и с их сексуальной эксплуатацией», заменившей рамочное решение 2004/68/JHA Совета министров ЕС, было решено, что государства – члены Евросоюза должны ввести уголовную ответственность, в частности, за приобретение или же хранение детской порнографии (статья 5, пункт 2). Тем не менее, в этом же документе оставляется на усмотрение государств – членов ЕС принятие решения касательно того, стоит ли вводить уголовную ответственность применительно к случаям, когда такого рода порнографические материалы хранятся их производителями сугубо в целях своего личного пользования (постольку, поскольку ни один из этих материалов не использовался в целях его продуцирования, и при условии отсутствия опасности распространения таковых материалов).  Этот выбор Европейского Союза полностью соответствует положениям статьи 9 «Будапештской конвенции», которой вводится уголовная ответственность за производство, предложение или же предоставление в пользование, распространение или передачу, приобретение или же простое хранение детской порнографии, находящейся в компьютерной системе или же на компьютерных носителях данных. Тем не менее, введение в текст документа пунктов о «приобретении» и о «хранении» вышеуказанных материалов оставляют за сторонами конвенции право на оговорки.  Кроме того, позиция Европейского союза по этому вопросу была подкреплена положениями конвенции Совета Европы «О защите детей от сексуальной эксплуатации и сексуальных злоупотреблений» (CETS N 201), открытой для подписания в 2007 году. Цель этого международного документа заключается в гармонизации норм уголовного права сторон конвенции, направленной на защиту детей от сексуальной эксплуатации. В соответствии со статьей 20 вышеуказанной конвенции, следует ввести уголовную ответственность, в частности, за *«приобретение детской порнографии для личного пользования или же для другого лица»,* а также за «*хранение детской порнографии*». | |
| Слайды 27 - 28 | Статья 10 «Будапештской конвенции» касается вопросов нарушения авторских прав. Следует отметить, что ею не вводится никаких концептуально новых норм по данному предмету. Скорее, в конвенции просто подчёркивается необходимость того, чтобы ранее существовавшие нормы, регламентирующие авторские права в реальной жизни, были перенесены в сетевое пространство и применялись бы там. Иными словами: то, что запрещено в реальной жизни, должно быть запрещено и в сети. Нарушение авторских прав, совершаемое в сети или же с использованием компьютерной системы, должно подвергаться такому же наказанию, как и в материальном мире. На этом основании в «Будапештской конвенции» содержатся ссылки на уже существующие международные договора и соглашения по данному вопросу. (Парижский акт от 24 июля 1971 г., Бернскую конвенцию и на договора ВОИС). | |
| Слайд 29 | На этом этапе следует рассмотреть две последние статьи «Будапештской конвенции», отсылающие нас к материальному уголовному праву. В них речь идёт, с одной стороны, о наказаниях за пособничество и подстрекательство и, с другой стороны, об уголовной ответственности юридических лиц.  В статье 11 «Будапештской конвенции» описываются деяния, заключающиеся в оказании пособничества и в подстрекательстве, которые должны быть предусмотрены во внутригосударственных законодательствах всех государств – сторон настоящей конвенции. Тем не менее, следует признать, что компьютерные интернет преступления зачастую совершаются при участии многих сторон с размытыми границами степени ответственности каждой из них, что потенциально затрудняет вынесение обвинения. | |
| Слайд 30 | И наконец, в статье 12 конвенции содержится требование того, чтобы все стороны ввели уголовную ответственность за деяния, совершаемые юридическими лицами. В Европейском Союзе введение уголовной ответственности за деяния, совершаемые юридическими лицами, является серьезным предметом обсуждения, вызывающим немало споров. Поэтому он также находится в центре внимания Совета Европы.  С точки зрения Европейского Союза и Совета Европы, компании и другие юридические лица несут разного рода ответственность (уголовную и иную) за преступные деяния, совершаемые их представителями, действующими от их имени и представляющими их интересы. Кроме того, конвенция постановляет, что ответственность юридического лица наступает также и в случае недосмотра или же недостаточного контроля со стороны компании или же иного юридического лица за своим законным представителем.  Некоторые европейские страны предпочитают использовать нормы гражданского, а не уголовного права при регламентации ответственности юридических лиц. | |
| Слайд 32 | Часть вторая - Национальное материальное уголовное право | |
| Слайды 33 - 43 | Инструкторам надо поместить здесь ссылки на нормы национального права. | |
| Слайд 44 | Чать третья – анализ конкретных случаев из практики | |
| Слайд 45 | 1. **Случай 1**  * **Изложение фактов / ситуации**   Бобби является сотрудником полиции. Как-то вечером, будучи на дежурстве, он замечает автомобиль марки «Мерседес», припаркованный рядом с его домом. Он не знает, чей это автомобиль, но подозревает, что он принадлежит начальнику его жены. Бобби звонит на свой участок и просит операционистку Мэри заглянуть в базу данных и сообщить ему, кому принадлежит замеченный им «Мерседес», сказав, что он только что проехал на красный свет. Мэри подтверждает, что автомобиль действительно принадлежит начальнику его жены.  *Совершил ли Бобби уголовно наказуемое правонарушение?*   * **Рассматриваемые темы:**   *Получил ли Бобби доступ к компьютерной системе?*  *Был ли этот доступ противозаконным (несанкционированным)?*   * **Вопросы для обсуждения:**   Непосредственный доступ к компьютеру имела Мэри, а не Бобби. У неё есть разрешение (санкция) на доступ к данным в компьютере. Она не виновна. Именно Бобби, действуя через невиновное лицо, получил доступ к данным, солгав Мэри (один из примеров использования приёмов социотехники). Значит ли это, что доступ был санкционированным?  У обоих, и у Бобби, и у Мэри, есть допуск – право доступа к компьютерной базе данных полиции. Но этот допуск жёстко обусловлен тем, что запрос должен быть связан с выполнением профессиональных обязанностей сотрудников полиции. Совершается ли правонарушение в том случае, когда доступ к информации происходит с превышением полномочий и вышеуказанное условие не соблюдается?  А что если бы Бобби сам находился в это время на участке и мог бы, стоя у Мэри за спиной, следить за тем, как она на вполне законных основаниях делает запрос о владельце «Мерседеса»?  Таким образом, Бобби мог бы получить доступ к интересующим его компьютерным данным (параллельно возникает вопрос о «преднамеренности» его действий - «умысле»). В этом случае Бобби, конечно же, сам за компьютером не сидел, но информацию он всё же получил, не имея на то права (хотя при подобных обстоятельствах это было бы очень трудно доказать).  Эта конкретная ситуация была сконструирована таким образом, чтобы заставить слушателей задуматься над вопросом законности и противозаконности (несанкционированности) доступа к компьютерным данным.  Можно также предложить слушателям подумать над тем, изменилось бы с юридической точки зрения положение Бобби, если бы он пошел к себе в участок и заглянул в картотеку, чтобы узнать, кто владелец интересующего его «Мерседеса» (содержащаяся в ней информация та же, что и в компьютерной базе)? Суть вопроса здесь заключается в том, что юридически защите подлежит в данном случае не сама информация как таковая, а носитель, на котором она хранится. Хотя и данные также могут быть защищены другими нормами, по которым действия Бобби также могут квалифицироваться как правонарушение.  В полицейских компьютерных базах, наряду со множеством других конфиденциальных данных, хранится большой объем информации личного характера. Допуск к такого рода сведениям должен предоставляться только на законных основаниях. Сотрудники и операторы британской полиции часто попадаются на несанкционированном доступе к компьютерным данным в личных целях, то есть: в поисках информации, которая может представлять интерес для прессы или же для того или иного частного лица, подкупившего коррумпированного сотрудника органов. Бывает, что такой несанкционированный поиск ведётся для того, чтобы узнать, находится ли отдельный человек или группа лиц в активной разработке. | |
| Слайд 46 | 1. **Случай 2**  * **Изложение фактов / ситуации**   На сотрудника охраны банка выходит преступная группировка, требующая от него установить приспособление известное под названием «аппаратный кейлоггер» (миниатюрный прибор, регистрирующий все нажатия клавиш/кнопок) на обратной стороне ряда компьютерных терминалов, используемых работниками его банка. Вышеуказанное устройство регистрирует все нажатия клавиш пользователем, перехватывает пароли и иную информацию, позволяющую третьему лицу, имеющему доступ к банковскому терминалу, регистрировать движение средств по счетам клиентов банка.  «Аппаратный кейлоггер» позволяет также записывать телефонные звонки, осуществляемые по «скайпу» пользователем терминала.  Кроме того, преступники установили на пульт управления звукозаписывающий «жучок», регистрирующий в частности и входящие/исходящие телефонные звонки, осуществляемые пользователем терминала.  *Имел ли здесь место противозаконный перехват?*   * **Рассматриваемые темы:**   *- Имел ли здесь место противозаконный перехват?*  *- Был ли этот перехват осуществлён с использованием технических средств?*  *- Передавались ли при этом входящие или исходящие данные?*   * **Вопросы для обсуждения:**   «Аппаратный кейлоггер» представляет собой техническое устройство, перехватывающее данные, которые передаются с терминала. Соответственно, это действие является перехватом, осуществляемым абсолютно противозаконно.  Как здесь с юридической точки зрения обстоят дела со звонками по «скайпу»? В данном случае связь шла по той же линии, что и остальные данные, передаваемые с компьютерного терминала. А если бы для звонков по «скайпу» использовался другой компьютер? Ведь в соответствии с формулировками, содержащимися в «Будапештской конвенции», «компьютерная система» определяется как *«любое устройство или группа взаимосвязанных или смежных устройств, одно или более из которых, работая в соответствии с установленной программой, осуществляет автоматизированную обработку данных»;* а «компьютерные данные» как *«любое представление фактов, информации или понятий в форме, приемлемой для обработки компьютерной системой, включая программы, способные обязать компьютерную систему выполнять ту или иную функцию».*  Юридическая квалификация использования «жучка» может оказаться немного сложнее. Идёт ли здесь речь о «перехвате»? Британский суд постановил следующее: для того, чтобы факт перехвата рассматривался как установленный, должно иметь место подключение к линии или прибору передачи сигнала. В рассматриваемом же случае, регистрация сигнала происходила независимо от его передачи, хотя полученная при этом информация одна и та же вне зависимости от того, был ли инструмент перехвата «подключён к линии передачи» или нет.  А если бы «кейлоггер» был установлен руководством самой компании, озабоченным тем, чтобы её сотрудники не использовали интернет неположенным образом?  Большинство телекоммуникационных систем используют как частные сети, так сети общего пользования. Там, где сообщение выходит за пределы сети, являющейся вашей собственностью, оно переходит из частной сферы в общественную. Контролирующая инстанция частной телекоммуникационной системы вправе иметь доступ к сообщениям, передаваемым с использованием этой системы, точно также как, например, вы можете прослушивать телефонные разговоры по спаренному телефону домашней телефонной линии при условии, что ваш телефонный аппарат подключён к её участку, проходящему по вашей части дома.  Эта конкретная ситуация приведена здесь для того, чтобы заставить слушателей задуматься над каждым из элементов противозаконного перехвата компьютерных данных в процессе их передачи с использованием технических средств.  Слушатели должны уяснить себе, что эта норма направлена на защиту в большей степени содержания сообщений, нежели чем сопутствующей технической информации, связанной с операцией их адресации или же со стоимостью этой услуги. | |
| Слайд 47 | 1. **Случай 3**  * **Изложение фактов / ситуации**   Члены бандформирования общаются друг с другом через систему электронной почты в интернете, доступной из любой точки мира. Вместо того, чтобы обмениваться мейлами, которые могут быть перехвачены полицией, или же послужить обличающей уликой в случае обнаружения таковых в их компьютерах, они используют схему «электронной почты до востребования». Конкретно, вместо того, чтобы отправить уже составленное сообщение, один из членов банды переносит его в раздел «черновики». Получатель сообщения, другой её член, имея пароль доступа к этому электронному почтовому ящику, заходит в его «черновики», считывает сообщение и точно таким же образом отвечает на него.  *Если бы у полиции был доступ к разделу «черновики» вышеуказанного почтового ящика, то можно ли квалифицировать это как перехват?*   * **Рассматриваемые темы:**   *Находится ли сообщение в процессе передачи?*   * **Вопросы для обсуждения:**   Во многих государствах от полиции требуется, чтобы она доказала критически высокую степень подозрительности тех или иных действий, прежде чем ей будет дано разрешение на перехват содержания сообщений. Несанкционированное получение доказательств может привести к закрытию дела или же к тому, что такие доказательства будут рассматриваться как недопустимые.  Компьютерные технологии и интернет-приложения значительно облегчают общение по электронной почте, через чаты, системы обмена сообщениями в реальном времени, «твиттер» и так далее. Часто сообщения хранятся в памяти системы в ожидании того, когда их оттуда извлекут предполагаемые получатели. Может ли такое сообщение, ожидающее извлечения из памяти, рассматриваться как находящееся в процессе передачи? Применительно к нашему случаю невозможно определить, было ли сообщение, оставленное в разделе «черновики», прочтено тем получателем, которому оно предназначалось. Должен ли закон предоставлять одинаковую защиту тем, кто сознательно предпочитает идти в обход нормальных способов передачи сообщений по электронной почте, и тем, кто пользуется ею как положено?  Речь в данном случае идёт об общепринятом и внешне вполне пристойном способе общения между преступными элементами общества. Вне зависимости от того, будут ли делаться попытки получить доступ к этим сообщениям посредством перехвата или же иными способами, реакция запрашиваемой стороны зависит от внутригосударственного законодательства и позиции национальных судов. Но в таком случае представители запрашивающей стороны не должны забывать следующее: если у них возникла необходимость в обращении к системе взаимной юридической помощи для получения такого рода данных, то запрашиваемое государство может счесть, что речь идёт именно о перехвате (так как в запросе говорится о доступе к содержанию обмена сообщениями), и потребовать подачи запроса на более высоком правовом уровне на получение подобного судебного разрешения. | |
| Слайд 48 | 1. **Случай 4**  * **Изложение фактов / ситуации**   Сотрудник полиции Бобби взял мобильный телефон своей супруги, вычислил пароль и прослушал оставленное на нём голосовое сообщение, которое она ещё не успела открыть.  *Является ли это перехватом?*   * **Рассматриваемые темы:**   *- Находится ли это голосовое сообщение в процессе передачи?*  *- Имел ли место перехват компьютерных данных?*   * **Вопросы для обсуждения:**   До тех пор, пока сообщение не открыто получателем, оно находится в процессе передачи, даже если при этом оно хранится в памяти системы. Возможно, что физически сообщение хранится в цифровом виде на сервере телефонной компании и поэтому Бобби получил доступ к компьютерным данным. Является ли телефонный аппарат ЭВМ (компьютером)? Может являться таковым, так как он осуществляет автоматизированную обработку данных. Сотрудники полиции, имеющие дело в рамках следственных действий с телефонным аппаратом, должны не забывать об этом и убедиться, не надо ли им получить соответствующее разрешение на доступ к хранящимся сообщениям. Положение меняется в том случае, если получатель уже прослушал оставленные для него сообщения и решил сохранить их.  Этот конкретный случай ставит перед слушателями те же вопросы, что и предыдущий. Он выступает в качестве иллюстрации вполне стандартной ситуации, в которой может оказаться любой сотрудник полиции, изымающий во исполнении ордера на обыск компьютер, в памяти которого хранятся как открытые, так и не открытые мейлы. Этот случай также служит дополнительным напоминанием о том, что положения статьи 3 «Будапештской конвенции» распространяются на все формы передачи электронных данных, будь то факсом, по телефону, по электронной почте или же через файлообменник. | |
| Слайд 49 | 1. **Случай 5**  * **Изложение фактов / ситуации**   Бобби интересуется темой НЛО и убеждён, что российское правительство захватило инопланетный звездолёт, приземлившийся в Сибири в начале ХХ-го века. Он заходит на рекрутинговый сайт российской армии, в котором имеется ссылка на сайт российских ВВС. Для того, чтобы зайти на него, нужно знать пароль. Бобби с помощью программы по взлому паролей удаётся получить доступ на этот сайт. У него уходит определённое время на то, чтобы изучить систему и скопировать ряд файлов. Он также пытается удалить все файлы системного журнала («лог-файлы»), чтобы стереть следы своего захода во избежание опознания его русскими. И, наконец, он видоизменяет титульную страницу сайта, заменив эмблему российских ВВС на изображение НЛО.  *Совершил ли Бобби правонарушение?*   * **Рассматриваемые темы:**   *Может ли несанкционированный доступ как таковой быть приравнен к правонарушению, квалифицируемому как вмешательство в базу данных и в работу компьютерных систем?*  *Может ли уничтожение доказательств совершения несанкционированного доступа рассматриваться как правонарушение?*  *Была ли серьёзно нарушена работа компьютера ещё до наступления уголовной ответственности?*   * **Вопросы для обсуждения:**   Эта норма направлена на обеспечение компьютерным данным и программам такой же правовой защиты от умышленного повреждения, как и материальным объектам, находящимся в чьей-либо собственности.    У Бобби не было разрешения на доступ к сайту ВВС, защищённому паролем. Таким образом, совершенный им доступ образует состав правонарушения, квалифицируемого как противоправный, (несанкционированный) доступ.  Бобби удалил данные, файлы системного журнала («лог-файлы») и эмблему ВВС. Даже если он, возможно, и создал не свои «лог-файлы», конфигурация системы такова, что она зарегистрировала произведённые в ней действия. Бобби был не вправе удалять эти файлы системного журнала («лог-файлы»). Руководство ВВС может заинтересоваться тем, кто зашел в его систему.    Видоизменив титульную страницу сайта, он одновременно удалил определённые данные из системы и добавил в неё новые. Хотя эти действия и не привели, по всей видимости, к значительной потере информации, они могут поставить ВВС в неловкое положение. Конечно же, Бобби вправе заявить в свою защиту, что он лишь зашел на сайт в поисках информации и ограничился удалением файлов системного журнала («лог-файлов») и иных незначительных данных. Тем не менее, может ли какой бы то ни было системный администратор верить в возможность обеспечения целостности и сохранности цифровых данных после такого противозаконного вмешательства?  Было ли при подобных обстоятельствах совершено правонарушение? Ответ на этот вопрос зависит от того, как вышеописанные деяния толкуются с точки зрения российского законодательства. Может так случится, что пороговая величина их тяжести не будет установлена. Тем не менее, системный администратор, вполне возможно, будет вынужден временно вывести сайт из эксплуатации. Обычно это делается для того, чтобы оценить последствия вмешательства и, прежде всего, определить, не содержалось ли на таком сайте конфиденциальной или же секретной информации. Особая осторожность необходима при работе с системами, сбои в работе которых могут представлять опасность для широкой общественности. В качестве примера здесь можно привести автоматизированные системы управления ядерными электростанциями.  Если чисто теоретически предположить, что компьютерная система, доступ к которой получил Бобби, была предназначена для автоматизированного управления ядерной электростанцией, то была бы квалификация его правонарушения по статьям 4 и 5 «Будапештской конвенции» достаточной для отражения всей тяжести подобного вмешательства, которое может быть приравнено к нападению на инфраструктурный объект государственной важности? | |
| Слайд 50 | 1. **Случай 6**  * **Изложение фактов / ситуации**   Программа автоматизированной массовой рассылки электронных писем типа «СПАМ» ежедневно рассылает мейлы тысячам пользователей, которые их не ждут. Если получатель открывает такое сообщение, то происходит автоматическая загрузка на компьютер программы, которая никак не препятствует его работе, не считывает и не удаляет из него данные, и вообще не причиняет ему никакого вреда. Тем не менее, компьютер такого пользователя отныне «зомбирован» и входит в так называемую «бот-сеть». Лицо, удалённо управляющее этой сетью (т. н. «бот-контролёр»), может использовать входящие в неё компьютеры для достижения своих целей.  *Совершило ли лицо, ответственное за рассылку «СПАМА», правонарушения, предусмотренные статьями 4 и 5 «Будапештской конвенции»?*   * **Рассматриваемые темы:**     *Имел ли место несанкционированный доступ к компьютеру пользователя?*  *Были ли изменены данные на компьютере пользователя?*  *Был ли поврежден компьютер пользователя?*   * **Вопросы для обсуждения:**   Даже при отсутствии какого бы то ни было физического повреждения самоустановившаяся на компьютер пользователя программа вызывает изменение имеющихся в нём данных. Это изменение несанкционированное постольку, поскольку пользователь не был ни коем образом предупреждён об опасности изменения программного обеспечения, установленного на его компьютере, и не давал на то своего согласия. Является ли с юридической точки зрения рассылка «СПАМА» противозаконным деянием, или же это просто назойливая форма, скажем, рекламы, создающая некоторые неудобства? Становится ли это деяние противозаконным, только начиная с того момента, когда оно вызывает отрицательные, вредные последствия?  А если бы этот «СПАМ» содержал прикреплённый документ и приглашение открыть его, адресованное получателю, сопровождаемое фразой: «Это вам понравится»?  Можно конечно возразить, что получатель сам сделал свой выбор и дал тем самым согласие на загрузку данных на принадлежащий ему компьютер. Тем не менее, всё дело в том, что в действительности не всякое данное согласие является согласием осознанным и основанным на полной информации (т. н. «информированным согласием»). Хотя и на это можно возразить, что получатели, решающие открыть тот или иной прикреплённый файл, поступивший от неизвестного им лица, действуют на свой страх и риск.  Меняется ли что-нибудь от того, что пользователя не волнует вопрос, стал ли его компьютер частью «бот-сети» или нет?  Когда мы путешествуем по интернет-сети, мы заходим на разные сайты и загружаем с них данные, не обращая должного внимания на характер материалов, которые могут оказаться в нашем компьютере. Мы доверяемся названиям, которые сайты присваивают сами себе, наименованиям файлов или же результатам, выдаваемым поисковым мотором, и позволяющим нам принимать те или иные решения. Предполагается, что "кликая" на уменьшенную растровую пиктограмму для получения развёрнутого изображения, мы тем самым подтверждаем, что мы осведомлены о характере искомых данных, и даём наше полностью осознанное согласие. Но с другой стороны, если после «клика» на уменьшенную пиктограмму двигателя автомобиля мы видим на развёрнутом изображении авиационный двигатель, то нельзя утверждать, что наше согласие на получение таких данных было осознанным («информированным»).  Решение кликнуть на гиперссылку и открыть таким образом тот или иной сайт приводит к загрузке большого количества данных. Если сайт легальный, то значительная доля содержащейся на нём информации может относиться к его содержательной части, хотя и вперемешку с рекламой, размещённой на нём третьими лицами. И снова здесь мы совершили очередной осознанный выбор и дали своё косвенное согласие на получение рекламных объявлений, зная, что это является общепринятой практикой в интернете. Другим распространённым приёмом в интернет-индустрии стали так называемые «куки-файлы», то есть специальные маркерные файлы, автоматически загружающиеся с посещаемого веб-сервера на компьютер пользователя через навигатор (программу просмотра веб-страниц).  «Куки-файлы» выполняют самые различные функции. В том числе, они регистрируют все обращения каждого конкретного пользователя к данному веб-серверу. В веб-навигаторе пользователю предоставляется возможность («опция») самостоятельно сделать выбор: активировать или дезактивировать функцию «куки-файлов» в программе просмотра веб-страниц (иными словами, разрешить ей или запретить автоматически загружать вышеуказанные файлы на компьютер пользователя). Достаточно ли наличия в программе веб-навигатора такой «опции» (возможности выбора для пользователя) для утверждения того, что пользователь осознанно даёт согласие на загрузку подобных файлов на свой компьютер? | |
| Слайд 51 | 1. **Случай 7**  * **Изложение фактов / ситуации**   Бобби является бывшим сотрудником полиции. Его уволили за злоупотребление информацией, полученной из полицейских баз данных. Он решает отомстить органам. Бобби использует для этого программу рассылки электронной почты, позволяющую ему направлять до 70 000 мейлов в час на электронный адрес отделения, где он раньше работал. Он меняет заголовок электронной почты таким образом, чтобы в нём фигурировала фамилия начальника отделения. Тем самым для почтового сервера полиции отправленные мейлы поступают из законного источника. В результате сервер полиции не справляется с нагрузкой и отключается.  *Можно ли квалифицировать данное правонарушение как вмешательство в работу компьютерных систем?*   * **Рассматриваемые темы:**   *Отправка электронной почты («мейлов») предполагает получение или попытку получения доступа к компьютерной системе, в данном случае к системе сервера электронной почты. В каких пределах владельцем сервера разрешен подобный допуск?*  *Если у вас есть адрес электронной почты, разве это не значит, что тем самым вы приглашаете других лиц направлять вам мейлы?*   * **Вопросы для обсуждения:**   Это очередной вопрос из области права. Бобби вошел в систему и спровоцировал её отключение путём перегрузки вводимыми данными. Создавая электронный адрес, доступный для широкой публики, его владелец по умолчанию даёт своё косвенное согласие на получение сообщений. Бобби может в качестве довода заявить, что полиция дала таким образом согласие на получение электронных писем от любого лица, и что это не его вина, если её компьютерной системе не хватает мощностей для обработки такого количества сообщений. Но было ли в действительности дано согласие? Положим, владелец дома даёт своё согласие по умолчанию на то, чтобы почтальон клал в его почтовый ящик адресованные ему письма. Это согласие распространяется также и на рассылаемую по почте рекламу, скажем, рекламу пиццы. Но это не значит, что владелец дома давал согласие на получение такого её количества, что в один прекрасный день он не сможет даже открыть свою входную дверь, заваленную до верха рекламными объявлениями.  Не следует ли также особо подчеркнуть, что – в связи со внесением изменений в реквизиты отправки электронной почты – доступ к почтовому серверу был получен мошенническим способом? Согласия на получение таких мейлов с ложным адресом отправителя никто не давал.  Хотя приведённая выше ситуация касается электронной почты, общий описанный при её рассмотрении принцип применим ко всем попыткам поставить работу сайта под угрозу с помощью его перегрузки или же атак с целью нарушения нормального обслуживания. Заход на любой сайт приводит к обмену данными между пользователем и самим сайтом. Соответственно, заход на сайт предполагает наличие косвенного согласия пользователя на такой обмен, и в связи с этим возникают все те же вопросы, что были рассмотрены выше, когда речь шла о рассылке электронной почты. | |
