КОНВЕНЦИЯ О КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЯХ

ПРОТОКОЛ О КСЕНОФОБИИ И РАСИЗМА

Пояснительные доклады и инструктивные указания

www.coe.int/cybercrime

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Конвенция о компьютерных преступлениях (СЕД № 185)

Протокол о ксенофобии и расизма

Пояснительные Доклады
и Инструктивные Указания

Índice

Конвенция о компьютерных преступлениях (СЕД № 185)

Государства - члены Совета Европы и другие государства, подписавшие настоящую Конвенцию,

Учитывая, что цель Совета Европы состоит в достижении большей степени единства между его членами;

Признавая важность укрепления сотрудничества с другими государствами, подписавшими настоящую Конвенцию;

Будучи убеждены в необходимости проведения в приоритетном порядке общей политики в сфере уголовного права, нацеленной на защиту общества от компьютерных преступлений, в том числе путем принятия соответствующих законодательных актов и укрепления международного сотрудничества;

Сознавая глубокие перемены, вызванные внедрением цифровых технологий, объединением и продолжающейся глобализацией компьютерных сетей;

Будучи озабочены угрозой того, что компьютерные сети и электронная информация могут также использоваться для совершения уголовных преступлений и что доказательства совершения таких правонарушений могут храниться в этих сетях и передаваться по ним;

Признавая необходимость сотрудничества между государствами и частным сектором в борьбе против компьютерных

преступлений и необходимость защиты законных интересов в сфере использования и развития информационных технологий;

Полагая, что для эффективной борьбы против компьютерных преступлений требуется более широкое, оперативное и хорошо отлаженное международное сотрудничество в области уголовного права;

Будучи убеждены в том, что настоящая Конвенция необходима для сдерживания действий, направленных против конфиденциальности, целостности и доступности компьютерных систем и сетей и компьютерных данных, а также против злоупотребления такими системами, сетями и данными, путем обеспечения уголовной наказуемости таких деяний, описываемых в настоящей Конвенции, и предоставления полномочий, достаточных для эффективной борьбы с такими уголовными преступлениями, путем содействия выявлению и расследованию таких уголовных преступлений и судебному преследованию за их совершение как на внутригосударственном, так и на международном уровнях и путем разработки договоренностей относительно оперативного и надежного международного сотрудничества;

Памятуя о необходимости обеспечения должного баланса между интересами поддержания правопорядка и уважением основополагающих прав человека, как это предусмотрено Конвенцией Совета Европы о защите прав человека и основных свобод от 1950 года, Международным пактом Организации Объединенных Наций о гражданских и политических правах от 1966 года и также другими применимыми

международными договорами о правах человека, в которых подтверждается право каждого беспрепятственно придерживаться своих мнений, а также право на свободное выражение своего мнения, включая свободу искать, получать и распространять всякого рода информацию и идеи, независимо от государственных границ и права, касающегося невмешательства в личную жизнь;

Памятуя также о праве на защиту персональных данных, предусмотренном, например, в Конвенции Совета Европы 1981 года о защите физических лиц при автоматизированной обработке персональных данных;

Учитывая положения Конвенции Организации Объединенных Наций о правах ребенка от 1989 года и Конвенции, принятой Международной Организацией Труда о наихудших формах детского труда от 1999 года;

Принимая во внимание действующие конвенции Совета Европы о сотрудничестве в пенитенциарной сфере, а также аналогичные договоры, заключенные между государствами - членами Совета Европы и другими государствами, и подчеркивая, что настоящая Конвенция призвана служить дополнением к этим договорам в целях повышения эффективности уголовных расследований и процессуальных действий в отношении уголовных преступлений, связанных с компьютерными системами и компьютерными данными, а также обеспечения возможности сбора доказательств в электронной форме совершения уголовного преступления;

Приветствуя события последнего времени, способствующие дальнейшему росту международного взаимопонимания и сотрудничества в борьбе с киберпреступностью, включая меры, принятые Организацией Объединенных Наций, ОЭСР, Европейским Союзом и «Группой восьми»;

Напоминая о Рекомендациях Комитета Министров № R (85) 10 относительно практического применения Европейской конвенции о взаимной правовой помощи по уголовным делам в том, что касается судебных поручений о перехвате телекоммуникационных сообщений, № R (88) 2 о борьбе с пиратством в области авторского права и смежных прав, № R (87)15 о порядке использования персональных данных полицией, № R (95) 4 о защите персональных данных в сфере телекоммуникационных услуг, в особенности телефонных услуг, а также № R (89)9 о преступлениях, связанных с компьютерами, в которой изложены руководящие принципы для национальных законодательных органов в отношении определения некоторых компьютерных преступлений, и № R (95) 13 по проблемам уголовно - процессуального права, связанным с информационными технологиями;

Принимая во внимание Резолюцию № 1, принятую на 21 - ой Конференции министров юстиции стран Европы (Прага, 10 и 11 июня 1997 г.),. в которой Комитету Министров было рекомендовано поддержать проводимую Европейским комитетом по проблемам преступности (ЕКПП) работу по компьютерным преступлениям, чтобы обеспечить большую согласованность положений внутреннего уголовного права и сделать возможным использование эффективных средств расследования таких правонарушений, а также принятую на 23 - й

Конференции министров юстиции стран Европы (Лондон, 8 и 9 июня 2000 г.) Резолюцию № 3, побуждающую участвующие в переговорах стороны продолжать усилия в целях нахождения таких решений, которые позволят как можно большему числу государств стать участниками Конвенции, и подтверждающую необходимость создания оперативной и эффективной системы международного сотрудничества, должным образом учитывающей специфические потребности борьбы с преступностью в сфере компьютерных преступлений;

Принимая во внимание также одобренный на Втором совещании глав государств и правительств Совета Европы (Страсбург, 10 и 11 октября 1997 г.) План действий по поиску общих мер реагирования на развитие новых информационных технологий на основе норм и ценностей, принятых в Совете Европы;

Согласились о нижеследующем:

Глава I – Использование терминов

Статья 1 – Определения

Для целей настоящей Конвенции:

a. "компьютерная система" означает любое устройство или группу взаимосвязанных или смежных устройств, одно или более из которых, действуя в соответствии с программой, осуществляет автоматизированную обработку данных;

b. "компьютерные данные" означают любое представление фактов, информации или понятий в форме, подходящей для обработки в компьютерной системе, включая

программы, способные обязать компьютерную систему выполнять ту или иную функцию;

c. "поставщик услуг" означает:

i. любую государственную или частную структуру, которая обеспечивает пользователям ее услуг возможность обмена информацией посредством компьютерной системы,

ii. любую другую структуру, которая осуществляет обработку или хранение компьютерных данных от имени такой службы связи или пользователей такой службы;

d. "данные о потоках" означают любые компьютерные данные, относящиеся к передаче информации посредством компьютерной системы, которые генерируются компьютерной системой, являющейся составной частью соответствующей коммуникационной цепочки, и указывают на источник, назначение, маршрут, время, дату, размер, продолжительность или тип соответствующего сетевого сервиса.

Глава II – Меры, которые следует принять на национальном уровне

Часть 1 – Материальное уголовное право

Подраздел 1 – Преступления против конфиденциальности, целостности и доступности компьютерных данных и систем

Статья 2 – Противозаконный доступ

Каждая Сторона принимает законодательные и иные меры, необходимые для того, чтобы квалифицировать в качестве

уголовного преступления согласно ее внутригосударственному праву доступ, когда он является преднамеренным, к компьютерной системе в целом или любой ее части неправомерно. Любая Сторона может требовать, чтобы такие деяния считались преступными, если они совершены с нарушениями мер безопасности и с намерением завладеть компьютерными данными или иным умыслом или в отношении компьютерной системы, соединенной с другой компьютерной системой.

Статья 3 – Неправомерный перехват

Каждая Сторона принимает законодательные и иные меры, необходимые для того, чтобы квалифицировать в качестве уголовного преступления согласно ее внутригосударственному праву - умышленно осуществленный с использованием технических средств перехват неправомерно не предназначенных для общего пользования компьютерных данных, передаваемых в компьютерную систему, из нее или внутри такой системы, включая электромагнитные излучения компьютерной системы, несущей такие компьютерные данные. Любая Сторона может требовать, чтобы такое деяние считалось преступным, если оно было совершено с умыслом или в отношении компьютерной системы, соединенной с другой компьютерной системой.

Статья 4 – Воздействие на данные

1. Каждая Сторона принимает законодательные и иные меры, необходимые для того, чтобы квалифицировать в качестве уголовного преступления согласно ее внутригосударственному праву умышленное повреждение,

удаление, ухудшение качества, изменение или блокирование компьютерных данных неправомерно.