| Слайд 52 | 1. **Случай 8**  * **Изложение фактов / ситуации**   Бобби посылает электронное письмо на работу своей супруге, которая с ним больше не живёт. Он изменяет заголовок электронного письма таким образом, чтобы она подумала, что мейл пришел от одного из её друзей. Кроме того, к электронному сообщению прикреплена программа под кодовым названием «проход всюду», позволяющая Бобби следить за компьютером жены. Бобби не повезло. Он не успел воспользоваться этой программой, присутствие которой было обнаружено системным администратором. Последний был вынужден отключить систему для оценки масштабов ущерба от постороннего вмешательства в её работу.  *Совершил ли Бобби правонарушение, предусмотренное статьей 5 «Будапештской конвенции»?*   * **Рассматриваемые темы:**   *- Привели ли действия Бобби к удалению данных, находящихся в компьютерной системе?*  *- Создал ли Бобби помехи функционированию компьютерной системы?*  *- Были ли удаление данных или же создание помех функционированию компьютерной системы произведены противоправно?*   * **Вопросы для обсуждения:**   Реакция системного администратора на действия Бобби привела к тому, что пользователям системы было отказано в обслуживании. Соответственно, доступ к данным, содержащимся в компьютерной системе, был прерван, хотя, по всей видимости, и временно. Для того, чтобы деяние Бобби квалифицировалось как правонарушение, не требуется, чтобы данные были постоянно недоступны пользователям.  Выше мы уже обсудили ту степень заполнения электронного почтового ящика, в пределах которой её владелец даёт своё согласие на получение электронных сообщений.  В статье 5 «Будапештской конвенции» речь идёт о компьютерных системах, в рамках которых работают один или несколько соединённых друг с другом компьютеров. А является ли отдельно взятый компьютер, подключённый к интернету, частью компьютерной системы?  Рабочий компьютер жены Бобби, скорее всего, не является частью компьютерной системы, а возможно входит в локальную сеть или же сеть широкого доступа интернета. Учитывая всё вышесказанное, создал ли Бобби помехи работе компьютерной системы?  Бобби может возразить, что он не несёт ответственности за отказ в обслуживании, что это ни коем образом не входило в его намерения и что в действительности, наоборот, он заинтересован в нормальной работе компьютерной системы постольку, поскольку это позволило бы ему следить за женой. Зачастую атаки с целью нарушения нормального обслуживания пользователей недостаточно для отключения сайта. Тем не менее, поставщики интернет-услуг («провайдеры») прибегают к таким отключениям, чтобы свести к минимуму последствия атаки и неудобства для пользователей.  В приведённой выше ситуации, Бобби, как представляется, не имел намерения совершать правонарушение, предусмотренное статьей 5 «Будапештской конвенции», но это вовсе не значит, что ему удастся уйти от уголовной ответственности.  Здесь был дан один из примеров использования вирусов типа «Троянский конь» («Троян»), широко применяемых киберпреступниками для получения доступа к чужим компьютерам. | |
| Слайд 53 | 1. **Случай 9**  * **Изложение фактов / ситуации**   Группа «хакеров»-активистов, протестующих против использования подопытных животных для апробирования на них косметической продукции, ведёт распределенные атаки типа «отказ в обслуживании» (так называемые «DDоS-атаки») на веб-сайты глянцевых журналов и компаний-производителей косметики. Через свой сайт эта группа распространяет программное обеспечение, прозванное активистами «Сверхоружие», которое позволяет им координировать атаки на веб-сайты и доводить таким образом до максимума объем данных и пакетов, нацеленных на тот или иной веб-сайт в определённое время суток. Изначально эта программа была разработана системными администраторами как инструмент проверки надёжности компьютерных систем. «Сверхоружие» работает точно таким же образом, что и её первые версии, но новый пользовательский интерфейс этой программы значительно упростил работу с ней. Кроме того, на нём сейчас фигурирует эмблема вышеуказанной хакерской группы активистов.  *- Является ли правонарушением выкладка в сети программы «Сверхоружие» для свободной загрузки?*  *- Является ли правонарушением обладание программой «Сверхоружие»?*   * **Рассматриваемые темы:**   *Программа «Сверхоружие» применяется, в частности, для достижения законных целей; значит ли это, что её использование не может повлечь уголовного преследования?*  *Может ли выкладка в сети программы «Сверхоружие» для свободной загрузки быть приравнена к её распространению?*   * **Вопросы для обсуждения:**   Правонарушениями, предусмотренными интересующей нас статьей «Будапештской конвенции», являются: противоправный (несанкционированный) доступ, противоправный (несанкционированный) перехват, вмешательство в базу данных и в работу компьютерных систем.  Изначально рассматриваемое нами программное обеспечение было двойного назначения и использовалось в законных целях. Является ли правонарушением обладание этой программой после того, как её пользовательский интерфейс был изменен?  Вернёмся назад к уже рассмотренным нами ситуациям. Дело в том, что у программы «Проход всюду», с помощью которой Бобби пытался проникнуть в компьютер своей жены, есть и законное использование: такого рода программы позволяют пользователям получать дистанционный доступ к своим компьютерам.  Является ли правонарушением то, что у Бобби был пароль для взлома программы? Это может зависеть от его намерений: какие у него были законные основания для обладания подобным программным обеспечением? Есть ли какие бы то ни было доказательства, свидетельствующие о том, что он намеревался установить его с целью совершения правонарушения?  Состав этого правонарушения не позволяет квалифицировать как уголовно наказуемое деяние работу поставщиков законного программного обеспечения и его пользователей. Там, где есть доказательства наличия злого умысла (как это имеет место быть в вышерассмотренном случае), проблем может и не возникнуть. Тем не менее, в жизни зачастую случается так, что лица, вовлечённые в преступную деятельность в сфере компьютерной информации, параллельно вполне легально работают в этой же области и могут быть занятыми в промышленности профессионалами, разрабатывающими подобного рода программное обеспечение. Но когда им представляется удобный случай, они вполне подготовлены к использованию этих программ в качестве инструментов, содействующих совершению противозаконных деяний. А как обстоит дело с продавцами софта? Как предположительно они могут определить, с какой целью неизвестный им покупатель приобретает у них то или иное оборудование или же программное обеспечение? Или же признаки состава этого правонарушения слишком размыты? | |
| Слайд 54 | 1. **Случай 10**  * **Изложение фактов / ситуации**   Поставщик программного обеспечения создал программу криптографической защиты. Она делит содержимое на жестком диске на два раздела («тома»), для доступа к каждому из которых нужен свой пароль. Тем не менее, обычный пользователь видит на экране только один раздел («том»), в то время как существование скрытого раздела («тома») невозможно обнаружить с помощью легального, широкодоступного программного обеспечения.  Производитель утверждает, что данная программа может потребоваться любому лицу, которое под принужденным будет вынуждено сообщить пароль от видимого раздела («тома»). Таким образом содержимое второго, скрытого раздела («тома») остается нераскрытым, даже если взломщикам и известен пароль от первого.   * **Рассматриваемые темы:**   *Является ли уголовно наказуемым деянием производство, копирование, распространение и использование подобного программного обеспечения*?   * **Вопросы для обсуждения:**   Все мы постоянно переживаем за сохранность данных. Между тем, данная программа явно создана для удовлетворения потребностей лиц, вовлечённых в преступную деятельность, и в особенности тех, кто опасается, как бы содержимое их компьютеров не было использовано для привлечения их к уголовной ответственности. Эта программа им нужна не столько для совершения противоправных деяний, сколько для сокрытия таковых и сопутствующих доказательств.  Кроме того, киберпреступники могут прибегать и к другим программам или же компьютерным системам во избежание обнаружения следов их деятельности. Речь здесь идёт, в частности, о так называемых «анонимайзерах», позволяющих получать доступ к интересующим их интернет-ресурсам, не раскрывая своих истинных IP-адресов, или же о программах для безвозвратного удаления компьютерных улик с жесткого диска компьютера. | |
| Слайд 55 | 1. **Случай 11**  * **Изложение фактов / ситуации**   Ник работает в отделе информационных технологий крупной компании, имеющей свою внутрикорпоративную сеть связи (т. н. «интранет»). Внутренними правилами компании её сотрудникам запрещается использовать свои служебные компьютеры и подключаться к интернету для того, чтобы совершать покупки в сети. В свободное время Ник занялся разработкой программы, которая позволила бы компании выявлять тех её сотрудников, которые осуществляют платежи в сети, перехватывая информацию таким образом, чтобы впоследствии она могла использоваться в качестве улики во время дисциплинарного разбирательства. Нику для этого не хватает профессиональных навыков, и он выходит в сети на пользователя под ником «Юпитер». Совместно они дорабатывают это программное обеспечение, которое после его установки на компьютер пользователя активизируется в момент его выхода в сеть и начинает перехватывать данные, вводимые последним. Компания Ника было очень довольна, когда «Юпитер» приступил к развёртыванию этого программного обеспечения, несмотря на то, что оно стало, по сути дела, компьютерным «троянским конём» в её корпоративной системе «интранета».  *Совершил ли Ник правонарушение?*  *Совершила ли его компания правонарушение?*  *Совершил ли «Юпитер» правонарушение?*   * **Рассматриваемые темы:**   *Было ли это программное обеспечение изначально задумано (или же в дальнейшем приспособлено) с целью совершения вышеуказанного уголовно наказуемого правонарушения?*   * **Вопросы для обсуждения:**   Компьютерным злоумышленникам доступен широкий набор различных инструментов, позволяющих им совершать свои преступления или же облегчающие эту задачу. Можно купить код, позволяющий создать свою собственную «бот-сеть», или сразу купить такую сеть под ключ, или же, наконец, получить за деньги доступ к «бот-сети», с помощью которой можно совершать разного рода преступные деяния, например, заняться «выуживанием» у пользователей паролей и кодов доступа (т. н. «фишингом»).  «Юпитер» воспользуется этой программой для получения финансовой информации, которая может быть использована либо им самим, либо третьими лицами. Руководство компании, по-видимому, подумает, что Ник занимался этой разработкой в рабочее время. Сам же Ник ни в чём не виновен. Он просто по неосмотрительности доверился «Юпитеру» и помог ему обзавестись мощным орудием совершения преступлений. Ни у Ника, ни у компании не было преступных намерений, наличие которых по закону необходимо для квалификации правонарушения. Обстояло бы дело иначе, если бы «Юпитер» предложил эту программу на рынке другим компаниям, желающим отслеживать действия своих сотрудников в интернете? Может ли «Юпитер» возразить, несмотря на всю свою явную склонность к криминалу, что у этого программного обеспечения вполне законное предназначение? | |
| Слайд 56 | 1. **Случай 12**  * **Изложение фактов / ситуации**   Стефан использует имеющееся в открытой продаже программное обеспечение для работы с цифровыми изображениями для создания на своём домашнем компьютере банковской тратты, вполне похожей на настоящую. Изготовленную таким образом тратту он предъявляет своему банку, который принимает его за подлинную и осуществляет перевод соответствующих средств на счёт Стефана.  *Какое правонарушение совершил Стефан?*   * **Рассматриваемые темы:**   *- Является ли изготовление поддельной банковской тратты подлогом с использованием компьютерных технических средств?*  *- Можно ли рассматривать данное правонарушение совершенным лишь начиная с того момента, когда банковский служащий принял тратту как подлинную?*   * **Вопросы для обсуждения:**   Изготовление банковской тратты предполагает введение в компьютер недостоверных данных, так как создаваемая Стефаном тратта выписана на его имя. Здесь возникает вопрос, было ли это сделано неправомерно, или же Стефан вправе изготовить подобный документ с помощью своего собственного компьютера? У Стефана могло быть намерение использовать эту тратту для того, чтобы обмануть банк, но по какой-либо причине он мог никогда и не распечатать созданное им на экране изображение. Меняется ли степень ответственности Стефана в зависимости от того, распечатал он его на бумаге или нет?  Этот вид правонарушения был введён в законодательство не для того, чтобы можно было давать квалификацию подобного рода ситуациям. Хотя оно и может пригодиться, если в национальном законодательстве не найдётся иной квалификации деяния, заключающегося в производстве поддельных банковских тратт. Такого рода правонарушения лучше рассматривать с точки зрения субсидиарной ответственности, то есть как попытку их совершения.  Это правонарушение относится к тому разряду противоправных деяний, при совершении которых компьютер применяется в качестве орудия преступления. Применительно к данному случаю, таковое считается совершенным, начиная с того момента, когда банковский служащий, действуя вполне добросовестно, зарегистрировал банковскую тратту Стефана как подлинную. | |
| Слайд 53 | 1. **Случай 13**  * **Изложение фактов / ситуации**   Стефан всегда хвастался перед друзьями своими спортивными достижениями в юности. Последние относились к этому скептически. Тогда Стефан сумел получить доступ к базе данных школы, где он когда-то учился, и внести в неё изменения. В соответствии с новой редакцией получалось, что Стефан был капитаном школьной команды и завоевал несколько медалей.  *Образует ли это деяние состав правонарушения, квалифицируемого как подлог с использованием компьютерных технических средств?*   * **Рассматриваемые темы:**   Изменённые Стефаном данные никак не будут использоваться в юридических целях?   * **Вопросы для обсуждения:**   Стефан заменил данные в базе на ложные. Ясно, что этот доступ, равно как и внесение изменений в данные, были произведены противоправно. Оставляя в стороне другие правонарушения, которые Стефан мог совершить, всё же сомнительно, чтобы в данном случае он совершил подлог с использованием компьютерных технических средств, так как изменённые им данные не будут использоваться в юридических целях.  При совершении этого подлога не преследовались цели получения финансовой или же иной выгоды (в таком случае правонарушение в большей степени относилось бы к сфере мошенничества с использованием компьютерных технологий). Статья 7 «Будапештской конвенции» направлена на обеспечение сохранности и достоверности тех электронных данных, которые могут иметь последствия для правовых отношений. Под данными, «используемыми в юридических целях», имеются в виду протоколы и иные документы, имеющие юридическую значимость. | |
| Слайд 58 | 1. **Случай 14**  * **Изложение фактов / ситуации**   Потеряв работу в полиции и будучи вынужденным платить алименты своей бывшей жене после развода, Бобби ищет другие способы заработка. Он всегда интересовался биржевыми спекуляциями и приобрёл 1000 акций «Фландрской горнорудной компании», имеющей эксклюзивное право на эксплуатацию урановых рудников в Бельгии, заплатив по одному Евро за акцию. Бобби участвует в интернет-форуме, членов которого, также как и Бобби, привлекает игра на бирже. Бобби размещает на форуме сообщение, утверждающее, что его друг, входящий в состав правительства Бельгии, сообщил ему об открытии в Бельгии значительных запасов урановой руды. За этим сообщением последовал резкий рост курса акций «Фландрской горнорудной компании», подскочивший к концу недели до 1000 Евро за штуку. После этого Бобби продал свои акции.  *Совершил ли Бобби правонарушение?*   * **Рассматриваемые темы:**     *- Было ли размещённое Бобби сообщение ложным?*  *- Понесли ли другие лица ущерб в результате размещения на форуме этого ложного сообщения?*  *- Извлёк ли Бобби экономическую выгоду?*   * **Вопросы для обсуждения:**   Если сообщение, размещённое Бобби на интернет-форуме, было ложным, то он мог совершить правонарушение. Он ввёл ложные данные в компьютерную систему и извлёк для себя экономическую выгоду в результате роста стоимости акций.  Нуждается ли в доказательстве наличие причинно-следственной связи между введением в систему ложной информации и последствиями этого?  Потеряли ли что-нибудь остальные игроки в результате действий Бобби? Возможно, и потеряли, так как стоимость акций была оценена ими неверно и цена на них в определённый момент вероятно упадёт. Хотя надо признать, что рынок акций являет собой пример крайней неопределённости и зыбкости. Действительно, разве стоимость акции не измеряется той суммой, которую игрок желает за неё заплатить в тот или иной конкретный момент времени? Становился ли кто-нибудь по-настоящему жертвой мошенничества? Не являются ли подобного рода слухи и сообщения обычным делом в интернете? Разве кто-нибудь и в правду поверит этим рассылкам или же не увидит в них грубую попытку манипуляции курсом акций? Значит ли это, что мы не можем лгать в интернет-сети? | |
| Слайд 59 | 1. **Случай 15**  * **Изложение фактов / ситуации**   Стефан едет в банк. На автостоянке выясняется, что у него не хватает мелочи на оплату парковки. Тогда он кладёт в парковочный автомат жетон, оставшийся у него в кошельке после посещения прачечной. Получается так, что автомат срабатывает и выдаёт ему парковочный талон.  *Совершил ли Стефан правонарушение?*   * **Рассматриваемые темы:**   *- Является ли парковочный аппарат компьютером?*  *- Имеет ли какое-то значение, парковочный ли автомат автоматически выдал талон, или же живой парковщик был введён в заблуждение?*  *- Каков статус парковочного талона?*   * **Вопросы для обсуждения:**   Парковочный автомат является компьютером: он обрабатывает вводимые в него данные, производит расчет суммы в зависимости от стоимости парковки и выдаёт соответствующий парковочный талон на определённое время. То, что Стефан положил в автомат жетон от прачечной вместо монеты, приравнивается ко введению в компьютер ложных данных. В статье 7 «Будапештской конвенции» не содержится требования, чтобы эти данные вводились непосредственно живым человеком.  Парковочный талон был получен в результате подлога, так как данные, использованные для распечатки, оказались ложными, и введены были в автомат для получения документа, который рассматривался бы парковщиком как подлинный. В противном случае, сам парковщик Стефану талона не выписал бы. | |
| Слайд 60 | 1. **Случай 16**  * **Изложение фактов / ситуации**     После ареста Стефана полиция обнаружила у него реквизиты банковских карт значительного числа третьих лиц.  *Является ли хранение подобных данных уголовно наказуемым правонарушением?*   * **Рассматриваемые темы:**   *- Каков статус компьютерных файлов?*  *- Являются ли они по закону «вещью», несмотря на то, что в действительности материально существуют лишь только в виде строк бинарного кода?*   * **Вопросы для обсуждения:**   В Объединённом Королевстве владение материалами, предназначенными для последующего использования в мошеннических целях, является нарушением норм материального уголовного права. Понятие «материалы» включает в себя и компьютерные файлы. Конечно же, ещё надо доказать наличие преступных намерений. Хотя в подобных случаях трудно бывает найти уважительную, законно обоснованную причину хранения такого рода данных у себя.  Вероятно, данное деяние можно рассматривать как приготовление к преступлению. | |
| Слайд 61 | 1. **Случай 17**  * **Изложение фактов / ситуации**   Адам является членом закрытого сетевого сообщества, в рамках которого происходит обмен фотографиями с изображением детей, подвергающихся сексуальному насилию. Кроме того, он входит в объединение лиц, пользующихся файлообменником, на котором он размещает вышеуказанные фотографии для того, чтобы сделать их доступными для остальных членов объединения.  *Какое правонарушение совершил Адам?*   * **Рассматриваемые темы:**   Как можно квалифицировать производство детской порнографической продукции, её приобретение и распространение?  Адам загрузил фотографии из интернета. Равнозначна ли загрузка таковых изображений их производству? Загрузка и, в особенности, хранение кадров в памяти компьютера не равноценны обычному их просмотру по телевизору, так как просмотр материалов по компьютеру технически невозможен без их предварительной временной загрузки. В результате же загрузки в компьютере возникает новый объект в виде компьютерного файла. Таким образом, получается, что просмотр изображений по компьютеру предполагает создание в нём новых объектов. Для прокуроров констатация этого факта может оказаться полезной.  Файлообменники позволяют членам возникающих вокруг них сообществ делать общедоступной интересующие их данные. Размещая фотографии на файлообменнике, Адам делал их доступными для дальнейшего распространения. | |
| Слайд 62 | 1. **Случай 18**  * **Изложение фактов / ситуации**   Билла арестовали в аэропорту по возвращении из Камбоджи. В его ноутбуке было обнаружено большое количество видеоматериалов, на которых он фигурировал при совершений действий сексуального характера в отношении детей родом из Юго-Восточной Азии.  *Может ли Билл подвергнутся уголовному преследованию на основании этих видеоматериалов?*   * **Темы, к которым относится рассматриваемый случай**   *Подсудность.*  *Выбор основного преступления: хранение или же изготовление видеоматериалов?*   * **Вопросы для обсуждения:**   Здесь могут возникнуть некоторые вопросы в связи с подсудностью, так как видеоматериалы были изготовлены за рубежом.  Что касается хранения, то тут вопросов, по всей видимости, не возникает.  Но какую позицию следовало бы занять, если бы все видеоматериалы были обнаружены в незанятом пространстве жесткого диска компьютера?  Хранение предполагает одновременно знание того места, где хранятся материалы, и возможность ими распоряжаться. Билл мог знать, а мог и не знать, что удалённые изображения могут быть ещё доступны на жестком диске, но что без соответствующих технических средств и должной сноровки ему никогда не удастся их восстановить. Так или иначе, прокурору остаётся (при условии решения вопроса о подсудности) преследовать Билла в судебном порядке либо за изготовление инкриминируемых ему видеоматериалов, либо за их хранение в прошлом.  А какой бы могла быть позиция суда, если бы на найденных фотографиях были изображены обнажённые дети от 3 до 7 лет, играющие на пляже, а Билл бы объяснил, что он нудист, допустив при этом, что получает сексуальное удовольствие от просмотра этих фотографий?  Являются ли подобные видеоматериалы законными или нет, зависит от того, как вопрос толкуется с точки зрения местного законодательства. В Соединённом Королевстве, как правило, для этого требуется, чтобы на изображениях присутствовала «сексуальная составляющая», в то время как мотивация фотографирующего лица рассматривается, как второстепенный момент.  *Кто решает, какие видеоматериалы законны, а какие незаконны? Достаточно ли чётко прописаны признаки этого правонарушения и очерчены пределы квалификации?* | |
| Слайд 63 | 1. **Случай 19**  * **Изложение фактов / ситуации**   WWW.Iuvfishin.com является веб-сайтом, посвящённым проблемам «выуживания» у пользователей паролей и кодов доступа (т. н. «фишинга»). Он базируется в США. Владелец сайта обнаруживает, что его сайт подвергся хакерской атаке, в результате которой тысячи фотографий с изображением сцен насилия над детьми были загружены и внедрены в его файловую систему. Причём, это было сделано таким образом, чтобы вышеуказанные видеоматериалы оставались невидимыми для обычных посетителей сайта. Сайт зарегистрировал IP-адреса тех лиц, которые просматривали эти фотографии.  На этом основании IP-адрес, присвоенный Джону, был сообщен полиции вашей страны. Сотрудники полиции провели обыск у Джона и изъяли его компьютер, содержавший сотни фотографий с изображением сцен насилия над детьми. Через "журнал посещений" его веб-навигатора и данных, содержавшихся в инкриминированных файлах, удалось выяснить, что большинство этих видеоматериалов было загружено через интернет.   * **Темы, к которым относится рассматриваемый случай**   *- Доказательство ответственности Джона за эти видеоматериалы.*  *- Последствия обвинения в педофилии для подозреваемых лиц.*   * **Вопросы для обсуждения:**   Вышеописанный способ тайного хранения видеоматериалов достаточно широко известен. Прибегающие к нему члены группы посылают друг другу гиперссылки на тайно хранящиеся таким образом файлы. Тем не менее, было бы непредусмотрительно полагаться только на IP-адрес для получения ордера на обыск, не выяснив, каким образом он оказался зарегистрированным в системном журнале посещений сайта, на котором скрытно хранятся незаконные видеоматериалы. Случайные посетители могли зайти в инкриминируемый раздел без какой бы то ни было вины с их стороны, будучи перенаправлены туда с других сайтов, и не добиваться доступа к содержащимся в нём видеоматериалам, осознав, что они собой представляют. Конечно же, не исключено, что такие «киберпрохожие» могли неоднократно заходить на этот сайт или же просмотреть некоторые видеоматериалы.  Эти соображения необходимо учитывать при обсуждении того, насколько важно крайне осторожно подходить к каждому конкретному случаю прежде, чем выдвигать обвинения в педофилии в отношении того или иного лица. Особенно, если учитывать высокий уровень самоубийств среди обвиняемых в такого рода правонарушениях. Как и во всех других случаях совершения преступлений в сфере компьютерной информации, необходимо быть в состоянии «усадить подозреваемого за клавиатуру» в нужный момент, так как один и тот же IP-адрес может использоваться сразу несколькими лицами, или же сеть беспроводной связи может подвергнуться взлому. Не следует забывать, что подобные обвинения, выдвинутые в адрес невиновного лица, имеют зачастую катастрофические последствия. | |
| Слайд 64 | 1. **Случай 20**  * **Изложение фактов / ситуации**   Полиция США накрыла веб-сайт, на котором размещались узлы, предлагавшие на продажу видеоматериалы со сценами насилия в отношении детей (оплата осуществлялась в виде ежемесячного абонемента). Американские власти перехватили реквизиты тех лиц, которые оплатили доступ к инкриминируемым им материалам, включая IP-адреса, номера кредитных карточек, адреса электронной почты и выставления счетов, а также пароли. Одним из пользователей сайта является Освальд. По предъявлении ордера на обыск, содержимое его компьютера было изучено. Ничего предосудительного не найдено, так как Освальд загодя использовал программу по безвозвратному удалению файлов с жесткого диска без возможности их дальнейшего восстановления под названием «Уничтожение улик».  *Совершил ли Освальд правонарушение?*   * **Темы, к которым относится рассматриваемый случай**   *- Является ли совершенное Освальдом правонарушение основным или же влечёт только субсидиарную ответственность?*  *- Возникают ли в связи с этим случаем вопросы о подсудности?*  *- Имеет ли значение тот факт, что этот американский сайт был полностью автоматизированным?*  *- Что можно сказать об использовании программы «Уничтожение улик»?*   * **Вопросы для обсуждения:**   В компьютере Освальда не хранилось никаких инкриминируемых ему видеоматериалов и мы не можем доказать, что он когда бы то ни было заходил на вышеуказанный сайт с целью просмотра таковых, хотя одновременно мы в состоянии доказать факт оплаты абонемента с целью получения доступа к ним. То есть, иными словами, Освальд заплатил деньги третьему лицу, владельцу сайта в США, с целью склонения такового к распространению или же предоставлению доступа к видеоматериалам со сценами насилия в отношении детей. Образуют ли эти действия состав правонарушения?  То, что американский сайт является полностью автоматизированным, значит, что обработка данных реквизитов кредитных карточек осуществляется без человеческого участия. Тем не менее, разработка алгоритма процесса, управление сайтом и его поддержка являются делом рук конкретного человека, который извлекает из этого финансовую выгоду.  Само по себе использование программы по уничтожению доказательств в электронной форме не является незаконным. Если только Освальд не воспользовался этой программой во время полицейского расследования, его вряд ли можно рассматривать как лицо, совершившее правонарушение, связанное с осуществлением правосудия. Тем не менее, Освальд преследуется по суду в связи с тем, что использование подобных компьютерных программ может рассматриваться судом как отягчающее обстоятельство. | |
|  | Практические занятия (проводятся при наличии необходимых условий)  Не предусмотрено. | |
|  | Проверка знаний  Тренер должен проверить знания слушателей, задавая им конкретные вопросы по каждой из пройденных на занятиях тем. | |
| Слайды 65 и 66 | Подведение итогов занятия/выводы  Инструктору необходимо подвести итоги / проверить знания слушателей, которые должны быть в состоянии:   * перечислить материальные нормы уголовного права, связанные с киберпреступлениями, и некоторые из ключевых признаков, используемых для того, чтобы охарактеризовать таковые, исходя из положений «Будапештской конвенции» * перечислить материальные нормы уголовного права, связанные с киберпреступлениями, и некоторые из ключевых признаков, используемых для того, чтобы охарактеризовать таковые, исходя их положений действующего национального законодательства; * объяснить необходимость и выгодность гармонизации между национальными законодательствами и международными документами на основе, прежде всего, «Будапештской конвенции». * определить основные нормы материального права, которые можно применить при рассмотрении обсуждаемых конкретных случаев из судебной практики. | |