2. Любая Сторона может сохранить за собой право квалифицировать в качестве уголовного преступления только те предусмотренные пунктом 1 деяния, которые влекут за собой серьезный ущерб..

Статья 5 – Воздействие на функционирование системы

Каждая Сторона принимает законодательные и иные меры, необходимые для того, чтобы квалифицировать в качестве уголовного преступления согласно ее внутригосударственному праву умышленное создание неправомерно серьезных помех функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, ухудшения качества, изменения или блокирования компьютерных данных.

Статья 6 – Противозаконное использование устройств

1. Каждая Сторона принимает законодательные и иные меры, необходимые для того, чтобы квалифицировать в качестве уголовного преступления согласно ее внутригосударственному праву нижеследующие деяния в случае их совершения умышленно и неправомерно

a. Производство, продажа, приобретение для использования, импорт, оптовая продажа или иные формы предоставления в пользование:

i. Устройств, включая компьютерные программы, разработанных или адаптированных прежде всего для

целей совершения какого - либо из правонарушений, предусмотренных выше Статьями 2 - 5;

ii. Компьютерных паролей, кодов доступа или иных аналогичных данных, с помощью которых может быть получен доступ к компьютерной системе в целом или любой ее части, с намерением использовать их в целях совершения какого - либо из правонарушений, предусмотренных Статьями 2 -5;

b. владение одним из предметов, упомянутых в пунктах «a» «i» или «ii» выше, с намерением использовать его для совершения каких - либо правонарушений, предусмотренных Статьями 2 - 5. Любая Сторона может требовать в соответствии с законом, чтобы условием наступления уголовной ответственности являлось владение несколькими такими предметами.

2. Настоящая Статья не должна толковаться как устанавливающая уголовную ответственность в тех случаях, когда производство, продажа, приобретение для использования, импорт, оптовая продажа или иные формы предоставления в пользование или владение, упомянутые в пункте 1 данной Статьи, не имеют целью совершение правонарушений, предусмотренных Статьями 2 - 5 настоящей Конвенции, а связаны, например, с разрешенным испытанием или защитой компьютерной системы.

3. Сторона может сохранить за собой право не применять положения пункта 1 настоящей Статьи при условии, что такая оговорка не будет касаться продажи, оптовой продажи или иных форм предоставления в пользование предметов, указанных в пункте «a» «ii» настоящей Статьи.

Подраздел 2 – Правонарушения, связанные с использованием компьютерных средств

Статья 7 – Подлог с использованием компьютерных технологий

Каждая Сторона принимает законодательные и иные меры, необходимые для того, чтобы квалифицировать в качестве уголовных преступлений согласно ее внутригосударственному праву в случае совершения умышленно и неправомерно ввод, изменение, стирание или блокирование компьютерных данных влекущих за собой нарушение аутентичности данных с намерением, чтобы они рассматривались или использовались в юридических целях в качестве аутентичных, независимо от того, поддаются ли эти данные непосредственному прочтению и являются ли они понятными. Любая Сторона может требовать для наступления уголовной ответственности наличия намерения совершить обман или аналогичного злого умысла.

Статья 8 – Мошенничество с использованием компьютерных технологий

Каждая Сторона принимает законодательные и иные меры, необходимые для того, чтобы квалифицировать в качестве уголовных преступлений согласно ее внутригосударственному праву -в случае совершения умышленно и неправомерно - лишения другого лица его собственности путем:

a. любого ввода, изменения, удаления или блокирования компьютерных данных;

b. любого вмешательства в функционирование компьютерной системы, мошенническим или бесчестным намерением неправомерного извлечения экономической выгоды для себя или для иного лица.

Подраздел 3 – Правонарушения, связанные с содержанием данных

Статья 9 – Правонарушения, связанные с детской порнографией

1. Каждая Сторона принимает законодательные и иные меры, необходимые для того, чтобы квалифицировать в качестве уголовных преступлений согласно ее внутригосударственному праву в случае совершения умышленно и неправомерно следующих деяний:

a. производство детской порнографической продукции в целях распространения через компьютерную систему;

b. предложение или предоставление в пользование детской порнографии через компьютерную систему;

c. распространение или передача детской порнографии через компьютерную систему;

d. приобретение детской порнографии через компьютерную систему для себя или для другого лица;

e. владение детской порнографией, находящейся в компьютерной системе или на носителях компьютерных данных.

2. Для целей параграфа 1 настоящей Статьи в понятие "детская порнография" включаются порнографические материалы, изображающие:

a. участие несовершеннолетнего лица в откровенных сексуальных действиях;

b. участие лица, кажущегося несовершеннолетним, в откровенных сексуальных действиях;

c. реалистические изображения несовершеннолетнего лица, участвующего в откровенных сексуальных действиях.

3. Для целей вышеприведенного параграфа 2 термин "несовершеннолетние" означает любое лицо, не достигшее 18 - летнего возраста. Однако любая Сторона может устанавливать и более низкие возрастные пределы, но не ниже 16 лет.

4. Каждая Сторона может сохранить за собой право не применять, полностью или частично, положения подпараграфов «d» и «e» параграфа 1, а также подпараграфов «b» и «c» параграфа 2.

Подраздел 4 – Правонарушения, связанные с нарушением авторского права и смежных прав

Статья 10 – Правонарушения, связанные с нарушением авторского права и смежных прав

1. Каждая Сторона принимает законодательные и иные меры, необходимые для того, чтобы квалифицировать в качестве уголовного преступления согласно ее

внутригосударственному праву нарушений авторского права, как они определены в законодательстве этой Стороны во исполнение обязательств, взятых ею на себя по Парижскому Акту от 24 июля 1971 года, пересматривающему Бернскую Конвенцию об Охране Литературных и Художественных Произведений, по Соглашению о Торговых Аспектах Прав Интеллектуальной Собственности и по Договору об Авторском Праве Всемирной Организации Интеллектуальной Собственности (ВОИС) когда такие действия совершаются умышленно в коммерческом масштабе и с помощью компьютерной системы, за исключением любых моральных прав, предоставляемых этими Конвенциями.

2. Каждая Сторона принимает законодательные и иные меры, необходимые для того, чтобы квалифицировать в качестве уголовных преступлений согласно внутригосударственному праву нарушения прав, связанных с авторским правом, как оно определено законодательством этой Стороны во исполнение обязательств, взятых ею на себя согласно Международной Конвенции об Охране Интересов Артистов - исполнителей, Производителей Фонограмм и Вещательных Организаций (Римская Конвенция), Соглашению о Торговых Аспектах Прав Интеллектуальной Собственности и Договору ВОИС об Исполнителях и Фонограммах, когда такие акты совершены умышленно, в коммерческом масштабе и с помощью компьютерной системы, за исключением любых моральных прав.

3. Любая Сторона может сохранить за собой права в некоторых обстоятельствах не привлекать виновных к уголовной ответственности согласно положениям

параграфов 1 и 2 настоящей Статьи при условии, что имеются другие эффективные средства правовой защиты и что такая оговорка не ведет к частичной отмене Стороной своих международных обязательств, предусмотренных международными документами, упомянутыми в параграфах 1 и 2 настоящей Статьи.

Подраздел 5 – Дополнительные виды ответственности и санкции

Статья 11 – Покушение, соучастие или подстрекательство к совершению преступления

1. Каждая Сторона принимает законодательные и иные меры, необходимые для того, чтобы квалифицировать в качестве уголовных преступлений согласно ее внутригосударственному праву в случае, когда это делается умышленно, соучастие или подстрекательство к совершению любого правонарушения, предусмотренного положениями Статей 2 - 10 настоящей Конвенции.

2. Каждая Сторона принимает законодательные и иные меры, которые могут потребоваться для того, чтобы квалифицировать в качестве уголовных преступлений согласно ее внутригосударственному праву в случае, когда это делается умышленно, покушения на совершение любого правонарушения, предусмотренного положениями Статей 3 - 5, 7, 8, 9.1 «a» и «c» настоящей Конвенции.

3. Каждое Государство может сохранить за собой право не применять полностью или частично, положения параграфа 2 настоящей Статьи.

Статья 12 – Корпоративная ответственность

1. Каждая Сторона принимает законодательные и иные меры, необходимые для обеспечения возможности привлечения юридических лиц к ответственности за уголовное преступление, предусмотренное в соответствии с настоящей Конвенцией, которое совершается в его пользу любым физическим лицом, действующим самостоятельно или как часть одного из органов соответствующего юридического лица и занимающим ведущее положение него на основании:

a. полномочий представлять данное юридическое лицо;

b. права принимать решения от имени этого юридического лица;

c. рава осуществлять контроль внутри этого юридического лица.