|  |  |  |
| --- | --- | --- |
| Занятие 1.2.4 Процессуальное внутри-государственное законодательство | | **Продолжительность: 90 минут** |
| **Перечень материалов, необходимых для проведения занятия:**   * Ноутбук или ПК с операционной системой Windows 7 и с загруженным офисным пакетом приложений MS Office 2010; * Проектор с экраном; * Презентация «ПауерПойнт»; | | |
| **Цель:**  Настоящее занятие направлено на то, чтобы ввести участников из всех стран в следующую тему: следственные меры, предусмотренные национальным законодательством и национальными правовыми нормами в отношении электронных доказательств. | | |
| **Задачи:**  По окончании занятия слушатели должны быть в состоянии:   * перечислить национальные правовые нормы, регламентирующие использование доказательств в электронной форме (электронных доказательств); * перечислить предусмотренные национальным законодательством следственные меры по собиранию и обеспечению сохранности доказательств в электронной форме (электронных доказательств), а также требования, предъявляемые к порядку реализации вышеуказанных мер; раскрыть их смысл и важность; * выявить некоторые особенности национальных процессуальных норм, регламентирующих порядок работы с доказательствами в электронной форме (электронными доказательствами), по сравнению с соответствующими положениями международной правовой системы. | | |
| **Введение**  На занятии приводится пример того, как положения «Будапештской конвенции» были внедрены в национальное законодательство одной страны – в данном случае, Португалии. Инструкторам надо будет заменить представленные здесь сведения о Португалии соответствующей информацией о своей стране. | | |
| **Слайд №** | **Содержание:** | |
| Слайды 1 - 29 | Презентация «ПауерПойнт» (или подготовленная с помощью другой программы).  Слайды, демонстрирующиеся в этом разделе, приведены в качестве примера того, о чём может идти речь на местных практических занятиях (тренингах).  В идеальном варианте, на занятии, посвящённом доказательствам в электронной форме (электронным доказательствам), следует рассказать о международных правовых документах, подписанных или же ратифицированных каждым из государств, и о результатах работы по их переносу во внутригосударственное право.  Кроме того, необходимо дать описание видов следственных мер, предусмотренных национальным законодательством, а также объяснить важность соблюдения требований, предъявляемых к порядку собироания и обеспечения сохранности электронных доказательств.  Во второй половине занятия, ближе к концу, надо упомянуть, по мере возможности, о специфике национальных процессуальных норм, регламентирующих работу с электронными доказательствами. | |
| Слайд 2 | План занятия  Эта презентация состоит из трёх частей:   * в первой части рассказывается о процессуальных нормах, изложенных в «Будапештской конвенции»; * во второй части даётся описание процессуальных норм, присутствующих в национальном законодательстве; * в третьей части подводятся итоги усвоения материала, изложенного в двух предыдущих частях. | |
| Слайд 3 | По окончании этого занятия слушатели должны быть в состоянии объяснить относящиеся к его теме процессуальные нормы «Будапештской конвенции» и своего внутригосударственного законодательства. | |
| Слайд 5 | Часть первая – Процессуальные нормы «Будапештской конвенции»  Здесь необходимо особо подчеркнуть процессуальную важность «Будапештской конвенции». | |
| Слайд 6 | В соответствии со статьей 14 «Будапештской конвенции», содержащиеся в ней процессуальные нормы имеют весьма широкую сферу применения. Естественно, таковая распространяется на все перечисленные в этом международном документе виды расследуемых преступлений.  В то же время статья содержит ещё два дополнительных положения, значительно расширяющих сферу применения процессуальных норм конвенции, а именно:     * содержащиеся в конвенции процессуальные нормы могут быть применены к расследованию любого преступления, если таковое было совершено с использованием компьютерной системы; * содержащиеся в конвенции процессуальные нормы применимы также к собиранию доказательств в электронной форме (электронных доказательств), связанных с совершением какого бы то ни было преступления. Это значит, что потенциально любое преступление подпадает под действие процессуальных норм, изложенных в Конвенции о компьютерных преступлениях. | |
| Слайды 7 - 10 | В статьях 16 и 17 «Будапештской конвенции» описываются процессуальные нормы, призванные гарантировать оперативное обеспечение сохранности компьютерных данных и их санкционированное раскрытие. Оба этих положения крайне важны и имеют инновационный характер.  Обычные материальные улики, как правило, достаточно долговечны, в то время как электронные доказательства, физически существующие в виде цифровых данных, очень неустойчивы («волатильны») и могут весьма быстро исчезнуть.  Таким образом, статьей 16 вводится понятие «оперативного обеспечения сохранности» электронных данных, обозначающее принятие срочных мер обеспечения их целостности. Это сделано для того, чтобы у правоохранительных органов было время на получение соответствующих судебных ордеров на изъятие или же санкционированное раскрытие цифровых данных. При этом речь идёт как о содержащейся в них информации, так и о параметрах их передачи.  В обеспечении интернет-связи могут быть задействованы сразу несколько поставщиков интернет-услуг (провайдеров). Важно, чтобы у правоохранительных органов было право дать соответствующее указание любому провайдеру по маршруту передачи, обязующее его обеспечивать сохранность затребованных данных. Таким образом, в соответствии с положениями статьи 17 «Будапештской конвенции», от поставщика услуг может быть затребовано раскрытие параметров передачи данных в объемах достаточных для определения маршрута их следования в сети.  В статьях 16 и 17 «Будапештской конвенции» речь идёт о весьма специфических данных, необходимых в рамках особого рода следственных действий. Содержащиеся в них положения не следует путать с правовыми нормами, устанавливающими сроки хранения провайдерами параметров передачи данных. В соответствии с ними, поставщики интернет-услуг обязаны сохранять все сведения, относящиеся к параметрам передачи данных в течение определённого времени, на тот случай, если таковые будут востребованы правоохранительными органами. В «Будапештской конвенции» не содержится положений о сохранении этого рода сведений. | |
| Слайды 11 - 13 | Положения статьи 18 «Будапештской конвенции» также очень интересны. В соответствии с ними, каждая сторона конвенции должна принять законодательные меры, направленные на предоставление своим правоохранительным органам соответствующих полномочий, позволяющих им выдавать «ордера на получение данных». Этот судебный приказ может направляться органами правосудия как простым гражданам, так и поставщикам интернет-услуг с требованием предоставления компетентным органам данных, хранящихся в их компьютерных системах под их ответственность, или же сообщить имеющиеся у них абонентские данные о подписчиках интернет-услуг.  В соответствии с положениями «Будапештской конвенции», в «ордере на получение данных» должны быть указаны характер затребованных данных и пределы из раскрытия. Абсолютно ясно, что объемы затребованной следствием информации должны быть предварительно определены. Здесь речь идёт о запрещении «траулерного лова» частных компьютерных данных. Установление законом подобных рамок направлено на предупреждение злоупотребления этими новыми следственными полномочиями со стороны сотрудников правоохранительных органов. В мире материальных вещей досмотр / выемка имущества или же документов обычно направлены только на те материалы, которые напрямую связаны с расследуемым делом. В мире же цифровых данных оформление правовой нормой разрешения доступа ко всей информации, хранящейся на той или иной части аппаратного оборудования, сделало бы доступным все данные, имеющиеся на данном компьютере, в то время как они зачастую никак не связаны с расследуемым преступлением (например, когда речь идёт об электронной переписке) и затрагивают интересы третьих лиц.  Если коротко подвести итог всему вышеизложенному, то можно сказать, что статья 16 «Будапештской конвенции» (обеспечение сохранности данных) это, как бы, первый шаг, а 18 статья – второй. На этом этапе содержание сохранённых данных должно быть раскрыто органам власти. | |
| Слайды 14 - 19 | В статье 19 «Будапештской конвенции» речь идёт об обыске и выемке компьютерных данных.  В большинство национальных процессуальных норм включены общие положения о порядке проведения обыска и выемки, но не во всех содержатся специфические положения, регламентирующие вышеуказанные следственные действия в отношении компьютерных материалов. У многих судебных органов не возникает никаких вопросов, когда речь идёт об обычных процедурах обыска и выемки. Тем не менее, реальная жизнь учит нас, что при расследовании компьютерных преступлений следственные органы сталкиваются с ранее неизвестными проблемами, вызываемыми, например, взаимосвязанностью компьютерных систем.  Для решения этих новых проблем в «Будапештскую конвенцию» введены особые процессуальные нормы, регламентирующие порядок проведения обыска и выемки компьютерных материалов.  Например, в пункте 2 статьи 19 конвенции содержится одна из таких специфических норм. Она связана с возможным расширением пределов проведения обыска в том случае, если в ходе досмотра компьютерной системы следственные органы приходят к выводу о необходимости распространить его на другую компьютерную систему. В соответствии с вышеуказанным положением «Будапештской конвенции», когда уполномоченный орган власти на законных основаниях получает доступ к определённой компьютерной системе или же к её части, и когда во время их досмотра у него возникает обоснованное убеждение в том, что искомые данные хранятся в другой компьютерной системе на его же территории, таковой орган может «оперативно» распространить пределы обыска на другую компьютерную систему.  Говоря о выемке, необходимо особо выделить ряд моментов характерных для работы в новой цифровой среде: речь идёт о различных возможностях физического изъятия компьютерных данных в рамках вышеуказанного следственного действия.  В большинстве законодательств уже имеются нормы, регламентирующие порядок проведения обыска в материально-вещественном мире. Одновременно в них отсутствуют специфические положения, касающиеся новых и более эффективных существующих способов изъятия компьютерных данных.  В частности, в «Будапештской конвенции» содержится требование к подписавшим её государствам принять соответствующие законодательные меры, позволяющие в процессе санкционированной законом выемки:   * 1. производить физическое изъятие компьютерной системы;   2. производить копирование компьютерных данных в компьютере и сохранение полученной копии (что важно в случае хранения данных на основном сервере, когда физическое изъятие невозможно или же когда таковое может привести к слишком значительному посягательству на право доступа третьих лиц к этому серверу, например, если речь идёт о крупной компании);   3. обеспечивать целостность относящихся к расследуемому делу данных, хранимых в компьютере, и, наконец,   4. делать недоступными или же изымать такие компьютерные данные в компьютерной системе, доступ к которой уже был получен.   Последнее положение имеет важное значение, например, в тех случаях, когда физическое изъятие невозможно, но существует риск причинения серьезного вреда при получении третьим лицом доступа к этим данным.  За исключением простого изъятия данных, записанных на их собственном изначальном носителе, все вышеперечисленные процессуальные меры разработаны для специфического применения в киберсреде. | |
| Слайд 20 | Зачастую следственные органы нуждаются в получении более свежей информации по сравнению с той, что хранилась в памяти компьютерных систем. Сбор *в режиме реального времени* сведений о параметрах текущей передачи компьютерных данных позволяет вести расследование также в реальном времени. Об этом и идёт речь в статье 20 «Будапештской конвенции». Такого рода меры по внедрению в работу компьютерной системы требуют принятия особых законодательных норм. Таковые должны позволять правоохранительным органам собирать или же записывать данные в реальном времени с использованием соответствующих технических средств, а также предоставлять вышеуказанным органам полномочия по принуждению поставщиков интернет-услуг к сбору или же записи параметров передачи данных их пользователей, производящихся в режиме реального времени и нормальной работы.  Принятие такого рода следственных мер может оказаться очень важным, например, для установления источника сообщения с целью последующего выявления в реальном времени правонарушителя. | |
| Слайд 21 | Хотя и последняя в этом ряду, но не менее важная процессуальная норма содержится в статье 21 «Будапештской конвенции» и относится к перехвату информации, содержащейся в цифровых данных. Наряду со сведениями о параметрах передачи данных, правоохранительным органам иногда бывает необходимо знать реальное содержание сообщений, которыми обмениваются лица, подозреваемые в совершении преступления. В некоторых странах уже существуют соответствующие нормы, регламентирующие порядок перехвата телефонных разговоров, но не всеми разрешается органам перехватывать сообщения, идущие по другим каналам связи.  По этой причине в статью 21 «Будапештской конвенции» включены отдельные положения, позволяющие следственным органам перехватывать и записывать компьютерные данные в процессе их передачи.  В соответствии с положениями «Будапештской конвенции», применение перехвата данных, являющегося мощнейшей следственной мерой, разрешено только при расследовании ограниченного круга тяжких преступлений, список которых определяется национальным законодательством. | |
| Слайд 23 | Часть вторая – относящиеся к изучаемой теме процессуальные нормы в национальном законодательстве | |
| Слайды 24 - 31 | Инструкторам надо поместить здесь ссылки на нормы национального права. | |
|  | Практические занятия (проводятся при наличии необходимых условий)  Не предусмотрено. | |
|  | Проверка знаний  Инструктор должен проверить знания слушателей, задавая им конкретные вопросы по каждой из пройденных на занятии тем. | |
| Слайды 33 - 34 | Подведение итогов занятия/выводы  Инструктору необходимо подвести итоги / проверить знания слушателей, которые должны быть в состоянии:   * описать национальные правовые нормы, регламентирующие работу с доказательствами в электронной форме (электронными доказательствами); * описать совокупность соответствующих норм международной правовой системы (по мере возможности); * обсудить различные виды следственных мер, предусмотренные национальным законодательством, а также важность соблюдения требований, предъявляемых к порядку собирания и обеспечения сохранности электронных доказательств. * указать специфику национальных процессуальных норм, регламентирующих работу с электронными доказательствами, по сравнению с соответствующими положениями международной правовой системы. | |