2. В дополнение к случаям, уже предусмотренным в параграфом 1 настоящей Статьи, каждая Сторона принимает меры, необходимые для обеспечения возможности возложения ответственности на юридическое лицо в случаях, когда отсутствие руководства или контроля со стороны физического лица, упомянутого в параграфе 1, делает возможным совершение уголовного преступления, предусмотренного положениями настоящей Конвенции, в пользу этого юридического лица физическим лицом, действующим на основании данных ему полномочий.

3. В зависимости от применяемых соответствующей Стороной юридических принципов ответственность юридического лица может носить уголовный, гражданский или административный характер.

4. Такая ответственность не влечет за собой какого - либо смягчения и не снижает уголовной ответственности физических лиц, совершивших преступление.

Статья 13 – Санкции и меры

1. Каждая Сторона принимает законодательные и иные меры, необходимые для обеспечения того, чтобы к лицам, совершившим уголовные преступления, предусмотренные в соответствии с положениями Статей 2 - 11, эффективные, соразмерные и убедительные меры наказания, включая лишения свободы.

2. Каждая Сторона гарантирует, что к юридическим лицам, считающимся ответственными в соответствии с положениями Статьи 12, будут применены эффективные, соразмерные и убедительные меры наказания уголовного или не уголовного характера, включая денежные санкции.

Часть 2 – Процессуальное законодательство

Подраздел 1 – Общие положения

Статья 14 – Сфера применения процессуальных норм

1. Каждая Сторона принимает законодательные и иные меры, необходимые для установления полномочий и процедур, предусмотренных положениями настоящего раздела в целях проведения конкретных уголовных расследований или судебного разбирательства.

2. За исключением случаев, когда положениями Статьи 21 конкретно предусматривается иное, каждая Сторона

применяет полномочия и процедуры, упомянутые в параграфе 1 настоящей Статьи, в отношении:

a. уголовных преступлений, предусмотренных в соответствии со Статьями 2 - 11 настоящей Конвенции;

b. других уголовных преступлений, совершенных при помощи компьютерной системы;

c. сбора доказательств в электронной форме уголовного преступления.

3.a. Каждая Сторона может сделать оговорку о сохранении за собой права применять меры, упомянутые в Статье 20, только в отношении правонарушений или категорий правонарушений, указанных в этой оговорке, при условии, что круг таких правонарушений или категорий правонарушений не более ограничен, чем круг правонарушений, к которым она применяет меры, предусмотренные в Статье 21. Каждая Сторона рассматривает пути ограничения сферы действия такой оговорки, чтобы сделать возможным максимально широкое применение мер, упомянутых в Статье 20.

b. В том случае, когда Сторона ввиду ограничений в своем законодательстве, действующем на момент принятия настоящей Конвенции, не имеет возможности применить меры, предусмотренные Статьями 20 и 21, к информации, передаваемой по компьютерной системе поставщика услуг, которая:

i. используется для обслуживания замкнутой группы пользователей,

ii. не использует общественных сетей связи, а также не соединена ни с какими другими компьютерными системами, будь то общественными или частными, эта Сторона может сохранить за собой право не применять указанных мер к такой передаче информации. Каждая Сторона рассматривает пути ограничения этого права с тем, чтобы сделать возможным максимально широкое применение мер, упомянутых в Статьях 20 и 21.

Статья 15 – Условия и гарантии

1. Каждая Сторона обеспечивает, чтобы установление, исполнение и применение полномочий и процедур, предусмотренных настоящим Разделом, осуществлялись в соответствии с условиями и гарантиями, предусмотренными нормами ее внутригосударственного права, обеспечивающими надлежащую защиту прав человека и свобод, включая права, вытекающие из обязательств, которые Сторона взяла на себя по Европейской Конвенции о Защите Прав Человека и Основных Свобод, принятой Советом Европы в 1950 году Международным пактом о Гражданских и Политических Правах, принятым Организацией Объединенных Наций в 1966 году, а также другими применимыми международными договорами по правам человека и предусматривающими принцип соразмерности.

2. Такие условия и гарантии с учетом характера полномочий и процедур включают, среди прочего, судебный или иной независимый надзор, основания правомочности применения, ограничение сферы и сроков действия таких полномочий или процедур.