|  |  |  |
| --- | --- | --- |
| Занятие 1.3.1 Обзор проделанной работы | | **Продолжительность: 30 минут** |
| **Перечень материалов, необходимых для проведения занятия:**   * ноутбук или ПК с операционной системой Windows 7 и с загруженным офисным пакетом приложений MS Office 2010; * проектор с экраном; * презентация «ПауерПойнт»; | | |
| **Цель:**  Цель этого занятия заключается в том, чтобы проанализировать проделанную за предыдущие дни работу, получить отклики аудитории и убедиться в том, что поставленные на этом занятии задачи были решены. | | |
| **Задачи:**   * определить, насколько хорошо они усвоили учебный материал, преподнесённый им в предыдущие дни; * выявить те области, к которым они должны вернуться ещё раз, чтобы довести свои знания до необходимого уровня. | | |
| **Введение**  Это занятие было подготовлено таким образом, чтобы позволить слушателям проверить, насколько хорошо они поняли материал, преподнесённый им в предыдущие дни, и оценить, насколько каждый из них готов самостоятельно ответить на все вопросы, вытекающие из задач пройденных занятий. Кроме того, для инструктора представляется возможность проконтролировать уровень знаний слушателей и выявить те области, которые нуждаются в углублённой проработке. | | |
| **Слайды №** | **Содержание:** | |
| **Слайды**  **1 - 12** | **Презентация «ПауерПойт»** (или же подготовленная с помощью другой программы)  Слайды этой презентации составлены с таким расчётом, чтобы помочь инструктору и слушателям провести обзор работы, проделанной за предыдущие дни. Со своей стороны, инструктор должен подвести её промежуточный итог, используя в качестве критерия оценки пункты учебной программы и задачи предыдущих занятий. | |
|  | **Практические занятия** (проводятся при наличии необходимых условий)  Не предусмотрено. | |
|  | **Проверка знаний**  Тренер должен проверить знания слушателей, задавая им конкретные вопросы по каждой из пройденных на занятиях тем. | |
|  | **Подведение итогов занятия/выводы**  Всё занятие построено таким образом, чтобы слушатели смогли проанализировать на нём работу, проделанную за предыдущие дни. Соответственно, никакого отдельного подведения итогов по каждой из пройденных тем проводить не требуется. | |
| Занятие 1.3.2 & 1.3.3 Доказательства в электронной форме (электронные доказательства) | | **Продолжительность: 120 – 90 минут** |
| **Перечень материалов, необходимых для проведения занятия:**   * ноутбук или ПК с операционной системой Windows 7 и с загруженным офисным пакетом приложений MS Office 2010; * проектор с экраном; * доступ в сеть Интернет (при наличии); * презентация «ПауерПойнт»; * образчики аппаратных средств ЭВМ (при наличии); * копия руководства по использованию электронных доказательств, созданного при финансовой поддержке программы ЕС «ОИСИН». | | |
| **Цель:** Цель этого занятия заключается в том, чтобы дать работникам суда и прокуратуры соответствующие знания, относящиеся к различным вопросам использования доказательств в электронной форме (электронных доказательств), а именно: виды электронных доказательств, с которыми они могут столкнуться, способы их получения и работы с ними на этапах расследования и судебного разбирательства уголовных дел, порядок их предъявление в судебном заседании. Также будут предоставлены дополнительные сведения о трудностях, возникающих при получении такого рода доказательств из иной юрисдикции. | | |
| **Задачи:**  По окончании занятия слушатели должны быть в состоянии:   * рассказать, какие существуют виды электронных доказательств; * изложить основные наиболее эффективные методы изъятия электронных доказательств и работы с ними; * определить трудности, возникающие при работе с данными, сохраняющимися на жестком диске компьютера после отключения питания, с данными в оперативной памяти включённого компьютера («короткоживущими данными»), а также с интернет-источниками электронных доказательств; * выявить проблемы с получением доказательств из иной юрисдикции; * обсудить вопросы допустимости использования электронных доказательств в судебном разбирательстве с точки зрения их подлинности, точности и полноты. | | |
| **Время** | **Содержание:** | |
| 30 минут  30 минут  60 минут    60 минут  30 минут | * Введение (изложение плана занятия и его задач) * Часть 1 – Что представляют собой электронные доказательства? * Часть 2 – Процессуальный порядок собирания электронных доказательств и обращения с ними; передовой опыт в этой области. * Часть 3 – Вопросы правового характера, возникающие в связи с изучаемой темой. * Подведение итогов занятия/выводы. | |
| **Введение**  Для ведения этого занятия инструкторам даётся лишь его общая структура, на основе которой они выстраивают учебный материал, подаваемый как часть более обширной программы. По своему содержанию она не может быть исчерпывающей и окончательной, так как наука и техника развиваются столь стремительно, что любой более или менее подробный с технической точки зрения отчёт устаревает уже к моменту своей публикации. В данном случае принципиально важно для обеспечения должного отправления правосудия добиться того, чтобы присутствующие на нём работники суда и прокуратуры в достаточной степени овладели технической стороной изучаемого предмета в тех пределах, которые им необходимы по работе. Таким образом, на этом занятии даётся общий обзор основных компьютерных технических средств и объясняется, какой интерес они представляют с точки зрения уголовного правосудия. В качестве наглядного материала прилагается презентация «ПауерПойнт», использование которой оставляется на усмотрение инструкторов.    На этом занятии слушатели будут ознакомлены с техническими средствами, используемыми преступниками для совершения противоправных деяний, а также правоохранительными органами для раскрытия таковых. Соответственно, работники суда и прокуратуры будут сталкиваться с вышеуказанным компьютерным оборудованием в своей работе.  Большинство исходных материалов, использованных на этом занятии, взято из документа о порядке изъятия электронных доказательств (выходные данные - 2002/OIS/014[[4]](#footnote-4)), подготовленного благодаря финансированию Европейской комиссии в рамках осуществляемой ею общей программы по обмену кадрами, их подготовке и сотрудничеству между правоохранительными органами стран ЕС (программы «ОИСИН»). Он был создан несколько лет назад и частично устарел. Там, где это относится к изучаемому предмету, приводимые сведения были обновлены для включения в план настоящих практических занятий. Этот документ разрабатывался прежде всего для нужд правоохранительного сообщества; тем не менее, изложенные в нём принципы и процессуальные нормы могут быть взяты на вооружение системой уголовного правосудия других стран. Положения, изложенные в вышеуказанном документе, применимы ко всем делам, расследование которых предполагает проведение выемки доказательств в электронной форме.  При толковании мер, предлагаемых в данном документе, каждое государство – член должно принять во внимание действующие на его территории правовые акты и законодательные нормы, а также приобщить к нему контактные данные своей экспертной группы.  Если какие-либо организации или же учреждения пожелают применить у себя рекомендуемые процессуальные нормы, то им необходимо для этого определить в своём штатном расписании лиц, персонально отвечающих за каждый шаг/действие по их внедрению. | | |
| **Слайд №** | **Содержание:** | |
| Слайд 1 | **Презентация «РауерПойнт»** (или подготовленная с помощью другой программы) | |
| Слайд 2 | План занятия  На слайде показана разбивка занятия на части. Инструктор должен тщательно, попунктно разобрать их, останавливаясь при необходимости на тех специфических аспектах изучаемого предмета, которые представляют особый интерес для той или иной части аудитории. Кроме того, ему необходимо объяснить, в какой форме будет осуществляться подача материала и когда предусмотрено время для взаимного обмена мнениями и вопросов. Инструктору следует подчеркнуть, что этот практикум (тренинг) задумывался как мероприятие, ведущееся в режиме взаимного диалога, и что поэтому он ожидает от слушателей активного участия. Кроме того, он должен объяснить, предусмотрен ли экзамен, в какой форме и будет ли какой-нибудь «проходной балл». (для этой экспериментальной программы проведение экзамена не предусмотрено). | |
| Слайд 3 | Важно, чтобы слушатели уяснили себе задачи занятия, которые должны соответствовать требованиям «SMART ». Их надо подробно объяснить аудитории с самого начала с помощью наглядной информации на соответствующем слайде. | |
| Слайд 6 | Часть первая – Что представляют собой доказательства в электронной форме (электронные доказательства) | |
|  | Виды и источники электронных доказательств  Примеры  Инструктору следует начать обсуждение вопроса с определения различных видов электронных доказательств. Для этого ему необходимо попросить слушателей рассказать о том, что им конкретно известно по этому поводу. Далее инструктору надо выписать на доске все перечисленные слушателями виды таких доказательств, дополнив их при необходимости недостающими. В полученном таким образом перечне должны присутствовать доказательства различные по своему местонахождению (жесткий диск, оперативная память, запоминающие устройства, интернет) и источникам (таковые перечислялись в разделе, посвящённом компьютерным техническим средствам). | |
| Слайд 8 | Определение  Как правило, определение доказательства содержится в местном законодательстве. Так как этот курс адресуется к широкой международной аудитории, то использующееся в нём определение имеет общий характер. Оно взято из юридического словаря Блэка. Инструкторам необходимо заменить его определением в том виде, в котором оно сформулировано в национальном законодательстве страны проведения занятий.  «Доказательством являются любого рода улики или же доказательственные материалы, законно представленные на судебном разбирательстве спора актом сторон посредством предъявления свидетельских показаний, записей, документов, вещественных доказательств, конкретных предметов и так далее, с целью склонения членов суда или же присяжных заседателей к убеждённости касательно предмета спора. Как правило, электронная информация допустима в качестве доказательства в рамках судопроизводства». | |
| Слайды 9 - 10 | В настоящее время не существует международно признанного определения электронного доказательства. Тем не менее, во всех странах есть законодательные нормы, содержащие предписания, в которых в той или иной форме имеются ссылки на *электронные доказательства.*  Одним из примеров «удобного» определения доказательства в электронной форме может быть следующее: «Имеющие значение для расследования информация или же данные, которые хранятся на электронных устройствах или же передаются с их использованием».  ([www.nij.gov](http://www.nij.gov)[/topics/forensics/evidence/digital/digital-glossary.htm](http://www.nij.gov/topics/forensics/evidence/digital/digital-glossary.htm))  Здесь инструктору необходимо привести то определение электронного доказательства, которое фигурирует в национальном законодательстве станы, где проводятся практические занятия.  Борьба с современными формами преступности предполагает оказание помощи со стороны экспертов и специалистов в анализе доказательств и их верной интерпретации на этапах расследования дела и его судебного разбирательства. | |
| Слайд 12 | Источники и виды доказательств в электронной форме (электронных доказательств)  Здесь нет необходимости в возвращении к полному списку источников и видов электронных доказательств, приведённому в том разделе курса, где речь шла о технических компьютерных средствах. Таким образом, инструктору следует для повторения пройденного материала привести тот перечень, который был дан в начале этого занятия.  Источниками электронных доказательств могут быть любые электронные устройства. На этом этапе инструктор может остановиться на доказательной силе электронных доказательств на различных электронных устройствах и на их роли в расследовании конкретных дел.  Рассматриваемые виды электронных доказательств могут существовать в форме:   * статических данных (на жестком диске компьютера) * данных в реальном времени (в оперативной памяти включённого компьютера); * интернет-данных. | |
| Слайд 13 | Свойства доказательств в электронной форме (электронных доказательств)  Электронные доказательства обладают многими свойствами, ставящими под вопрос их допустимость в качестве традиционных средств доказывания. В большинстве случаев с ними работают и обращаются как с обычными уликами, в то время как ключевым условием успешного ведения следствия и судебного разбирательства в таких случаях является осознание работниками суда и прокуратуры специфики электронных доказательств и возникающих в связи с этим дополнительных проблем.  Как видно из примеров, приведённых в рамках этого курса, многие из затронутых вопросов имеют отношение как к электронным, так и к обычным доказательствам. Тем не менее, между ними есть некоторые различия, которые следует подчеркнуть. Действительно, доказательства в электронной форме:   * **неустойчивы («волатильны»):** * они легко поддаются изменению/искажению, * могут быть недолговечными; * **по своей природе:** * могут требовать специальных навыков для получения доступа к ним, * могут требовать заключения эксперта для их толкования, * могут требовать применения средств принуждения для получения доступа к ним, или же их использование может быть ограничено; * **по местонахождению:** * могут быть неразрывно связаны с материалами, не имеющими отношения к доказыванию, * могут находиться вне пределов юрисдикции; * **по своему объему:** * могут потребовать выявления доказательственных материалов на запоминающем устройстве * и отделения таковых от общей массы данных, не имеющих отношения к расследуемому делу. | |
| Слайд 14 | Вопросы, возникающие в связи с особенностями электронных доказательств  В связи с особыми свойствами доказательств в электронной форме возникает ряд вопросов, которые следует выделить особо, проиллюстрировав их конкретными примерами. Вопросы эти связаны со следующими моментами:   * показания с чужих слов, свидетельство, основанное на слухах, * регистрация деловых операций, * автоматизированные процессы, * смешанные доказательства, * объемы данных, * заключение эксперта. * **Неустойчивость.** Некоторые цифровые данные, обрабатываемые компьютерной системой, в высшей степени неустойчивы. Кроме того, они могут быть легко удалены или же изменены. Эта их особенность важна не только при оценке электронных доказательств, но и при осуществлении их сбора. Как правило, данные, хранящиеся только на ОЗУ (в оперативной памяти компьютерной системы) будут потеряны после отключения электропитания, если только не применить специальные технические средства для предупреждения этого. Так как информация в оперативной памяти компьютерной системы может иметь очень большую важность для следствия, технические методы собирания этих доказательств, отличаются от традиционно используемых для получения обычных доказательных материалов. * **Подверженность изменениям.** Цифровые данные подвержены искажению. Один из основополагающих принципов компьютерно-технической экспертизы заключается в обеспечении целостности и сохранности доказательств, предъявляемых в электронной форме. Полное протоколирование/фиксация всех следственных действий, проводящихся с электронными доказательствами, а также тщательное соблюдение порядка обращения с ними с целью обеспечения целостности и сохранности содержащихся в них компьютерных данных чрезвычайно важны для того, чтобы избежать подозрений в фальсификации таковых доказательств. В результате эксперты в области компьютерной криминалистики изыскивают возможности замены следственных действий по собиранию электронных доказательств, приводящих к искажению файлов на компьютере подозреваемого лица, на более тонкие методы работы. * **Децентрализованное хранение данных.** Доступность ШПД (широкополосного доступа в интернет) и удаленных серверов хранения данных повлияли на способы хранения информации. Если раньше при поиске компьютерных данных следственные органы могли сосредоточиться на жилище подозреваемого лица, то сегодня им надо учитывать тот факт, что искомая цифровая информация может физически храниться за рубежом, оставаясь при необходимости доступной подозреваемому на расстоянии. * **Темпы научно-технического прогресса.** Развитие науки и техники продолжается ускоренными темпами. Значительное количество научно-технических достижений ставит новые задачи перед специалистами судебной экспертизы. Подобное развитие ситуации требует постоянного повышения квалификации сотрудников, ответственных за собирание доказательств и за поддержание в должном состоянии экспертных технических средств таким образом, чтобы они отвечали современным требованиям. Разработка новых версий операционных систем и других видов программной продукции может привести к появлению иных форматов цифровых данных, потенциально представляющих интерес для следственных органов. Подобного же рода изменения происходят и в области создания новых аппаратных средств. Если раньше данные хранились на дискетах, то сегодня следственные органы должны учитывать возможность записи важной информации, скажем, на «МР3-плеерах» или же в памяти часов со встроенным запоминающим устройством. | |
| Слайды 18 - 19 | Часть вторая – Процессуальные нормы, регламентирующие порядок работы и обращения с электронными доказательствами; передовой опыт в этой области. | |
|  | Материал, изложенный в этой части занятия, во многом позаимствован из вышеуказанного руководства ЕС о порядке изъятия электронных доказательств. В нём представлены многочисленные подробности, позволяющие инструктору выстроить занятие. Таковые детально излагаются в руководстве для инструкторов и в сжатом виде попунктно перечисляются в пояснительных слайдах. В зависимости от пожеланий слушателей инструктору надо самому решить, насколько подробным должно быть изложение этого материала для выполнения поставленных задач.  Положения, изложенные в этом руководстве, применимы ко всем делам, расследование которых предполагает проведение выемки доказательств в электронной форме.  При толковании мер, предлагаемых в данном документе, каждое государство – член должно принять во внимание действующие на его территории правовые акты и законодательные нормы, а также приобщить к нему контактные данные своей экспертной группы.  Если какие-либо организации или же учреждения пожелают применить у себя рекомендуемые процессуальные нормы, то им необходимо для этого определить в своём штатном расписании лиц, персонально отвечающих за каждый шаг/действие по их внедрению. | |
| Слайд 20 | ОСНОВНЫЕ ПРИНЦИПЫ  При работе с доказательствами в электронной форме (электронными доказательствами) необходимо неукоснительно соблюдать следующие основные принципы:   1. присутствие на месте производства следственного действия, 2. обеспечение целостности и сохранности данных, 3. обязательность ведения протокола следственного действия, 4. экспертная поддержка, 5. необходимость специальной подготовки сотрудников, 6. соблюдение закона и приверженность принципам,   Далее следует объяснение вышеизложенных принципов. | |
| Слайд 21 | 1. **Присутствие на месте производства следственного действия**   Принцип: *Уполномоченный сотрудник никогда не должен находиться на месте производства следственного действия один.*  Необходимо, чтобы по меньшей мере двое сотрудников участвовали в следственном действии. С одной стороны, это позволяет им чувствовать себя увереннее, а с другой, отслеживать больше подробностей. Задействованные сотрудники должны планировать и координировать свою совместную работу. При возникновении непредвиденных ситуаций им так легче будет реагировать на них, так как «одна голова хорошо, а две – лучше». | |
| Слайд 22 | 1. **Обеспечение целостности и сохранности данных**   Принцип: *Никакие действия, предпринимаемые правоохранительными органами или же их сотрудниками, не должны вносить изменений в электронные устройства или же средства связи, на которые можно будет впоследствии опереться в суде.*  При работе с электронными устройствами и данными, состояние таковых должно оставаться неизменным. Это требование относится как к аппаратным средствам, так и к программному обеспечению. Отвечающий за проведение этого следственного мероприятия сотрудник несёт ответственность за целостность и сохранность материалов и оборудования, изъятых на месте происшествия и направляемых в камеру хранения вещественных доказательств. Таким образом обеспечивается их доказательная сила вплоть до предъявления в судебном заседании | |
| Слайд 23 | 1. **Обязательность составления протокола следственного действия**   Принцип: *При совершении следственного действия с электронным доказательством должен быть составлен и сохранён соответствующий протокол или иной письменный акт, в котором необходимо зафиксировать все действия, произведённые с вышеуказанным доказательством. Независимая третья сторона должна быть в состоянии изучить вышеуказанные действия и прийти к тому же результату.*  Совершенно необходимо тщательно всё фиксировать таким образом, чтобы позднее третья сторона могла восстановить последовательность всех действий, предпринятых на месте обыска/выемки первыми прибывшими туда сотрудниками. Этим будет обеспечена доказательная сила электронной улики в суде. Все действия, связанные с обнаружением, изъятием, хранением и транспортировкой электронного доказательства, следует полностью зафиксировать в протоколе. Таковой, в свою очередь, должен сохраняться и быть доступным для просмотра. | |
| Слайд 24 | 1. **Экспертная поддержка**   Принцип: *Если предполагается, что в ходе полицейской операции может быть обнаружено электронное доказательство, то ответственный за её проведение сотрудник полиции должен своевременно оповестить об этом соответствующего эксперта/вневедомственного специалиста.*  В рамках следственных действий, предполагающих проведение обыска/ выемки электронных доказательств, может оказаться необходимым проконсультироваться с вневедомственным экспертом. Таковые специалисты должны быть ознакомлены с вышеизложенными принципами и отвечать следующим требованиям:   * иметь необходимую подготовку и опыт работы по специальности; * обладать необходимыми следственными навыками и юридическими познаниями; * быть в курсе обстоятельств расследуемого дела и * обладать соответствующими редакционными способностями (для дачи как устного, так и письменного экспертного заключения). | |
| Слайд 25 | 1. **Необходимость специальной подготовки сотрудников**   Принцип: *Первые прибывающие на место происшествия сотрудники должны иметь соответствующую подготовку, позволяющую им самостоятельно провести обыск и выемку электронных доказательств за отсутствием эксперта.*  Бывают чрезвычайные ситуации, когда первым прибывшим на место сотрудникам необходимо самим собрать электронные доказательства и/или осуществить доступ к исходным данным, хранящимся в электронном устройстве или же на цифровом накопителе. В подобных случаях такие сотрудники должны предварительно пройти специальную подготовку с тем, чтобы они могли выполнить свои обязанности должным образом и объяснить значение и последствия своих действий. | |
| Слайд 26 | 1. **Соблюдение закона и приверженность принципам**   Принцип: *Расследующий дело орган и его сотрудники несут ответственность за обеспечение соблюдения закона, общих судебных и процессуальных норм, а также вышеперечисленных принципов, которым они должны быть привержены. Это положение применимо также к хранению электронных доказательств и к доступу к ним.*  При толковании мер, предлагаемых в данном документе, каждое государство – член должно принять во внимание действующие на его территории правовые акты и законодательные нормы.  Разработанная Советом Европы Конвенция о компьютерных преступлениях является одним из важнейших международных правовых документов. В настоящее время она открыта для подписания государствами – членами С. Е., а также странами, принявшими участие в её подготовке. Кроме того, конвенция открыта для присоединения к ней и других государств. | |
| Слайд 28 | Способы производства выемки  Рассмотрение различных способов производства выемки / изъятия доказательств в электронной форме (электронных доказательств) является важной частью настоящих практических занятий. У каждого из этих способов есть свои характерные черты, риски и результаты. Инструктор должен достаточно детально довести их до аудитории таким образом, чтобы слушатели осознали, насколько соблюдение описанного ниже порядка помогает судьям и прокурорам выполнять свои профессиональные обязанности. Нижеизложенные сведения должны помочь инструкторам в изложении соответствующего учебного материала.  Если говорить обобщенно, то можно сказать, что существует четыре способа производства выемки электронных доказательств:   1. путём конфискационного изъятия электронного оборудования и носителей информации; 2. путём копирования всего содержимого запоминающих устройств компьютерной системы (методом создания полного образа ЗУ); 3. путём конфискационного изъятия электронных носителей резервных копий данных; 4. путём избирательного копирования данных; 5. собирание доказательств в интернете.   Эти различные способы производства выемки / изъятия электронных доказательств рассматриваются в нижеследующих разделах. Следует отметить, что в рамках одного следственного действия по выемке возможны различные комбинации вышеперечисленных способов производства изъятия. Например, в той или иной конкретной ситуации может оказаться необходимым конфисковать как электронное оборудование, так и электронные носители резервных копий. | |
| Слайд 29 | 1. **Конфискационное изъятие электронного оборудования и носителей информации**   Этот способ производства выемки / изъятия может применяться в тех случаях, когда:   * объем оборудования, подлежащего конфискационному изъятию, невелик (например, автономный компьютер или небольшая компьютерная сеть в квартире подозреваемого лица); * отсутствует опасность того, что конфискация оборудования может повлечь серьёзные финансовые потери или иной ущерб; * когда конфискационное изъятие абсолютно необходимо в связи со специфическим характером совершенного правонарушения; * когда конфискационное изъятие необходимо / обязательно с целью прекращения преступной деятельности, осуществляемой с использованием конфискованного оборудования.   Преимущества этого способа производства выемки / изъятия следующие:   * обычно изъятие может быть произведено без помощи эксперта на месте; * на него, как правило, не уходит много времени; * в результате электронное доказательство оказывается под контролем следственных органов; * содержимое изъятого может быть проанализировано в подконтрольной обстановке.   Недостатки этого способа производства выемки / изъятия следующие:   * существует опасность повреждения оборудования; * существует опасность причинения вреда лицам, никак не связанным с расследуемым преступлением; * существует опасность того, что конфискационное изъятие оборудование станет препятствием для осуществления деятельности, не связанной с расследуемым преступлением.  1. **Копирование всего содержимого ЗУ компьютерной системы**   Этот способ производства выемки / изъятия, иногда называемый «способом зеркального отражения», предполагает использование специальных технических средств для создания полного образа (то есть, точной копии, «дубликата») содержимого запоминающих устройств (ЗУ) компьютерного оборудования или же цифровых накопителей на внешних носителях информации.  Этот способ производства выемки / изъятия может применяться в тех случаях, когда:   * объем оборудования, подлежащего конфискационному изъятию, значителен (например, когда речь идёт о малом или же среднем предприятии); * существует опасность серьёзных финансовых или иных потерь в результате бездействия / отсутствия оборудования (например, если ИТ-система рассматривается подозреваемым или же третьим лицом как жизненно необходимая); * когда конфискационное изъятие не является абсолютно необходимой мерой в связи со специфическим характером совершенного правонарушения;   Преимущества этого способа производства выемки / изъятия следующие:   * незначителен риск повреждения оборудования; * незначителен риск причинения вреда лицам, никак не связанным с расследуемым преступлением; * незначителен риск того, что конфискационное изъятие оборудования станет препятствием для осуществления деятельности, не связанной с расследуемым преступлением; * содержимое изъятого может быть проанализировано в подконтрольной обстановке.   Недостатки этого способа производства выемки / изъятия следующие:   * на месте её проведения необходимо иметь специальные технические средства; * на месте её проведения обычно необходима помощь эксперта; * существует опасность того, что часть доказательных материалов останется незамеченной; * на него, как правило, уходит много времени; * имеющее отношение к делу оборудование остаётся неподконтрольным правоохранительным органам.  1. **Конфискационное изъятие электронных носителей резервных копий данных**   Этот способ производства выемки / изъятия может применяться в тех же случаях, что и копирование всего содержимого ЗУ компьютерной системы, особенно если конфискационному изъятию подлежат большие объемы оборудования и данных (например, если речь идёт о больших компьютерных сетях с использованием мощных ЭВМ).  Преимущества здесь те же, что и при копировании всего содержимого ЗУ компьютерной системы с помощью создания полного образа копируемой информации, описанного в разделе 2 (практически, в этом случае отсутствует риск нанесения ущерба или вреда). Дополнительными преимуществами этого способа производства выемки / изъятия являются следующие:   * на месте её проведения специальных техсредств не требуется; * на месте её проведения можно обойтись без столь трудоёмких операций, как создание полного образа копируемой информации, занимающего много времени;   Недостатки этого способа производства выемки / изъятия следующие:   * на месте её проведения обычно необходима помощь эксперта; * обычно необходима помощь местного системного администратора; * существует опасность того, что часть доказательных материалов останется незамеченной (заранее никогда не известно, насколько полно сохранена информация на резервных копиях); * имеющее отношение к делу оборудование остаётся неподконтрольным правоохранительным органам.  1. **Избирательное копирование данных**   Этот способ производства выемки / изъятия может применяться только в исключительных случаях, когда ни один из вышеперечисленных способов использовать невозможно, то есть когда только выборочные (наиболее важные имеющие отношение к делу) данные могут быть скопированы с целью их последующего изучения. Помощь эксперта на месте проведения выемки обязательна.  Преимущества и недостатки этого способа те же, что и при конфискационном изъятии электронных носителей резервных копий. Его дополнительным недостатком является то, что невозможно произвести восстановление истории операций, осуществлённых с помощью компьютерной системы, что действительно ограничивает важность этого способа для следствия. Кроме того, надо особо позаботиться об обеспечении доказательной силы изъятой таким образом информации.     1. **Собирание доказательств в интернете**   Собирание доказательств в интернете является важной составляющей расследования и требует особых знаний, навыков и технических средств. В этом курсе не затрагиваются специфические вопросы, касающиеся сбора такого рода данных. Можно лишь подтвердить, что все перечисленные в нём основные принципы в равной степени относятся и к этой теме. Существуют различные способы собирания доказательств в Интернете, которые можно приблизительно разбить на две группы: 1) сбор данных в открытых источниках и 2) сбор, осуществляемый скрытно. Эта тема имеет свои правовые и процессуальные аспекты, которые сознательно здесь не рассматриваются как преждевременные. Она будет освещена в рамках расширенной программы практических занятий (тренинга). | |
| Слайды 30 - 40 | процессуальный порядок проведения выемки ДОКАЗАТЕЛЬСТВ В ЭЛЕКТРОННОЙ ФОРМЕ (электронных доказательств)  Как было указано во введении, документ, подготовленный при финансовом содействии программы ЕС «ОИСИН», главным образом посвящен вопросам процессуального порядка проведения выемки электронных доказательств. После поиска и обнаружения это следственное действие предполагает изъятие и фиксацию электронных доказательств. Оно состоит из следующих этапов, описанных в приведённых ниже разделах:   1. подготовка к проведению выемки (раздел [1](#_Lesson_No:_1.3.2)), 2. обеспечение безопасности на месте проведения обыска/выемки (раздел 2), 3. фиксация хода выемки на месте её проведения (раздел 3), 4. изъятие электронных доказательств (раздел 4), 5. упаковка, транспортировка и хранение электронных доказательств (раздел 5).   При разработке процессуального порядка, описанного в приведённых ниже разделах, были учтены основополагающие принципы изучения информационного пространства, содержащиеся в рекомендациях Совета Европейского союза.   1. **Подготовка к проведению выемки**   На этапе предварительного расследования, при получении ордера на обыск, необходимо установить могут ли при его проведении быть обнаружены какие-либо доказательстве в электронной форме (электронные доказательства), имеющие отношение к расследуемому делу. Если да, то руководитель оперативно-следственной группы должен без промедления оповестить об этом местное подразделение восстановления данных и/или вневедомственных экспертов. Прежде всего, необходимо решить, какой способ производства выемки выбрать (см. описание способов производства выемки на слайде 28). Следует заблаговременно с помощью специалистов собрать как можно больше сведений следующего характера:   * данные об используемых аппаратных средствах, операционной системе, программном обеспечении, приложениях и электронных носителях информации, * информация об используемых сетях и средствах связи (наименование провайдера[[5]](#footnote-5), характеристики линии телефонной/факсимильной связи, тип модема, наличие локальной сети[[6]](#footnote-6), характеристики сетевого оборудования и т. д.), * лицо, ответственное за работу компьютерной системы и/или сети (например, есть ли свой системный администратор или же его функции выполняет посторонняя компания), * каковы предположительно объёмы оборудования, подлежащего изъятию при выемке (соответствующий способ производства выемки приведён в разделе 1), * каков объем данных, подлежащих копированию (соответствующий способ производства выемки приведён в разделах 2 и 4), * есть ли в компьютерной системе электронные носители резервных копий данных (соответствующий способ производства выемки приведён в разделе 3).   На подготовительном этапе необходимо:   * убедиться в получении всех необходимых разрешений на проведение выемки электронных доказательств (например, получить ордер на обыск в соответствии со всеми требованиями действующего законодательства); * собрать максимум информации об информационно-вычислительной системе, подлежащей изъятию (см. выше); * сформировать оперативную группу (при включении в её состав, при необходимости, и специалистов со стороны); * поставить перед каждым её членом конкретную задачу; * разъяснить членам группы, как выполнять поставленные перед ними задачи (предварительно все они должны пройти специальную базовую подготовку); * обеспечить наличие технических средств, необходимых для производства выемки (логистическое обеспечение).   Как указывалось выше, все совершаемые следственные действия должны соответствовать требованиям внутриведомственных нормативных документов, а также положениям законов Европейского союза, конкретного государства, под юрисдикцией которого находится место проведения выемки, и местного законодательства.  Личный состав оперативной группы, производящей выемку  Если заранее известно, что на месте проведения обыска могут быть обнаружены доказательства в электронной форме (электронные доказательства), следует включить в состав оперативной группы сотрудников, прошедших специальную подготовку и имеющих навыки поиска и изъятия вычислительной техники и электронных доказательств. В некоторых случаях, может быть необходимо проконсультироваться с вневедомственным экспертом (см. также раздел 4). Например, если компьютерная система обслуживается внешним системным администратором или компанией, можно рассмотреть возможность привлечения их в качестве cвидетелей-экспертов (при условии, что таковые не являются подозреваемыми лицами по делу). Минимальное требование к личному составу состоит в том, чтобы оперативные работники, оказывающиеся первыми на месте проведения обыска, прошли предварительную спецподготовку и обладали базовыми навыками изъятия электронных доказательств.  Подбор личного состава оперативной группы и постановка задач её членам должны осуществляться в зависимости от этапа проведения выемки (см. также начало слайда 30). Этапы этого следственного действия и соответствующие им задачи описаны в нижеследующих разделах (2-5).  Всех членов группы следует должным образом проинструктировать по поводу того, как выполнять поставленные перед ними задачи. Например, они должны знать, при каких обстоятельствах можно обращаться с электронными доказательствами как с обычными вещественными, а когда необходимо использовать особые меры предосторожности при работе с ними (например, им надо знать, что при снятии отпечатков пальцев с электронных устройств нельзя применять алюминиевую пудру). Кроме того, им должно быть известно, что в определённых ситуациях необходимо обратиться в экспертную группу, контактные данные которой должны быть им известны заранее.  Технические и инструментальные средства произведения выемки  Для проведения изъятия электронных доказательств могут потребоваться специальные инструменты и технические средства, перечень которых меняется по мере развития науки и техники. Ниже прилагается базовый набор основных технических и инструментальных средств, которые могут понадобиться при проведении обыска и выемки. Их наличие у личного состава оперативной группы должно быть гарантировано лицом, отвечающим за её материально-техническое обеспечение.   * Инструменты для разборки и демонтажа: * отвертки (плоская, крестовая, а также специальные от производителя, например, Compaq, Macintosh); * наконечники (шестигранные, типа Торкс и защищенного типа); * плоскогубцы (стандартные и тонкогубцы); * кусачки (для удаления кабельных стяжек); * маленькие щипчики. * Средства фиксации хода следственного действия: * протокол обыска и выемки (опись имущества); * этикетки и наклейки (для маркировки и идентификации составных частей системы, в том числе проводов и разъёмов); * этикетки для кабелей; * этикетки для вещественных доказательств (со шнуровкой и самоклеющиеся); * другие необходимые средства; * несмываемые цветные маркеры (для кодировки и идентификации изъятых предметов); * фотоаппарат и/или видеокамера (для фотографирования предметов и изображений на экране). * Упаковочные материалы и транспортная тара: * антистатические мешки (для защиты изымаемого оборудования, типа печатных плат; следует избегать материалов, генерирующих / накапливающих статическое электричество, таких как полиэтиленовые мешки); * антистатическая пузырчатая пленка; * кабельные стяжки (для крепления кабелей); * пакеты и упаковочная плёнка для доказательств; * коробки для упаковки дискет, для JAZ/ZIP съёмных дисков, для DVD, или для компакт-дисков; * упаковочные материалы (следует избегать материалов, генерирующих / накапливающих статическое электричество, таких как пенополистирол или пенопласт); * упаковочные картонные коробки или прочные ящики различных размеров (при наличии оригинальной упаковки использовать следует именно её). * Средства связи: * мобильный телефон или другие средства связи для получения консультаций (не следует использовать их в непосредственной близости от компьютерного оборудования); * контактная информация для поддержки (например, номера телефонов экспертной лаборатории). * Другие принадлежности: * маленький фонарик с кронштейном; * перчатки; * ручная тележка; * широкие резиновые ленты; * увеличительное стекло (лупа); * бумага для принтера; * диск для копирования данных и/или компакт-диск (если проведено обучение по его использованию для целей компьютерной криминалистики); * неиспользуемые дискеты; * Транспортные средства (для доставки на место проведения обыска/выемки и обратно оперативной группы с техническими и инструментальными средствами, а также изъятых доказательств).  1. **Обеспечение безопасности на месте проведения обыска/выемки**   Действуя в соответствии с юрисдикционными нормами, лица, оказывающиеся первыми на месте производства обыска/выемки, должны обеспечить безопасность всех присутствующих при этом лиц и целостность всех находящихся там доказательственных материалов, то есть, как обычных вещественных доказательств, так и доказательств в электронной форме (электронных доказательств).  