3. В той мере, в какой это соответствует общественным интересам, в частности обоснованному отправлению правосудия, Сторона рассматривает влияние предусмотренных данным разделом полномочий и процедур на права, ответственность и законные интересы третьих сторон.

Подраздел 2 – Оперативное обеспечение сохранности накопленных компьютерных данных

Статья 16 – Оперативное обеспечение сохранности хранимых компьютерных данных

1. Каждая Сторона принимает законодательные и иные меры, необходимые для того, чтобы ее компетентные органы имели возможность путем выпуска распоряжений или иным образом оперативно обеспечивать сохранностьконкретных компьютерных данных, включая данные о потоках информации, которые хранятся в компьютерной системе, в частности, когда имеются основания полагать, что эти компьютерные данные особенно подвержены риску утраты или изменения.

2. Если Сторона реализует положения приведенного выше параграфа 1 посредством выпуска распоряжения какому - либо лицу об обеспечении сохранности конкретных хранимых компьютерных данных, находящихся во владении или под контролем этого лица, то эта Сторона принимает такие законодательные и иные меры, какие могут быть необходимы для того, чтобы обязать данное лицо хранить эти компьютерные данные и обеспечивать их целостность в течение необходимого периода времени, не превышающего девяноста дней, с тем чтобы компетентные органы могли

добиться раскрытия этих компьютерных данных. Сторона может предусмотреть возможность последующего продления действия такого распоряжения.

3. Каждая Сторона принимает законодательные и иные меры, необходимые для того, чтобы обязать хранителя или другое лицо, которому поручено обеспечивать сохранность компьютерных данных, сохранять конфиденциальность выполнения таких процедур в течение срока, предусмотренного ее внутригосударственным правом.

4. Полномочия и процедуры, упомянутые в настоящей Статье, устанавливаются в соответствии с положениями Статей 14 и 15.

Статья 17 – Оперативное обеспечение сохранности и частичное раскрытие данных о потоках информации

1. Каждая Сторона принимает в отношении данных о потоках информации, сохранность которых должна быть обеспечена в соответствии с положениями Статьи 16, такие законодательные и иные меры, какие могут быть необходимы для того, чтобы:

a. гарантировать, чтобы такое оперативное обеспечение сохранности данных о потоках информации было возможным независимо от того, сколько поставщиков услуг были вовлечены в передачу соответствующего сообщения один или более;

b. гарантировать оперативное раскрытие компетентным органам этой Стороны или лицу, назначенному этими органами, достаточного количества данных о потоках

информации, которое позволит соответствующей Стороне идентифицировать поставщиков услуг и путь, которым передавалось данное сообщение.

2. Полномочия и процедуры, упомянутые в настоящей Статье, устанавливаются в соответствии с положениями Статей 14 и 15.

Подраздел 3 – Распоряжение о предъявлении

Статья 18 – Распоряжение о предъявлении

1. Каждая Сторона принимает законодательные и иные меры, необходимые для того, чтобы предоставить ее компетентным органам полномочия отдавать распоряжения:

a. лицу на ее территории - о предъявлении конкретных компьютерных данных, находящихся во владении или под контролем этого лица, которые хранятся в компьютерной системе или на том или ином носителе компьютерных данных;

b. поставщику услуг, предлагающему свои услуги на ее территории, - о предъявлении находящихся во владении или под контролем этого поставщика услуг сведений о его абонентах.

2. Полномочия и процедуры, упомянутые в настоящей Статье, устанавливаются в соответствии с положениями Статей 14 и 15.

3. Для целей настоящей Статьи термин "сведения об абонентах" означает любую имеющуюся у поставщика услуг информацию о его абонентах в форме компьютерных

данных или любой другой форме, кроме данных о потоках или содержании информации, с помощью которой можно установить:

a. вид используемой коммуникационной услуги, принятые с этой целью меры технического обеспечения и период оказания услуги;

b. личность пользователя, его почтовый или географический адрес, номера телефона и других средств доступа, сведения о выставленных ему счетах и произведенных им платежах, имеющиеся в соглашении или договоре на обслуживание;

c. любые другие сведения о месте установки коммуникационного оборудования, имеющиеся в соглашении или договоре на обслуживание.

Подраздел 4 – Обыск и выемка хранимых компьютерных данных

Статья 19 – Обыск и выемка хранимых компьютерных данных

1. Каждая Сторона принимает законодательные и иные меры, которые могут потребоваться для предоставления ее компетентным органам полномочий на обыск или иной аналогичный доступ к:

a. компьютерным системам или их частям, а также хранящимся в них компьютерным данным;

b. носителям компьютерных данных, на которых могут храниться искомые компьютерные данные, на ее территории.

2. Каждая Сторона принимает законодательные и иные меры, необходимые для обеспечения того, чтобы в случае, когда ее компетентные органы производят обыск или получают аналогичный доступ к определенной компьютерной системе или ее части в соответствии с положениями параграфа 1 «a» и имеют основания полагать, что искомые данные хранятся в другой компьютерной системе или ее части на территории этой Стороны, и когда такие данные на законном основании могут быть получены из первой системы или с ее помощью, такие органы имели возможность оперативно распространить производимый обыск или иной аналогичный доступ на другую систему.

3. Каждая Сторона принимает законодательные и иные меры, необходимые для предоставления ее компетентным органам полномочий производить выемку компьютерных данных, доступ к которым был получен в соответствии с положениями параграфов 1 или 2, или иным аналогичным образом обеспечивать их сохранность. Эти меры должны включать предоставление полномочий:

a. производить выемку компьютерной системы, ее части или носителей, используемых для хранения компьютерных данных, либо иным аналогичным образом обеспечивать их сохранность;

b. изготавливать и оставлять у себя копии соответствующих компьютерных данных;

c. обеспечивать целостность относящихся к делу хранимых компьютерных данных;

d. делать компьютерные данные, находящиеся в компьютерной системе, доступ в которую был получен, недоступными или изымать их из нее.

4. Каждая Сторона принимает законодательные и иные меры, необходимые для предоставления ее компетентным органам полномочий требовать от любого лица, обладающего знаниями о функционировании соответствующей компьютерной системы или применяемых мерах защиты хранящихся там компьютерных данных, предоставления в разумных пределах необходимых сведений, которые позволяют осуществить действия, предусмотренные параграфами 1 и 2.

5. Полномочия и процедуры, упомянутые в настоящей Статье, устанавливаются в соответствии с положениями Статей 14 и 15.

Подраздел 5 – Сбор компьютерных данных в режиме реального времени

Статья 20 – Сбор в режиме реального времени данных о потоках информации

1. Каждая Сторона принимает законодательные и иные меры, необходимые для предоставления ее компетентным органам полномочий:

a. собирать или записывать с применением технических средств на территории этой Стороны,

b. обязать поставщиков услуг в пределах имеющихся у них технических возможностей:

i. особирать или записывать с применением технических средств на территории этой Стороны;

ii. сотрудничать с компетентными органами и помогать им собирать или записывать в реальном режиме времени данные о потоках информации, связанные с конкретными сообщениями на территории этой Стороны, передаваемыми по компьютерной системе.

2. Если какая - либо Сторона в силу устоявшихся принципов ее системы внутригосударственного права не может принять меры, предусмотренные параграфом 1 «а», то вместо этого она может принять законодательные и иные меры, какие могут быть необходимы для обеспечения сбора или записи в режиме реального времени данных о потоках информации, связанных с указанными сообщениями, на ее территории путем применения технических средств на этой территории.

3. Каждая Сторона принимает законодательные и иные меры, необходимые для того, чтобы обязать поставщика услуг соблюдать конфиденциальность самого факта осуществления любых полномочий, предусмотренных настоящей Статье, и любой информации об этом.

4. Полномочия и процедуры, упомянутые в настоящей Статье, устанавливаются в соответствии с положениями Статей 14 и 15.

Статья 21 – Перехват данных о содержании

1. Каждая Сторона принимает законодательные и иные меры в отношении ряда серьезных правонарушений,

подлежащих квалификации в соответствии с нормами внутригосударственного права, необходимые для того, чтобы наделить ее компетентные органы полномочиями:

a. собирать или записывать с применением технических средств на территории этой Стороны,

b. обязать поставщика услуг в пределах имеющихся у него технических возможностей:

i. собирать или записывать с использованием технических средств на территории этой Стороны,

ii. сотрудничать с компетентными органами и помогать им в сборе или записи в режиме реального времени данных о содержании указанных сообщений на ее территории, передаваемых с помощью компьютерных систем.