Этот этап включает в себя следующие действия:   * соблюдая юрисдикционные нормы, обеспечить безопасность работы оперативной группы на месте совершения преступления: * удалить всех присутствующих из зоны непосредственной близости к месту изъятия доказательств (включая оборудование и источники электропитания); * принять меры физической и электронной защиты данных: * обнаружить, обеспечить сохранность, внести в протокол и сфотографировать все устройства, содержащие недолговечные данные; * вести наблюдение за потенциально подозрительными и иными лицами с целью предупреждения искажения или же уничтожения улик; * не выпускать из поля зрения компоненты ИТ-инфраструктуры с целью предупреждения искажения или же уничтожения улик; * обнаружить и внести в протокол другие относящиеся к делу электронные компоненты, не подлежащие изъятию; * обнаружить, пометить и внести в протокол телефонные и сетевые линии связи, к которым подключены изымаемые устройства; * решить, какие дополнительные доказательные данные необходимо снять с изымаемых устройств (например, следы ДНК, наркотических или же легковоспламеняющихся веществ, отпечатки пальцев и т. д.); * при обращении с такого рода доказательственными материалами, следует выполнять общие процессуальные правила, изложенные в соответствующих справочных руководствах; * кроме того, следует отложить использование в этих целях методов, которые могут привести к уничтожению содержащихся на изъятых носителях электронных данных, вплоть до фиксации таковых в качестве доказательств; * по окончании изъятия электронных доказательств снять латентные отпечатки пальцев с клавиатуры, компьютерной «мыши», дискет, лазерных дисков и других компьютерных компонентов, на которых могут оставаться скрытые отпечатки пальцев или же другие материальные доказательства, которые необходимо зафиксировать; * не следует использовать алюминиевую пудру для снятия отпечатков пальцев с носителей электронной информации, так как при этом могут быть повреждены компоненты компьютерной системы и сами данные; * осмотреть место проведения обыска с целью обнаружения не электронных доказательств, которые могут быть связаны с расследуемым делом, а именно: * блокнотов с паролями доступа и другими рукописными записями, * листов бумаги со следами вдавленности в местах рукописного текста; * инструкций по работе с аппаратным оборудованием и программным обеспечением; * календарей и ежедневников; * текстов или графических компьютерных распечаток; * фотографий или * документов, содержащих информацию личного характера, которая в дальнейшем может быть полезна для взлома паролей доступа (таковая, в большинстве случаев, напрямую связана с личной жизнью и близким окружением пользователей; например, это может быть номерной знак автомобиля, даты рождения близкого человека или детей, их телефонные номера, любимые занятия и т. д.); * провести предварительный опрос: * выявить и установить личность всех лиц (свидетелей, субъектов опроса и др.) на месте проведения обыска/выемки в момент их входа в помещение, выяснить и зафиксировать их местонахождение в помещении; * при проведении опроса необходимо использовать специальные формуляры/вопросники для записи сведений, полученных от опрашиваемых лиц; * руководствуясь внутриведомственными нормативными документами и положениями действующего законодательства, получить от опрашиваемых лиц сведения следующего характера: * предназначение того или иного устройства/системы (например, учет использования системных ресурсов); * кто является владельцем/пользователем тех или иных устройств/систем, обнаруженных на месте проведения обыска/выемки, а также какие используются при их включении пароли доступа (см. ниже), имена пользователей/«логины», какая фирма обеспечивает выход в интернет (интернет-провайдер); * любые иные пароли доступа к компьютерной системе, программам или же данным. Не следует забывать о том, что на одном рабочем месте может использоваться множество паролей доступа, например, к BIOS, к системе, к списку деловых партнёров, для выхода в локальную сеть или в интернет, для пользования приложениями и электронной почтой (кроме того, пароли могут существовать в виде кодовых фраз для шифрования в системе PGP, маркеров доступа или же программ-планировщиков); * какие существуют иные способы обеспечения безопасности доступа к компьютерной системе или же схемы самоуничтожения данных; * другие места хранения данных, кроме жесткого диска компьютерной системы; * любая эксплуатационная и техническая документация к аппаратным средствам и программному обеспечению, установленному на компьютерной системе.  1. **Фиксация хода и результатов выемки на месте её проведения**   Фиксация ведётся постоянно в течение всего производства следственного действия выемки на месте его проведения. Чрезвычайно важно точно зафиксировать местонахождение и состояние компьютеров, электронных носителей информации, других электронных устройств и обычных вещественных доказательств. В предыдущих и следующих разделах главы даются более подробные указания касательно того, что конкретно должно быть зафиксировано. В этом разделе приводится лишь общий обзор этих инструкций.  В общем и целом, подлежат фиксации следующие моменты (в процессе изъятия этот список может быть расширен):   * место проведения выемки: * составить эскизный план компьютерной системы, включая положение «мышки» и месторасположение её компонентов, вплоть до «мышки»; * сфотографировать / заснять на видео / зафиксировать всё место проведения выемки[[7]](#footnote-7) (если возможно, с охватом в 360 градусов); * компьютерные системы и их электронные компоненты / устройства / оборудование:   - фиксации подлежат:   * подробные реквизиты всего обнаруженного оборудования, относящегося к расследуемому делу (то есть, производитель, марка, серийный номер); * техническое состояние и месторасположение каждой компьютерной системы, содержащей или же включающей в себя электронные доказательства (указать, включено устройство, выключено или же находится в режиме ожидания); * все входящие и исходящие соединения (кабельные и беспроводные) между компьютером и другими устройствами; для этого необходимо: * пометить этикетками все порты и кабельные соединения (включая соединения периферийных устройств) таким образом, чтобы впоследствии можно было точно собрать всю систему обратно; * пометить отдельными этикетками неиспользованные порты соединения; выявить наличие компоновочного блока портативного компьютера в поисках других электронных носителей информации; * подробно зафиксировать состояние экрана на момент проведения следственного действия: * сфотографировать переднюю часть компьютера с экраном и другими компонентами; * сделать записи касательно того, что изображено на экране; * произвести видеосъемку экрана с действующими программами; максимально полно зафиксировать всеми имеющимися средствами то, что отображается на экране компьютера. * зафиксировать другие, не подлежащие изъятию электронные компоненты, которые могут относиться к расследуемому делу; * сведения от лиц, находящихся на месте проведения выемки: * опросить вышеуказанных лиц и вписать их ответы в заранее подготовленный формуляр вопросника; * подлежат фиксации: * личные данные всех присутствующих в обыскиваемом помещении; * личные данные всех пользователей компьютерной системой/оборудованием, относящихся к расследуемому делу; * замечания, комментарии, сведения, исходящие от пользователей/владельцев компьютера и свидетелей. * действия, предпринимаемые на месте проведения обыска/выемки: * составить протокол следственных действий/выемки с описанием всех произведённых следственных действий, а также с указанием даты и точного времени их проведения.     В раскрытии преступлений, совершенных с использованием вычислительной и электронной техники, большую роль могут играть также и изъятые в ходе выемки обычные («не электронные») вещественные доказательства. Соответственно, необходимо позаботиться о своевременном обнаружении таких доказательств, изъятии и обеспечении их сохранности. Кроме того, вспомогательные материалы, облегчающие изучение электронных доказательств, могут существовать в виде: блокнотов с паролями доступа и другими рукописными записями, листов бумаги со следами вдавленности в местах рукописного текста, инструкций по работе с аппаратным оборудованием и программным обеспечением, календарей и ежедневников, текстов или графических компьютерных распечаток, фотографий. Следует обеспечить их сохранность для дальнейшего анализа. По большей части, эти материалы находятся в непосредственной близости от компьютера или же связанных с ним аппаратных средств. Обнаружение, выемка, обеспечение сохранности и фиксация доказательств должны производиться при строгом соблюдении положений внутриведомственных нормативных документов и действующего законодательства.   1. **Упаковка, транспортировка и хранение электронных доказательств.**   Компьютер и связанные с ним электронные компоненты отличаются непрочностью и повышенной чувствительностью к разного рода внешним воздействиям: температуре, уровню влажности, вибрации, ударам, присутствию статического электричества и источников электромагнитного излучения, а также к некоторым штатным операциям (скажем, включения и выключения). Поэтому при упаковке, транспортировке и хранении доказательств в электронной форме (электронных доказательств) необходимо принимать особые меры предосторожности. Для сохранения доказательной силы изъятых материалов вплоть до их предъявления в судебном заседании необходимо должным образом фиксировать все операции по упаковке, транспортировке и хранению электронных доказательств.  Как правило, со всеми компьютерными компонентами и электронными носителями информации следует обращаться как можно осторожнее, так как неумелое обращение с ними может привести к повреждению и уничтожению электронных доказательств.     * Упаковка: * перед тем, как приступить к упаковке, необходимо убедиться в том, что все изъятые электронные доказательства должным образом задокументированы и помечены; * по мере возможности, перевозить изъятые электронные доказательства надо в их оригинальной упаковке; * за отсутствием таковой необходимо использовать антистатическую упаковку (изготовленную из бумаги или же антистатической плёнки). Следует избегать упаковки из материалов, генерирующих/накапливающих статическое электричество, таких как стандартные пластиковые мешки; * нельзя свёртывать/сгибать такие электронные носители информации как дискеты, лазерные диски (CD-ROMы), магнитные ленты, а также наносить на них царапины; * нельзя прикреплять самоклеющиеся этикетки на поверхность электронных носителей. По мере возможности необходимо использовать для упаковки таковых коробки или же конверты; * необходимо убедиться в том, что вся тара, используемая для упаковки электронных доказательств, должным образом промаркирована; * при изъятии нескольких компьютерных систем необходимо избрать такую маркировку упаковочной тары, которая позволила бы их собрать снова в изначальном виде. * транспортировка * во время транспортировки необходимо держать электронные доказательства вне зоны действия источников электромагнитного излучения. Радиопередатчики, магнитные сердечники громкоговорителей, автомобильные сиденья с подогревом – вот примеры тех объектов, которые могут вывести из строя электронные доказательства; * убедиться, что упакованное электронное оборудование защищено от внешнего механического воздействия: тряски, ударов, - а также от воздействия жары и влажности; * обеспечить такую укладку внутри автотранспортного средства неупакованных компьютеров и других электронных устройств, которая позволила бы свести к минимуму воздействие тряски и вибрации при транспортировке. Например, сами компьютеры надо положить на пол, а мониторы на сиденья автотранспортного средства экраном вниз, закрепив их ремнём безопасности; * тяжёлые предметы не следует ставить на меньшие по размерам компоненты электронного оборудования или носители информации; * по мере возможности, не следует долгое время хранить в автотранспортных средствах изъятые электронные доказательства; * хранение: * необходимо обеспечить инвентаризацию электронных доказательств в соответствии с требованиями соответствующих ведомственных инструкций; * хранить электронные доказательства надо в охраняемом помещении при умеренной температуре и влажности; * они должны быть ограждены от источников электромагнитного излучения, а также защищены от воздействия сырости, пыли и других вредных загрязняющих веществ; * в этих целях необходимо использовать охраняемую камеру хранения, должным образом оборудованную: * системой контроля допуска, * системой пожарной безопасности, предполагающей наличие пожарной сигнализации, огнетушителей, запрещение курить в её кладовой части и в прилегающих помещениях, * системой поддержания температурного режима и влажности; * системой защиты от электромагнитных излучений (одним из источников которых могут быть, например, направленные радиоизлучатели), * запрещается хранить легковоспламеняющиеся материалы (например, моющие жидкости или бумагу) в одном месте с электронными доказательствами или же поблизости от них; * пол должен быть покрыт материалом, не генерирующим статического электричества; * запрещается хранить электронные доказательства в помещении, по которому проходят водопроводные трубы (особенно на уровне потолочных перекрытий); * следует помнить о том, что электронные доказательства не подлежат продолжительному хранению в связи с опасностью утраты данных, хранящихся в их электронной памяти (дат, времени, конфигурации системы). Так как время работы аккумуляторов ограничено, то после их разрядки целый ряд данных теряется. Поэтому соответствующий персонал должен быть проинформирован о том, что электронные устройства, работающие на батарейках (такие как, например, PDA или PC/CMOS), требуют к себе срочного внимания. | |
| Слайды 42 - 51 | Исследование и анализ электронных доказательств  Судебная компьютерно-техническая экспертиза  Термин «судебная компьютерно-техническая экспертиза» используется для описания методичного исследования информационно-технического оборудования с целью обнаружения электронных доказательств. Как правило, судебная экспертиза проводится после того, как преступление уже было совершено. По сравнению с обычными следственными действиями, при проведении компьютерно-технической экспертизы возникает лишь одна трудность - она связана с постоянной эволюцией компьютерных технологий и с увеличением количества информации, хранящейся в цифровой форме, и, соответственно, с ростом объемов потенциальных доказательств. В этих условиях очень многое зависит от того, насколько юридически приемлемо использование электронных доказательств в ходе судебного разбирательства. Это в определённой степени ограничивает возможности компьютерно-технической экспертизы, призванной действовать в рамках правовых норм. Даже если научно-технический прогресс и позволит проводить новые виды криминалистического исследования, применение их результатов будет ограничено существующими законными рамками.  **Этапы расследования, требующие привлечения судебных компьютерно-технических экспертов**  Судебные эксперты привлекаются для вынесения заключений не только по уголовным, но и по гражданским делам. Также они играют большую роль в разработке стратегии защиты и в подготовке кадров. При расследовании уголовных дел их участие необходимо на четырёх этапах:   * на этапе выявления значимых для расследования доказательств. Компьютерно-технический эксперт играет важную роль при разработке стратегии следственных действий. Предварительно, ещё до начала таковых, он может оказать помощь правоохранительным органам при определении оптимальных технических методов их проведения. Во время производства следственных действий эксперт может, например, проанализировать конфигурацию компьютерной сети в жилище подозреваемого лица с целью обнаружения мест возможного нахождения электронных носителей информации. * на этапе собирания/выемки/обеспечения сохранности доказательств. Собирание электронных доказательств возможно не только на месте их физического нахождения в конкретном обыскиваемом помещении, но и в местах удалённого доступа, где они также могут храниться. На следователя, приступившего к собиранию доказательств (а также на оперативных работников, оказывающихся первыми на месте обыска/выемки) ложится большая ответственность за результаты всего следственного действия. Скажем, если они принимают стандартные решения по обеспечению сохранности данных, то существует опасность потери следов важной информации. В качестве примера можно задаться вопросом, как поступить с работающим компьютером подозреваемого лица? Обычно, стандартный метод в таких случаях заключается в отключении электропитания компьютера, вместо остановки его работы с помощью операционной системы. Но в тех случаях, когда правонарушитель использовал шифровальные средства, отключение компьютера от электросети может привести к декодированию файлов. Следовательно, оперативный работник, оказывающийся первым на месте обыска/выемки, должен принять решение в зависимости от основной цели следствия.   Значение компьютерно-технической экспертизы велико не только при проведении следственных действий на месте нахождения данных, имеющих отношение к делу. Судебные эксперты могут также оказать помощь следствию при подготовке запросов, направляемых поставщикам интернет-услуг, и при вынесении прилагаемых к делу заключений, необходимых для подтверждения достоверности собранных доказательств.   * на этапе всестороннего исследования/анализа изъятых электронных доказательств и аппаратного оборудования. Как правило, он является самой сложной фазой всего процесса компьютерно-технической экспертизы. Оперативные работники, оказывающиеся первыми на месте обыска/выемки, зачастую изымают несколько устройств хранения данных, каждое из которых может содержать многие тысячи файлов. Даже сам по себе объем данных, подлежащих исследованию, является серьёзной проблемой для экспертизы. В этих условиях одна из основных задач экспертов заключается в выявлении сведений, представляющих интерес для следствия, и установление их относимости к расследуемому делу, а также взаимосвязи друг с другом. Широк круг их обязанностей: от обнаружения противозаконного содержания в компьютерной системе подозреваемого до анализа имеющихся в ней файлов системного журнала («лог-файлов»). Кроме того, не все действия, предпринимаемые злоумышленником при совершении компьютерного преступления, оставляют за собой следы. Тем не менее, исследуя все имеющиеся в их распоряжении доказательства, компьютерно-технические эксперты могут восстановить то, каким образом было совершено компьютерное правонарушение. По окончании третьего этапа составляется полный отчёт (заключение) о проделанной исследовательской работе и методах, использованных для получения доказательств.   **Примеры различных видов судебной компьютерно-технической экспертизы**  На протяжении всех четырёх вышеописанных этапов (особенно, на третьем) возможно проведение экспертных работ различных видов. Правильность выбора вида компьютерно-технической экспертизы зависит от многих факторов и, прежде всего, от характера самого расследуемого правонарушения.  Среди наиболее распространённых видов компьютерно-технической экспертизы можно перечислить следующие:   * Аппаратно-компьютерная экспертиза. В случае изъятия работниками следственных органов аппаратных средств судебные эксперты могут изучить его для сбора информации, относящейся к данной компьютерной системе. Подобного рода исследование необходимо, например, для доказательства того, мог ли правонарушитель подключать свою компьютерную систему к интернету. Также, аппаратно-компьютерная экспертиза может потребоваться, если известно (благодаря передаче информации о компьютерной системе при регистрации), что подозреваемое лицо использовало аппаратные средства особой конфигурации. * Функциональная экспертиза программного обеспечения. Программы, установленные на аппаратных средствах компьютера, играют важную роль в работе компьютерной системы. Судебные эксперты могут установить, например, функции компьютерных вирусов и других вредоносных программ, или же восстановить все операции, выполненные той или иной программой. Более того, роль этот вида экспертизы может оказаться важной при определении того, подлежит ли уголовному преследованию производство/продажа той или иной программы двойного назначения (то есть, программы, используемой для достижения как законных, так и противозаконных целей). * Программно-компьютерная экспертиза предполагает исследование программного обеспечения, установленного на компьютерной системе подозреваемого лица. В результате её проведения следственные органы могут получить информацию, представляющую важность для дальнейшего расследования дела. Это в особенности касается шифровальных программ и программного обеспечения, используемого для безвозвратного удаления файлов. Если подобные программы установлены на компьютере подозреваемого лица, то в связи с этим необходимо произвести дополнительные следственные действия. * Выявление значимой для расследования информации в цифровом виде. Компьютерные данные могут находиться в разного рода запоминающих устройствах. Даже на жестком диске файлы могут храниться различными способами. Поэтому выявление места и способа хранения относящихся к расследуемому делу доказательств требует особых усилий.   Одним из нововведений, создающих дополнительные трудности в выявлении значимой для расследования цифровой информации, является расширяющаяся практика хранения данных на удалённом сервере. Как подчёркивалось выше, повсеместное распространение широкополосного доступа в интернет и удаленных серверов хранения данных повлияло на способы хранения информации. Разместив данные на удалённом сервере, подозреваемое лицо может профилактически предвосхитить изъятие у него компьютера. Тем не менее, правоохранительные органы имеют возможность получить доступ к информации, хранящейся на удалённом сервере. В таком случае обращение к компьютерно-технической экспертизе позволяет проверить, обращался ли подозреваемый к услугам удалённого сервера или нет.  Выявление значимой для расследования цифровой информации не ограничивается одними только файлами. В базах данных программных средств, используемых подозреваемым лицом для нахождения информации в своём компьютере, также могут находиться сведения, относящиеся к расследуемому делу. Даже во временных файлах, создаваемых системой, могут содержаться интересующие следствие улики.   * Выявление скрытых файлов. Правонарушители могут использовать различные технические способы, делающие невидимыми файлы в запоминающем устройстве, с тем, чтобы не допустить раскрытия их содержания правоохранительными органами. Особенно если речь идёт о следственных действиях по выявлению противозаконного содержания. Благодаря компьютерно-технической экспертизе становиться возможным выявлять скрытые файлы и делать их доступными для следственных органов. * Восстановление удалённых файлов. При использовании правонарушителем программных средств безвозвратного удаления файлов содержавшаяся в них информация, как правило, восстановлению не подлежит. Но в тех случаях, когда правонарушители не знают о существовании подобных программ, то простое удаление цифровой информации из памяти компьютера необязательно делает её недоступной для правоохранительных органов, которые могут использовать для её восстановления специальные программные средства. * Расшифровка зашифрованных файлов и разделов (томов), восстановление паролей. Преступный мир всё чаще прибегает к использованию шифровальных (криптографических) средства. Таковые создают значительные трудности для работы правоохранительных органов, делая недоступной зашифрованную информацию. Судебная компьютерно-техническая экспертиза позволяет найти подход к расшифровке зашифрованных файлов и запоминающих устройств. Кроме того, экспертное сообщество может оказать содействие правоохранительным органам в разработке методологии получения доступа к зашифрованным файлам, например, благодаря использованию программ по взлому шифра.   Кроме шифрования правонарушители также используют системы парольной защиты для воспрепятствования доступа к некоторым данным. Обычно в таком случае компьютерно-технические эксперты прибегают к программам восстановления паролей для того, чтобы помочь следствию получить доступ к информации несмотря на систему парольной защиты.   * Исследование файлов. Существуют различные способы исследования/анализа файлов, хранящихся в запоминающих устройствах. В ходе судебной компьютерно-технической экспертизы основное внимание может быть сосредоточено, например, на содержании файлов. Кроме изучения подозрительных файлов в ручном режиме, может применяться при работе с текстовыми файлами система поиска по ключевым словам или же программные средства, которые позволяют вести автоматический поиск известных следствию видео и фотоматериалов в компьютере подозреваемого лица.   Как подчёркивалось выше, компьютерные данные легко поддаются искажению («манипуляциям»). Судебная компьютерно-техническая экспертиза позволяет доказать факт наличия искажения или же подлога компьютерного документа.  Более того, при её проведении учитываются и метаданные, содержащие сведения, например, о времени, когда тот или иной документ открывался или был изменён в последний раз. Анализ метаданных может быть также необходим для установления личности создателя файла, содержащего, скажем, послание с угрозами, или же для определения серийного номера видеокамеры, использовавшейся для производства детской порнографии.   * Экспертиза на предмет установления авторства текста. При размещении угроз или же возбуждающих ненависть или вражду высказываний на интернет-блогах/форумах исследование «лог-файлов» может не привести к установлению личности автора вышеуказанных материалов в том случае, если подозреваемое лицо производило их рассылку из, скажем, интернет-кафе или же использовало для этого службу анонимной связи. Применение усовершенствованных методов лингвистического анализа текста может помочь в определении того, действительно ли подозреваемое лицо написало до этого инкриминируемые ему статьи и оставило таким образом информацию, которая способствовала его выявлению. * Сохранение целостности данных. Как указывалось выше, обеспечение целостности и сохранности компьютерных доказательств является основным условием их допустимости в суде. Судебный компьютерно-технический эксперт может обеспечить защиту целостности файлов при собирании доказательств. В некоторых случаях это позволяет правоохранительным органам не прибегать к изъятию аппаратных средств, ограничиваясь копированием значимых для расследования файлов. Таким образом обеспечивается их целостность и защита от попыток какого бы то ни было искажения содержащихся в них данных в процессе расследования. В частности, копирование включает создание полного образа запоминающего устройства. * Отслеживание по IP-адресу. Правонарушители, использующие интернет для совершения своих преступлений (например, при загрузке детской порнографии или же при проведении атаки на компьютерную систему) оставляют за собой следы. Анализ параметров передачи цифровых данных, в также исследование «лог-файлов», оставляемых в компьютере поставщиками интернет-услуг, позволяют эксперту (и следствию) определить интернет-провайдера подозреваемого и его выходы в интернет. Подобный анализ может быть затруднён, если правонарушитель использовал программные средства обезличивания связи. Но даже и в этом случае экспертизу нельзя считать невозможной. Одним из примеров такого экспертного обеспечения является программа «верификатор IP-адресов компьютеров» (CIPAV), использовавшаяся в США для установления личности подозреваемых, работавших через службу анонимной связи. * Исследование сообщений, доставленных по электронной почте («мейлов»). Электронная почта стала весьма распространённым средством связи. Естественно, что её анализ занимает важное место в судебной компьютерно-технической экспертизе. Понимая, насколько относительно легко установить личность отправителя электронного письма с угрозами или же сообщения с прикреплённым противозаконным содержанием, правонарушители очень часто имеют произвольно созданные электронные адреса, зарегистрированные с использованием вымышленных личных данных. Даже в таких случаях экспертиза информации, содержащейся в заголовке электронного сообщения, и «лог-файлов», оставленных провайдером электронной почты могут иногда позволить установить личность подозреваемого лица. * Отслеживание финансовых сделок. Совершение ряда преступлений, включая торговлю детской порнографической продукцией, предполагает осуществление финансовых сделок. В этих условиях возможно выявить правонарушителя, изучив данные торговых точек и финансовых учреждений, задействованных в проведении подобных сделок. В качестве примера можно привести расследование в Германии одного дела о торговле в сети детской порнографией. Правонарушители, загружавшие запрещённые законом порнографические материалы с коммерческого сайта, были выявлены эмитентами их кредитных карт, по реквизитам которых «вычислили» покупателей, использовавших эти карточки для покупки детской порнографии на специализированных сайтах. Проведение такого рода экспертизы затруднено, если правонарушители используют методы обезличенного платежа. * Получение в реальном времени параметров передачи цифровых данных и перехват содержания таковых. Средства судебной компьютерно-технической экспертизы позволяют осуществлять в реальном времени мониторинг за процессом передачи данных. В положениях проекта Совета Европы «Киберпреступность» предусматривается возможность непосредственного реагирования правоохранительных органов на действия подозреваемого лица в момент совершения им правонарушения. * Мониторинг работы служб общего пользования, которые могут использоваться правонарушителями для обмена материалами, защищёнными авторским правом или же имеющими противозаконное содержание. В рамках проводимых следственных действий работа таких служб (например, обмен информацией на «чатах» и форумах) может отслеживаться средствами судебной компьютерно-технической экспертизы. * Дистанционная судебная компьютерно-техническая экспертиза. В настоящее время потребность в средствах проведения дистанционной компьютерно-технической экспертизы является предметом обсуждения. Они позволили бы вести в реальном времени дистанционное собирание электронных доказательств и дистанционный мониторинг работы компьютерной системы подозреваемого лица без его ведома.   Проведение такой экспертизы в интересах следствия требует особой подготовки и соблюдения детально проработанного порядка, основывающегося на общепринятых процессуальных нормах и методах.  Как проводится судебная компьютерно-техническая экспертиза (СКТЭ)?  Существует два способа проведения СКТЭ:   * в ручном режиме: несмотря на наличие средств автоматизации анализа цифровых данных, судебная компьютерно-техническая экспертиза проводится по большей части в ручном режиме. При этом особые трудности возникают в тех случаях, когда необходимо обработать большие объемы данных; * в автоматическом режиме: некоторые работы по исследованию данных (в особенности это относится к поиску текстовых файлов по ключевому слову, восстановлению удалённых файлов и к расшифровке зашифрованных данных) могут быть осуществлены с помощью технически достаточно сложных средств автоматизации анализа данных.   В большинстве случаев, судебные эксперты сочетают работу в ручном режиме с использованием программных средств автоматической обработки данных.   * Представление/предъявление доказательств в суде. Как правило, судебные эксперты доказательств в суде не предъявляют. Тем не менее, они могут играть важную роль в уголовном процессе. Они могут выступать в качестве свидетелей-экспертов, помогающих участникам судебного разбирательства понять, как возникли предъявляемые доказательства, как они собирались и оценивались. | |
| Слайды 52 - 59 | Часть третья - Вопросы правового характера, возникающие в связи с изучаемой темой. | |
|  | НЕКОТОРЫЕ ВОПРОСЫ, ОТНОСЯЩИЕСЯ К ПОЛУЧЕНИЮ КОМПЬЮТЕРНЫХ ДОКАЗАТЕЛЬСТВ  Современные формы преступной деятельности, осуществляемой в коммуникационных сетях, направленной против них или же существующей с их помощью, сегодня таковы, что для борьбы с ними требуется помощь экспертов и специалистов при собирании электронных доказательств, анализе и правильном их толковании в суде.  Конечно же, факт этот не новый: вот уже многие века учёные люди - эксперты в своём деле – помогают судьям, прокурорам и адвокатам разбираться в технических вопросах. Например, в течение многих столетий врачи играли основную роль при определении, выяснении и оценке в суде возможных причин наступившей смерти, объясняя всё это своим языком, с использованием медицинских терминов. Сегодня весь вопрос заключается в том, что с появление новой среды, прозванной информационным пространством, возникли и новые проблемы, до сих пор трудно поддающиеся решению.  С одной стороны, постоянный научно-технический прогресс не всегда сопровождается столь же постоянным пересмотром и обновлением правовых инструментов, и не всегда действующие процессуальные нормы узаконивают постоянно совершенствующиеся технические средства собирания компьютерных доказательств.  С другой стороны, как на этапе начальной подготовки, так и на курсах повышения квалификации обучающиеся сотрудники правоохранительных органов, работники суда и прокуратуры обычно не успевают за техническим прогрессом в данной области.  Одновременно постоянно возникают новые разновидности правонарушений, для понимания сути которых нужны специальные знания. Техническая экспертиза необходима не только для доказывания преступной деятельности, но и для объяснения того, в чём она конкретно заключается. Если мы все отлично знаем, что значит «убийство», и что необходима судебно-медицинская экспертиза для установления причин смерти, то «отказ в обслуживании» является таким видом преступления, для уяснения сути которого требуется понимание принципов работы компьютерных сетей.  В большинстве стран мира отсутствуют особые правовые нормы, регламентирующие собирание доказательств в электронной форме (электронных доказательств). В некоторых из них введён особый процессуальный порядок осуществления, например, перехвата сообщений. Но, как правило, правовые нормы, относящиеся к собиранию электронных доказательств, основываются на законодательных положениях, существовавших ещё до появления интернета. Когда-то суды принимают к рассмотрению электронные документы в качестве доказательств, приспосабливая к ним обычные нормы права, а когда-то не принимают. В таком случае необходимо обогащать существующую правовую систему новыми нормами с поправкой на действительность.  Многие страны Европы ещё не ввели в своё законодательство правовые нормы, относящиеся к электронным доказательствам, с указанием критериев, которые суды должны использовать при оценке и рассмотрении электронных доказательств.  Собирание и оценка электронных доказательств дело весьма деликатное, как правило, затрагивающее основополагающие права, такие, скажем, как право на неприкосновенность личной жизни или же право на тайну переписки и иных сообщений. Таким образом, иногда судьи не могут уяснить сами для себя, являются ли те или иные действия в области собирания электронных доказательств нарушением вышеперечисленных прав или нет.  Сетевая компьютерная преступность (киберпреступность) имеет планетарные масштабы. Преступная деятельность в этой сфере ведётся одновременно в разных странах и подпадает под действие самых различных юрисдикций. По самой своей природе киберпреступность транснациональна. Преступления, совершенные в информационном пространстве с применением сетей связи, создают серьезные проблемы по определению конкретного места, где было совершено правонарушение, и установлению того, какие же конкретно правоохранительные органы компетентны в каждом конкретном случае расследовать дело. Конечно, с помощью одной только будапештской Конвенции о компьютерных преступлениях не решить всех возникающих в этой сфере проблем, но тем не менее, в ней можно найти ответы на некоторые сложные вопросы.  Предполагается, что, как это делается обычно в других случаях, стороны «Будапештской конвенции» будут расследовать преступления, совершенные на их территории. Дополнительно конвенцией устанавливается следующее правило: стороны должны заявить о том, что они компетентны предпринимать следственные действия и вести судебное разбирательство по делам, в которых замешаны их собственные граждане, в случае совершения ими преступления за рубежом и при условии, что их преступные деяния подлежат наказанию и по законодательству того места, где таковые имели место.  Это положение имеет большой практический смысл. Хотя в законодательствах ряда стран и содержатся положения в защиту их универсальной юрисдикции, таковой принцип не всегда и не везде признан.  Действительно, во многих ситуациях трудно бывает определить подсудность тех или иных дел, руководствуясь общепринятыми нормами права. Например, одно компьютерное преступление может быть совершено одновременно в целом ряде стран и иметь там множество потерпевших, или же может совершаться сразу несколькими правонарушителями, территориально находящимися в разных местах.  Пока не будет проведена во всех странах гармонизация норм, регламентирующих подсудность уголовных дел, может случиться так, что одно и то же правонарушение окажется подсудным двум судам различных стран, несмотря на то, что существуют на этот счёт соответствующие общие положения «Будапештской конвенции».  На уровне же Европейского Союза была разработана важная Директива 2006/24/EC Европейского парламента и Совета Евросоюза от 15 марта 2006 г., касающаяся исключительно собирания компьютерных доказательств. Это первый обязательный к исполнению повсюду в Европейском Союзе документ об «удержании данных, генерируемых или обрабатываемых в связи с предоставлением общедоступных услуг электронной связи или же с использованием публичных коммуникационных сетей». | |
|  | Практические занятия (проводятся при наличии необходимых условий).  В рамках этого занятия они не предусмотрены за отсутствием гарантий того, что во всех местах его проведения будут в наличии технические средства должного уровня и доступ в интернет, необходимый для их проведения.  На будущее инструктора могут добавочно ввести практические занятия в учебный план в том случае, если на месте их проведения будут соблюдены все необходимые технические условия. | |
|  | **Проверка знаний**  На этом занятии никакой дополнительной проверки в дополнение к вышеперечисленным требованиям в настоящее время не предусмотрено. Также, не требуется проводить никакого официального зачёта. | |
| Слайды 63 - 64 | Подведение итогов занятия/выводы  Инструктору следует подвести итоги/проверить знания, чтобы убедиться в том, что слушатели усвоили изложенный им на занятии материал, и в состоянии:   * рассказать, какие существуют виды электронных доказательств; * изложить основные наиболее эффективные методы изъятия электронных доказательств и обращения с ними; * определить трудности, возникающие при работе с данными, сохраняющимися на жестком диске компьютера после отключения питания, с данными в оперативной памяти включённого компьютера («короткоживущими данными»), а также с интернет-источниками электронных доказательств; * выявить проблемы с получением доказательств из другой юрисдикции; * обсудить вопросы допустимости использования электронных доказательств в судебном разбирательстве с точки зрения их подлинности, точности и полноты;   Задачи занятия могут быть достигнуты путём проведения коллективного обсуждения изучаемого материала, опроса слушателей, заполнения контрольных вопросников или же с помощью других общепризнанных методов.  Это занятие задумывалось таким образом, чтобы задать ориентировочные характер и уровень технической осведомлённости, требуемые от судей и прокуроров для эффективного исполнения ими своих профессиональных обязанностей. Его авторы не претендуют на исчерпывающий анализ изучаемого предмета и там, где это им кажется важным, дают ссылки на дополнительные источники информации.  Рекомендуется, чтобы разработчики практических занятий при их подготовке использовали самые современные сведения о последних достижениях науки и техники постольку, поскольку таковые влияют на поведение преступного мира, а также отражаются на правовых нормах, на положениях процессуального права и порядке доказывания вины в рамках той юрисдикции, при которой должны проводиться практические занятия (тренинги). Существуют такие технологические прорывы, которые сказываются на работе всей системы уголовного правосудия. Здесь в качестве примера можно привести появление твёрдотельных устройств хранения данных или же методики проектирования интернет систем по принципу «Веб 2.0.» (Web 2.0.). Таким образом, будет необходимо включить в программы подготовки немало важных тем по мере возрастания их значимости. | |

|  |  |  |
| --- | --- | --- |
| Занятие 1.3.4 Международное сотрудничество | | **Продолжительность:**  **90 минут** |
| **Перечень материалов, необходимых для проведения занятия:**   * ноутбук или ПК с операционной системой Windows 7 и с загруженным офисным пакетом приложений MS Office 2010; * проектор с экраном; * презентация «Пауер Пойнт». | | |
| **Цель:**  Это занятие направлено на то, чтобы напомнить важность международного сотрудничества. На нём представлен общий обзор имеющихся в наличии инструментов взаимодействия между странами в области противодействия сетевой компьютерной преступности (киберпреступности), главным из которых является будапештская Конвенция о компьютерных преступлениях. Также на этом занятии речь пойдёт о том, как пользоваться вышеуказанными инструментами, какова скорость реагирования на запросы, поступающие в рамках международного сотрудничества, и их эффективность. | | |
| **Задачи**  По окончании занятия слушатели должны быть в состоянии:   * осознать планетарные масштабы интернет сети и международный характер сетевой преступности (киберпреступности); * объяснить важность международного сотрудничества и выявить инструменты международного сотрудничества, имеющиеся в нашем распоряжении в борьбе с киберпреступностью; * оценить потребность в быстродействующих и эффективных каналах международного сотрудничества и в соответствующих инструментах; определить способы, сроки и действенность их использования; * описать усилия международных организаций по внедрению новых форм и механизмов международного сотрудничества; * обсудить будапештскую «Конвенцию о компьютерных преступлениях», определить основные утверждаемые в ней принципы, содержащиеся в конвенции обеспечительные меры, а также работу сети «24/7» по оказанию правовой взаимопомощи. | | |
| **Слайд №** | **Содержание:** | |
|  | **Введение**  На этом занятии подчёркивается важность международного сотрудничества при расследовании конкретных преступлений в сфере компьютерной информации и рассматриваются регламентирующие его международные юридические документы (главным образом, будапештская Конвенция о компьютерных преступлениях). | |
| Слайд 2 | 1. Первая часть презентации посвящена, главным образом, международному измерению сетевой компьютерной преступности (киберпреступности). Так как эта тема уже затрагивалась на предыдущих занятиях, то здесь она будет упомянута очень коротко. 2. Во второй части перечисляются некоторые меры противодействия киберпреступности на международном уровне. 3. В третьей части подчёркивается роль будапештской Конвенции о компьютерных преступлениях в борьбе с киберпреступностью. 4. В четвёртой части презентации особое внимание уделяется инструментам международного сотрудничества, предусмотренным «Будапештской конвенцией». 5. Пятая часть посвящена общему обзору всех тем, изложенных в этой презентации. | |
| Слайд 3 | Задачи занятия  В общем и целом, это занятие направлено на то, чтобы подвести слушателей к осознанию планетарных масштабов интернет сети и международного, транснационального характера сетевой компьютерной преступности (киберпреступности).  Также будет затронут вопрос, касающийся важности международного сотрудничества в борьбе с киберпреступностью и международных юридических документов, регламентирующих таковое сотрудничество.  Кроме того, на занятии будет подчёркнута потребность в быстродействующих и эффективных каналах международного сотрудничества и описаны инструменты его осуществления.  Далее, будет дан обзор усилий, предпринимаемых международными организациями по внедрению новых форм и механизмов международного сотрудничества.  В особенности, будет упомянута будапештская «Конвенция о компьютерных преступлениях» и выделены основные содержащиеся в ней принципы и обеспечительные меры; также речь пойдёт о работе сети «24/7» по оказанию правовой взаимопомощи. | |
| Слайд 4 | Часть первая - международное измерение сетевой компьютерной преступности (киберпреступности).  В рамках весьма сжатого обзора инструктор возвращается к теме международного масштаба компьютерной преступности. | |
| Слайд 5 | Это очевидный факт, что интернет распространился по всей планете, где он доступен почти всем.  Одновременно с расширением сетей интернета росла и киберпреступность, к которой соответственно надо подходить как к явлению планетарного масштаба. Не признав этого, нельзя до конца понять истинную природу сетевой компьютерной преступности. | |
| Слайд 6 | В этих условиях киберпреступность является самым «транснациональным» видом преступной деятельности. Следовательно, для эффективного расследования преступлений в сфере компьютерной информации необходимо действенное международное сотрудничество. Без него маловероятно, что борьба с сетевой преступностью увенчается успехом. | |
| Слайд 7 | Если говорить конкретно, то при совершении преступления в информационном пространстве (киберпространстве) органы уголовного правосудия сталкиваются с весьма трудными вопросами, которые им надо решить в первоочередном порядке.  Учитывая повсеместное распространение интернета, не всегда бывает легко установить место совершения преступления с точки зрения его подсудности. Предположим, что лицо, совершающее преступление, находится в точке «А», компьютер пострадавшего – в точке «Б», а сами противозаконные действия по установлению связи с этим компьютером осуществлялись преступником через провайдера, расположенного в точке «В», и что все вышеперечисленные точки подпадают под действие разных юрисдикций. В подобной ситуации первая проблема, которую должен решить уполномоченный сотрудник правоохранительных органов, состоит в том, чтобы определить подсудность совершенного преступления с точки зрения места применяемой юрисдикции. Действительно, прежде всего необходимо юридически установить место совершения преступления, чтобы затем определить, нормы какого материального права применять, и какие органы компетентны рассматривать дело (полиции, прокуратуры, суда).  Следственные органы должны оставаться в пределах своей юрисдикции, расследуя дела, относящиеся к их территориальной подсудности. В соответствии с этим принципом, расследование уголовного дела ограничено пределами юрисдикции следственного органа.  В связи с подобным положением вещей встаёт два рода нерешённых вопросов:   * Их первая категория относится к проведению международных («трансграничных») расследований: как сотрудник правоохранительных органов может на законных основаниях вести расследование вне пределов своей страны при том, что следственные действия надо производить в срочном порядке? Как он может получать и собирать доказательства, хранящиеся «в чужом доме», в другой стране, если он чувствует, что доказательный материал может очень скоро исчезнуть? * Вторая категория вопросов касается собирания электронных доказательств на удалённых серверах хранения данных (в так называемых «компьютерных облаках»). Действительно, в этом случае никто не знает, где физически могут храниться те или иные данные. Возможно, что никто не знает, под действие какой национальной юрисдикции подпадают данные, размещённые на «компьютерном облаке». Как сотрудник правоохранительных органов может получать и собирать данные, хранящиеся на «компьютерном облаке», вне зависимости от того, где оно физически находится? | |
| Слайды 9 и 10 | Часть вторая – международные меры противодействия сетевой компьютерной преступности (киберпреступности)  В связи с тем, что сегодня интернет распространился по всему миру и потенциально используется каждым жителем планеты, к киберпреступности необходимо подходить как к явлению планетарного масштаба. Цель второй части настоящей презентации состоит в описании тех конкретных важных мер, которые предпринимаются в Европе в области борьбы с киберпреступностью. | |
| Слайды 11 - 13 | «Интерпол» является широко известной международной организацией, объединяющей в своих рядах представителей правоохранительных органов стран всего мира. На январь 2012 года он насчитывал 190 членов со всех континентов нашей планеты. Цель «Интерпола» заключается в укреплении международного сотрудничества между правоохранительными органами стран участниц. С этой целью данной организацией была создана глобальная система связи «Интерпола», а также специализированные базы данных и аналитические структуры.  «Интерпол» стал одной и первых международных организаций, выразивших озабоченность в связи с ростом компьютерной преступности и организовавших в 1995 г. экспертные группы по обсуждению данной проблемы. С той поры «Интерпол» развивает усилия по оказанию помощи полиции и другим правоохранительным органам всего мира в усилении их потенциала противодействия киберпреступности.  Для достижения вышеуказанной цели «Интерпол» создал сеть Национальных центральных бюро (НЦБ), работа которых направлена на оказание помощи его членам на постоянной основе. В сентябре 2011 г. она насчитывала около 120 НЦБ по всему миру. Национальные центральные бюро «Интерпола» на местах работают по той же схеме, что и национальные контактные центры «Сети 24/7», созданные во исполнение положений статьи 35 будапештской Конвенции о компьютерных преступлениях. В некоторых государствах – сторонах конвенции НЦБ «Интерпола» стали также и контактными центрами «Большой восьмёрки» (G8) на местах. В эту сеть включены все контактные центры «Большой восьмёрки». Целью этой структуры является оказание содействия органам местной полиции в срочном нахождении в другой стране необходимых экспертов и в получении срочной помощи при расследовании дел, связанных с использованием компьютерных технических средств, а также при собирании доказательств. Служба работает круглосуточно семь дней в неделю.  Целью НЦБ является организация обмена опе­ративно-розыскной информацией и другого рода сведениями между правоохранительными органами государств-членов «Интерпола», а также оперативного обеспечения. Главным образом, работа НЦБ направлена на ускорение обмена чисто опе­ративной информацией по соответствующим специальным каналам «Интерпола». Здесь речь может идти об отпечатках пальцев, данных о ДНК-профилях, сведениях о подозреваемых террористах и о находящихся в розыске лицах, потерянных или же украденных проездных документах, краденых произведениях искусства и так далее. Этот вид потенциально важной информации, предоставляемой «Интерполом», без всякого сомнения, чрезвычайно необходим при расследовании конкретных дел. Тем не менее, он не востребован в срочных запросах об обеспечении сохранности, например, компьютерных данных или же параметров передачи цифровых данных, а также о принятии любых других мер, направленных на собирание и сохранение электронных доказательств (что, собственно говоря, и естественно, принимая во внимание цели создания сети НЦБ). Иными словами, сотрудничество, осуществляемое в рамках этой сети опорных пунктов «Интерпола» на местах, основывается на тех же основных принципах, которыми эта организация руководствуется во всех остальных случаях. | |
| Слайд 14 | Европейский Союз (ЕС) поддерживает «Будапештскую конвенцию». Его представители даже принимали участие в качестве наблюдателей в составлении её проекта. С тех пор ЕС побуждает все государства–члены к ратификации этого международного договора. И действительно, значительное количество государств – членов ЕС ратифицировало его, и все уже подписали.  Естественно, сам Европейский Союз также располагает широким набором инструментов международного сотрудничества (даже если не учитывать самые недавние документы, основанные на принципе взаимного признания). Большинство преимуществ европейской системы сотрудничества проистекает из возможности установления прямых контактов между судебными органами государств-членов ЕС. Это позволяет любому судье или прокурору напрямую направить соответствующий запрос своим коллегам из другого государства ЕС. Этот очень мощный инструмент, которым располагают правоохранительные органы Европы, используется также и при раскрытии преступлений в сфере компьютерной информации. | |
| Слайд 15 | Кроме того, в 2005 г. Европейский Союз (ЕС) принял обязательный к исполнению документ - Рамочное решение Совета министров ЕС 2005/222/JHA от 24 февраля 2005 г. по вопросу о компьютерных атаках на информационные системы. Кроме всего прочего, в нём также речь идёт о работе международной сети контактных центров «Сеть 24/7» в области расследования компьютерных преступлений. В частности, это рамочное решение включает в себя правила, касающиеся *«существующей сети контактных центров».* Статьей 11.1 решения постановляется следующее: все государства-члены Европейского Союза обязаны обеспечить использование существующей сети постоянно действующих контактных центров круглосуточной оперативной связи при обмене информацией, касающейся перечисляемых в этом документе правонарушений (незаконный доступ к информации в информационных системах, незаконное вмешательство в информационные системы и базы данных, а также подстрекательство, соучастие, оказание помощи в совершении и попытка совершения вышеперечисленных противоправных деяний).  Хотя в статьях рамочного решения об этом и не говорится, тем не менее, ясно, что *существующая сеть контактных центров* это также и сеть «Большой восьмёрки»/Совета Европы. | |
| Слайд 16 | «Европол» является самостоятельной организацией Европейского Союза, цель которой заключается в повышении эффективности сотрудничества между правоохранительными органами государств-членов ЕС. Начиная с 1999 г. его деятельность включает в себя принятие мер по содействию анализу опе­ративно-розыскной информации и обмену данными между государствами-членами ЕС. Сетевая компьютерная преступность (киберпреступность) представляет собой одну из наиболее значительных сфер приложения сил «Европола». Кроме всего прочего, «Европол» может в большой степени способствовать осуществлению положений 26 статьи "Будапештской конвенции" благодаря своим налаженным каналам передачи т. н. «внеплановой информации», о которой идёт речь в вышеуказанной статье.  В январе 2013 г. был создан Европейский центр по борьбе с киберпреступностью, входящий в состав «Европола». | |
| Слайд 17 | Никто не знает к чему в будущем придет организация под названием «Евроюст», но в настоящее время она уже является крупным агентством, специализирующимся в области сотрудничества на уровне органов суда и прокуратуры между государствами-членами Европейского Союза. Цель «Евроюста» состоит в укреплении международного сотрудничества в борьбе с так называемой «крупной преступностью» путём координации работы национальных судебных органов.  В этих условиях «Евроюст» уполномочен способствовать координации действий компетентных органов власти различных государств-членов ЕС, а также содействовать работе международной системы взаимной юридической помощи и приведению в исполнение требований об экстрадиции.  Как юридическое лицо, «Евроюст» был создан в декабре 2000 г. во исполнение рекомендации саммита Европейского Совета в г. Тампере. В его состав входит по одному представителю от каждого из 27 государств-членов Европейского Союза. Борьба с компьютерной преступностью также относится к сфере полномочий «Евроюста». | |
| Слайд 18 | В июне 1998 г. была создана в рамках Европейского Союза «Европейская судебная сеть по уголовным делам», целью которой также является борьба с организованной преступностью и терроризмом в ЕС путём укрепления и упрощения сотрудничества между судебными органами государств-членов ЕС.  Практически эта сеть состоит из так называемых «пунктов связи», созданных на основе подразделений национальных центральных судебных органов, отвечающих в каждом из государств-членов ЕС за международное сотрудничество в судебной сфере. Такой «пункт связи» может быть представлен «связным» судьей.  Одна из задач «Европейской судебной сети по уголовным делам» состоит в предоставлении справочной информации судебным работникам других стран-членов ЕС с целью содействия международному сотрудничеству между государствами, каждое из которых имеет свою систему судоустройства и свой правовой режим. Учитывая подобные обстоятельства, сотрудники «Европейской судебной сети по уголовным делам» создали программное средство под названием «Атлас», позволяющее юристам легко находить на местах компетентные органы, уполномоченные в каждом из государств-членов ЕС получать запросы в рамках системы взаимной юридической помощи или же отвечать на них.  Предполагается, что местные судебные органы могут выходить на «пункты связи», которые призваны упростить сотрудничество в судебной сфере между государствами-членами ЕС, а также помогать этим органам оформлять заявки на предоставление информации в рамках такового сотрудничества.  Подобная организация, позволяющая делать это просто и без проволочек, может быть очень полезной при собирании электронных доказательств. | |
| Слайд 19 | Очевидно, что Европейская конвенция о взаимной правовой помощи по уголовным делам, принятая Советом Европы в 1959 году, стоит у истоков будапештской Конвенции о компьютерных преступлениях. Поэтому у разработчиков «Будапештской конвенции» не было намерения охватить все существующие вопросы международного сотрудничества; в её тексте содержатся ссылки лишь на новые, ранее не существовавшие и более оперативные каналы и механизмы сотрудничества.  Все государства-члены Совета Европы (за исключением Сан-Марино) ратифицировали эту конвенцию. Это значит, что из всех сторон «Будапештской конвенции» единственным не членом стороной конвенции 1959 г. являются Соединённые Штаты Америки.  Данный факт свидетельствует о дополнительной ценности «Будапештской конвенции», впервые устанавливающей единые правовые рамки международного сотрудничества между большинством европейских государств и США на уровне органов полиции и суда. Этот аспект особенно важен по следующей причине: пунктом 2 статьи 14 конвенции устанавливается, что её процессуальные нормы, регламентирующие международное сотрудничество, должны применяться не только к уголовным правонарушениям, предусмотренным статьями 2 – 11, но и к другим уголовным правонарушениям, совершенным с использованием компьютерных систем, а также к собиранию доказательств в электронной форме, свидетельствующих о совершении иных уголовно наказуемых деяний. | |
| Слайд 21 | Часть третья – Международные меры реагирования на киберпреступность: будапештская Конвенция о компьютерных преступлениях | |
| Слайды 22 - 25 | Как уже говорилось на предыдущих занятиях, «Будапештская конвенция» была открыта для подписания 23 ноября 2001 г. и вступила в силу в июле 2004 года. К апрелю 2013 г. 57 государств были либо сторонами конвенции, либо подписали её или же получили приглашение присоединиться к ней.    Применительно к конкретным делам в сфере киберпреступности, стороны конвенции получают в своё распоряжение новаторские инструменты расследования, главным образом, в области международного сотрудничества. Вышеуказанные новые перспективы открываются там, где расследуемое преступление является одним из правонарушений, предусмотренных конвенцией, а также в других случаях, когда преступное деяние было совершено с использованием компьютерной системы, или же когда доказательства совершения такового записаны и хранятся на цифровых запоминающих устройствах. Об этом и идёт речь в статье 14 «Будапештской конвенции».  Впервые международное сообщество приложило совместные усилия для согласования и принятия универсального договора в сфере сетевой компьютерной преступности (киберпреступности) и использования доказательств в электронной форме (электронных доказательств) в надежде на то, что возможно большинство государств действительно встанет на защиту его целей и задач. На сегодняшний день «Будапештская конвенция» остаётся первым и единственным международным договором о киберпреступности, имеющим обязательную юридическую силу.  Каждая страна, ратифицировавшая эту конвенцию и ставшая её стороной, получает очень важный доступ к универсальным инструментам сотрудничества одновременно с полицейскими и судебными органами остальных государств-сторон.  «Будапештской конвенцией» создаются новые каналы и инструменты международного сотрудничества. Некоторые её положения являются в высшей степени новаторскими и исключительными, что не мешает рассматривать их как адекватную и необходимую реакцию на новые проявления киберпреступности.  Тем не менее, Конвенция о компьютерных преступлениях является не только обязательным к исполнению договором, посвящённым вопросам международного сотрудничества. В статье 23 конвенции указывается, что сама она подлежит применению в рамках других существующих значимых инструментов международного сотрудничества в сфере борьбы с уголовной преступностью. И далее, в статье 27 описываются общие принципы, которые следует соблюдать при отсутствии иных применимых в подобных случаях международных конвенций или договоров.  С другой стороны, следует подчеркнуть, что процессуальными правилами, вводимыми статьями «Будапештской конвенции», создаются новые инструменты и каналы сотрудничества между её сторонами. Эти новые механизмы отсутствовали в ранее существовавших международных юридических документах. | |
| Слайд 27 | Часть четвёртая – «Будапештская конвенция» - инструменты международного сотрудничества  Положения «Будапештской конвенции», относящиеся к международному сотрудничеству, излагаются в главе III этого документа. В большинстве своём это материальные и процессуальные нормы, присутствующие также и в других международных конвенциях. Остальные же носят более новаторский характер и должны быть объяснены более детально. | |
| Слайды 28 и 29 | Статья 26 конвенции относится к ситуации, когда органы власти одной стороны конвенции раскрывают в ходе ведущегося на их территории расследования некую информацию, которую – по их мнению – необходимо довести до сведения компетентных органов другой стороны, не получив при этом от неё никакого запроса. Это может происходить в тех случаях, когда полученные сведения представляются полезными или же необходимыми для открытия расследования уголовного правонарушения, предусмотренного положениями «Будапештской конвенции». В то время как раньше предоставление взаимной помощи было абсолютно пассивным (то есть, государство «А» обращалось с просьбой об оказании помощи к государству «Б»), то конвенцией поощряется более инициативный подход. Тем не менее, в соответствии с пунктом 2 статьи 26 конвенции, такое «самопроизвольное» предоставление «внеплановой» информации может быть обусловлено, например, требованием о неразглашении переданных сведений или же об ограниченном их использовании. | |
| Слайды 30 - 32 | В статье 29 излагается одно из самых главных положений «Будапештской конвенции». Ею определяются правила, касающиеся оперативного обеспечения сохранности данных, хранящихся в компьютерной системе на территории, подпадающей под другую юрисдикцию. Этим задаётся правовая структура параллельная существующей внутригосударственной совокупности норм, регламентирующих данную сферу. В общем, этим положением разрешается одной договаривающейся стороне ходатайствовать перед другой стороной об оперативном обеспечении сохранность данных, если одновременно запрашивающая сторона выразит своё намерение оформить официальный запрос о предоставлении ей помощи в производстве обыска, выемки или же иных подобных действий.  В таком случае, запрашиваемая сторона обязана предпринять соответствующие шаги, чтобы оперативно и с должным усердием обеспечить сохранность указанных в запросе данных, действуя при этом в соответствии с требованиями своего внутреннего законодательства.  Как уже указывалось выше, это один из новых инструментов международного сотрудничества, содержащихся в «Будапештской конвенции». Необходимость его разработки объясняется особой природой работы в информационном пространстве. Всем известно, что реакция на запрос об оказании международной помощи наступает не сразу. Оперативный характер принимаемых мер диктуется необходимостью срочно обеспечить сохранность данных, которые могут быть полностью удалены в самые кратчайшие сроки.  Здесь важно указать на то, что в данном случае речь идёт лишь о мере по обеспечению сохранности, принимаемой в связи со срочностью вопроса, и не предполагающей автоматического раскрытия информации, содержащейся в сохраняемых таким образом данных. В действительности же, там, где раскрытие информации разрешено, применяются очень жесткие, ограничительные правила (если только не имеются в виду просто параметры передачи цифровых данных).  На практике, после оперативного обеспечения сохранности данных, произведённого по запросу, могут выясниться причины, по которым нельзя раскрывать их содержание запрашивающей стороне.  Важно здесь учитывать и то, что запрашиваемая сторона не может ставить в качестве условия обеспечения сохранности данных наличие двойной наказуемости. | |
| Слайды 33 и 34 | Раскрытие параметров передачи цифровых данных является предметом статьи 30 «Будапештской конвенции». Для решения этого вопроса в тексте конвенции прописывается упрощённый механизм производства данного действия с целью облегчения международного сотрудничества. Конвенцией не предусматривается никаких особых процессуальных правил произведения оперативного раскрытия вышеуказанных данных точно так же, как их не существует и во внутригосударственном праве на национальном уровне. Таким образом, хотя этого нигде явно не сказано, Конвенция о компьютерных преступлениях де факто сближает («гармонизирует») национальные правовые нормы, регламентирующие оперативное обеспечение сохранности/раскрытия цифровых данных, с одной стороны, и соответствующие положения в сфере международного сотрудничества, с другой. | |
| Слайды 35 и 36 | В статье 31 конвенции определяются общие нормы, регламентирующие оказание взаимопомощи при доступе к хранящимся компьютерным данным. В этой статье, а также в статье 23, на которую она ссылается, выражено общее пожелание того, чтобы стороны «максимально широко» сотрудничали при расследовании и судебном разбирательстве дел в сфере киберпреступности. Но новые обязательные механизмы сотрудничества в ней отсутствуют. Иными словами, все виды сотрудничества в сфере компьютерной преступности подпадают под действие уже существующих договоров и международных юридических документов, регламентирующих международное сотрудничество при расследовании обычных правонарушений.  Практически, в статье 31 «Будапештской конвенции» лишь утверждается применимость к киберпространству общих норм, уже многие годы существующих в реальной жизни. | |
| Слайды 37 и 38 | Статьей 32 конвенции предоставляется возможность правоохранительным органам одного государства – стороны конвенции получать доказательства, хранящиеся в компьютере, физически расположенном на территории другого госудасртва-стороны вышеуказанного договора, не прибегая при этом ни к какому запросу о международном сотрудничестве. Это можно сделать в том случае, если в рамках расследования ведущему его сотруднику необходимо получить открытую информацию из компьютера, расположенного на территории иностранного государства или же из компьютера, разрешение на доступ к которому было дано лицом, уполномоченным на то законом.  Касательно информации из открытых источников (открытой информации) следует заметить, что изучением «открытых источников» могут заниматься по собственной инициативе и простые гражданин большинства стран. Собственно говоря, смысл данной статьи заключается в том, чтобы разрешить сотрудникам правоохранительных органов делать это на законных основаниях и одновременно юридически фиксировать добытые таким образом сведения как имеющие доказательную силу.  Но у этого положения есть ещё одна совершенно неожиданная сторона. Дело в том, что в физическом материальном мире нет эквивалента новым возможностям, открывающимся в информационном пространстве: в прошлом уполномоченному сотруднику надо было самому ехать в другую страну и обращаться за помощью к местным властям. Сам он сделать ничего не мог, и на производство любого следственного действия ему надо было испрашивать дозволения местных органов власти.  В статье 32 «Будапештской конвенции» содержится обратное утверждение. В соответствии с ней, любой сотрудник правоохранительных органов из любой страны мира может получить информацию из другой страны, даже если эта информация и не «из открытых источников» при условии, что лицо, уполномоченное законом раскрыть таковые данные, даёт на то своё юридически значимое и добровольное согласие. Такие следственные действия не нуждаются ни в какой санкции со стороны государства, под юрисдикцией которого находится место хранения информации. Некоторые государства не могут спокойно воспринимать Конвенцию о компьютерных преступлениях в связи с этой формулировкой. Они утверждают, что таковая попирает принцип суверенитета. Тем не менее, никаких других контрпредложений или же иных решений сложных проблем «трансграничного» расследования дел или поиска доказательств в «компьютерных облаках» не поступало. Реальная жизнь показывает, что в большинстве случаев невозможно расследовать компьютерное преступление или же собирать электронные доказательства на международном уровне, используя традиционные методы и каналы. Невозможно потому, что по затраченному времени они несовместимы с недолговечностью («волатильностью») и неустойчивостью электронных доказательств. Вот почему сотрудник правоохранительных органов, расследующий дело с соблюдением новых правил «Будапештской конвенции», будет более эффективным.  Но, с другой стороны, иногда действительно бывает совершенно невозможно использовать обычные каналы сотрудничества. Чтобы в этом убедиться, достаточно взять пример хранения данных на удалённых серверах (на «компьютерных облаках»). В этом случае ни сами пользователи, ни следственные органы точно не знают, где физически хранятся те или иные данные, затребованные полицией. | |
| Слайды 39 и 40 | Статья 33 «Будапештской конвенции» касается вопросов международного сотрудничества в области перехвата сообщений. Её нельзя рассматривать, как новый инструмент в данной области: этот метод уже предусмотрен другими международными юридическими документами, обязательными к исполнению. В действительности, статья 33 конвенции нацелена на другое, а именно, на сбор в реальном времени параметров передачи цифровых данных.  С другой стороны, большинство важных норм, устанавливаемых статьей 33, содержат ссылки на пределы применения этой следственной меры. Они установлены материальными и процессуальными нормами внутригосударственного права. Соответственно, эта форма сотрудничества будет предусмотрена каждым государством в тех же случаях, что и сбор в реальном времени параметров передачи цифровых данных местными правоохранительными органами. | |
| Слайды 41 - 43 | Положения, содержащиеся в статье 35 «Будапештской конвенции», являются одними из наиболее важных для осуществления собственно оперативно-розыскной деятельности. Ими накладывается на все договаривающиеся стороны обязательство по созданию на своей территории постоянно действующих опорных пунктов («контактных центров»), входящих в состав так называемой «Сети 24/7», международной сети национальных контактных центров, работающих 24 часа в сутки 7 дней в неделю.  Общая задача этих контактных центров состоит в оказании содействия международному сотрудничеству. Они могут решать её путём предоставления технических консультаций другим контактным центрам, а также путём включения своих собственных механизмов оперативного обеспечения сохранности данных, собирания доказательств или же выявления и установления личности подозреваемых.  Эта постоянно действующая сеть опорных пунктов на местах, имеющая в своём составе экспертов в области высокотехнологичной преступности, задумывалась как инструмент оказания помощи другим специалистам из зарубежных стран или иных юрисдикций при расследовании уголовных дел с международными разветвлениями. Она призвана решать новые проблемы, возникающие в связи с быстрым ростом количества преступлений, совершаемых с использованием самых современных достижений науки и техники. Иногда следственные действия по раскрытию компьютерного преступления требуют весьма оперативного обеспечения сохранности электронных данных с тем, чтобы было возможно обнаружить местонахождение подозреваемых лиц и преследовать их по суду. Этого невозможно достичь с помощью ранее существовавших традиционных механизмов международного сотрудничества. Констатация данного факта повышает роль «Сети 24/7»: через неё можно очень оперативно предоставить/получить помощь и необходимые сведения, даже если потом и надо будет оформлять официальный запрос на них. | |
|  | **Практические занятия (при наличии необходимых условий)**  Не предусмотрены. | |
|  | Проверка знаний  Тренер должен проверить знания слушателей, задавая им конкретные вопросы по каждой из пройденных на занятиях тем. | |
| Слайды 45 и 46 | Подведение итогов занятия/выводы  Инструктору необходимо подвести итоги / проверить знания слушателей, которые должны быть в состоянии:   * осознать планетарные масштабы интернет сети и международный характер сетевой преступности (киберпреступности); * объяснить важность международного сотрудничества и выявить инструменты международного сотрудничества, имеющиеся в нашем распоряжении в борьбе с киберпреступностью; * оценить потребность в быстродействующих и эффективных каналах международного сотрудничества и в соответствующих инструментах; определить способы, сроки и действенность их использования; * описать усилия международных организаций по внедрению новых форм и механизмов международного сотрудничества; * обсудить будапештскую «Конвенцию о компьютерных преступлениях», определить основные утверждаемые в ней принципы, содержащиеся в конвенции обеспечительные меры, а также работу сети «24/7» по оказанию правовой взаимопомощи. | |

|  |  |  |
| --- | --- | --- |
| Занятие 1.3.5 Заключительное занятие | | **Продолжительность: 90 минут** |
| **Перечень материалов, необходимых для проведения занятия:**   * ноутбук или ПК с операционной системой Windows 7 и с загруженным офисным пакетом приложений MS Office 2010; * проектор с экраном; * презентация «ПауерПойнт»; * вопросники. | | |
| **Цель:**  На этом занятии слушателям должна быть предоставлена возможность высказать своё мнение о пройденном курсе и помочь ведущему его инструктору выявить моменты, нуждающиеся в совершенствовании. Инструктору же необходимо ещё раз пройтись по всему материалу курса и убедиться в том, что его цели и задачи достигнуты. | | |
| **Задачи:**  Во время этого занятия слушатели должны:   * высказать своё мнение об эффективности курса; * заполнить вопросники, оценивающие качество работы ведущих его инструкторов; * определить, на какой следующий уровень владения изучаемым предметом необходимо выйти для совершенствования своих теоретических знаний и практических навыков. | | |
| **Введение**  В рамках всего курса это занятие важное: оно необходимо для того, чтобы узнать мнение слушателей о его содержании и о методах подачи материала. На нём надо заполнить все оформленные в виде формуляров вопросники. Инструктору следует ещё раз пройтись по всем занятиям курса и убедиться в том, что его цели и задачи достигнуты. По окончании занятия инструктор несёт ответственность за учёт откликов аудитории и за внесение в курс необходимых изменений, касающихся как отдельных деталей, так и целых его модулей, нуждающихся в корректировке в соответствии с требованиями времени. | | |
| **Слайд №** | **Содержание:** | |
| Слайд 1 | Презентация «ПауерПойнт» (или созданная с помощью другой программы)  Настоящая презентация является вспомогательным подспорьем при обсуждении материала, пройденного в течение всего курса. До начала занятия инструктор должен раздать вопросники. При некоторых обстоятельствах может быть уместным выдать их на руки в самом начале прохождения курса с тем, чтобы слушатели заполняли формуляры по мере усвоения материала, пока свежи в памяти впечатления. Кроме того, под конец курса некоторые слушатели склонны к тому, чтобы не заполнять их полностью. | |
| Слайды 2 и 3 | Построенное по той же схеме, что и предыдущие, это занятие должно начинаться с изложения слушателям его плана и поставленных задач. | |
| Слайды 4 - 21 | Расписание занятий одновременно является и полезным наглядным пособием для обзорного восприятия слушателями содержания всего курса. Инструктору следует воспользоваться им для подведения итогов.  Инструктору необходимо бегло пройтись по планам и задачам всех занятий, собрав при этом отклики, замечания и соображения слушателей. Их следует записать для последующего использования. | |
| Слайд 22 | Инструктор отвечает за то, чтобы слушатели заполнили вопросники. После этого ему необходимо собрать их и передать представителю СЕ на курсе или же выслать в СЕ при первой же представившейся возможности. | |
|  | Практические занятия(при наличии необходимых условий)  Не предусмотрено (если не считать заполнения вопросников СЕ). | |
|  | **Проверка знаний**  Сам формат заключительного занятия очень подходит для проверки инструктором усвоения слушателями учебного материала путём их опроса во время сбора откликов аудитории. | |
|  | **Подведение итогов занятия/выводы**  Инструктор должен предоставить слушателям возможность высказаться и собрать их отклики. | |

# Оценка слушателями учебного материала и работы инструктора

Оценка качества учебного материала и работы инструктора является важной составной частью этого курса практических занятий. Таким образом, слушателям необходимо предоставить всё необходимое время для высказывания своих отзывов, комментариев и предложений относительно пройденного материала.

Курс разрабатывался как общий, и в таком качестве большая часть его учебного материала изложена на диапозитивах презентации «ПауерПойнт», хотя и без практических упражнений, которые обычно прилагаются к подобного рода пособиям.

Соответственно, был подготовлен формуляр вопросника, который следует далее в этом разделе. Инструктор отвечает за его заполнение и пересылку в Совет Европы с целью дальнейшего усовершенствования настоящего курса.

# Оценка уровня знаний, полученных слушателями

В рамках этого курса никакой проверки полученных знаний не требуется. Тем не менее, при изложении материала в будущем, особенно в тех странах, где учебная программа предполагает проведение аттестации, данный пункт может быть пересмотрен. Соответственно, в таком случае проводиться она должна в соответствии с установленным в этой стране порядком.

# Приложение

**Прилагаемые к курсу презентации «ПауерПойнт»**

Занятие 1.1.1 - Введение в курс

Занятие 1.1.2 - Введение в сетевую компьютерную преступность

Занятия 1.1.3, 1.2.2 & 1.2.5 – Технические средства

Занятие 1.3.1 - Обзор проделанной работы

Занятие 1.2.3 - Киберпреступление как уголовно наказуемое деяние в соответствии с положениями национального законодательства

Занятие 1.2.4 - Процессуальное внутригосударственное законодательство

Занятие 1.3.1 - Обзор проделанной работы

Занятия 1.3.2 & 1.3.3 - Доказательства в электронной форме

Занятие 1.3.4 - Международное сотрудничество

Занятие 1.3.5 - Заключительное занятие

1. Совместный проект Европейского Союза и Совета Европы «Усиление потенциала противодействия сетевой преступности (киберпреступности) в рамках регионального сотрудничества в области уголовного правосудия» (CyberCrime@IPA) направлен на укрепление эффективного сотрудничества между органами уголовного правосудия стран западной части Балканского полуострова и Турции в борьбе с сетевой преступностью («киберпреступностью»). [↑](#footnote-ref-1)
2. \* Любая ссылка на Косово в этом документа вне зависимости от того, идёт ли речь о самом территориальном образовании, его органах власти или же населении, должна толковаться в полном соответствии с положениями Резолюции № 1244 Совете Безопасности ООН и без какого бы то ни было ущерба для статуса Косово. [↑](#footnote-ref-2)
3. http://eur-lex.europa.eu/LexUriServ/site/en/oj/2005/l\_069/l\_06920050316en00670071.pdf [↑](#footnote-ref-3)
4. http://register.consilium.europa.eu/pdf/en/03/st14/st14583.en03.pdf [↑](#footnote-ref-4)
5. Поставщик интернет-услуг [↑](#footnote-ref-5)
6. [↑](#footnote-ref-6)
7. [↑](#footnote-ref-7)