2. Если какая - либо Сторона в силу устоявшихся принципов ее системы внутригосударственного права не может принять меры, предусмотренные параграфом 1 «a», то вместо этого она может принять законодательные и иные меры, какие могут быть необходимы для обеспечения сбора или записи в режиме реального времени данных о содержании указанных сообщений на ее территории путем применения технических средств на этой территории.

3. Каждая Сторона принимает законодательные и иные меры, необходимые для того, чтобы обязать поставщика услуг соблюдать конфиденциальность самого факта осуществления любых полномочий, предусмотренных настоящей Статьей, и любой информации об этом.

4. Полномочия и процедуры, упомянутые в настоящей Статье, устанавливаются в соответствии с положениями Статей 14 и 15.

Часть 3 – Юрисдикция

Статья 22 – Юрисдикция

1. Каждая Сторона принимает законодательные и иные меры, необходимые для установления юрисдикции в отношении любого правонарушения, предусмотренного в соответствии с положениями Статей 2 - 11 настоящей Конвенции, когда такое правонарушение совершено:

a. на ее территории;

b. на борту судна, плавающего под флагом этой Стороны;

c. на борту самолета, зарегистрированного согласно законам этой Стороны;

d. одним из ее граждан, если это правонарушение является уголовно наказуемым в месте его совершения или если это правонарушение совершено за пределами территориальной юрисдикции какого - либо Государства.

2. Каждая Сторона может сохранить за собой право не применять или применять только в определенных случаях или условиях нормы, касающиеся юрисдикции, установленные в параграфах 1.b-d настоящей Статьи или любой их части.

3. Каждая Сторона принимает меры, необходимые для установления юрисдикции в отношении правонарушений, упомянутых в параграфе 1 Статьи 24 настоящей Конвенции,

в случаях, когда предполагаемый правонарушитель находится на ее территории, и она не выдает его (ее) другой Стороне по получении запроса о выдаче, основываясь исключительно на его (ее) гражданстве.

4. Настоящая Конвенция не исключает никакую уголовную юрисдикцию, осуществляемую в соответствии с нормами внутригосударственного права.

5. Если на юрисдикцию в отношении предполагаемого правонарушения, предусмотренного в соответствии с настоящей Конвенцией, претендует более одной Стороны, заинтересованные Стороны по мере необходимости проводят консультации с целью определить наиболее подходящую юрисдикцию для осуществления судебного преследования.

Глава III – Международное сотрудничество

Часть 1 – Общие принципы

Подраздел 1 – Общие принципы международного сотрудничества

Статья 23 – Общие принципы международного сотрудничества

Стороны осуществляют максимально широкое сотрудничество друг с другом в соответствии с положениями настоящей главы и путем применения соответствующих международных документов о международном сотрудничестве по уголовным делам, согласованных договоренностей, опирающихся на единообразное или основанное на

взаимности законодательство, а также норм внутригосударственного права в целях проведения расследований или судебного преследования в отношении уголовных преступлений, связанных с компьютерными системами и данными, или сбора доказательств по уголовному преступлению в электронной форме.

Подраздел 2 – Принципы в отношении выдачи

Статья 24 – Выдача

1.a. Настоящая Статья применяется между Сторонами в отношении выдачи в связи с уголовными преступлениями, определенными в соответствии со Статьями 2 - 11 настоящей Конвенции, при условии, что согласно законам обеих заинтересованных Сторон за них предусматривается наказание в виде лишения свободы на максимальный срок не менее одного года или более суровое наказание.

b. В случаях, когда между двумя или более Сторонами действует соглашение, заключенное на основе единообразного или основанного на взаимности законодательства или договора о выдаче, включая Европейскую Конвенцию о выдаче (ETS № 024), согласно которым должно применяться иное минимальное наказание, применяется положение о минимальном наказании, предусмотренное в таком соглашении или договоре.

2. Уголовные преступления, предусмотренные параграфом 1 настоящей Статьи, рассматриваются как входящие в число преступлений, предполагающих выдачу, в любом двустороннем или многостороннем договоре о выдаче, существующем между Сторонами. Стороны обязуются включать

такие преступления в число преступлений, предполагающих выдачу, в любые двусторонние и многосторонние договоры о выдаче, которые будут заключены между ними.

3. Если какая - либо Сторона, выдвигающая в качестве условия выдачи наличие договора, получает запрос о выдаче от другой Стороны, с которой у нее нет договора о выдаче, она может рассматривать настоящую Конвенцию как юридическое основание для выдачи в связи с любым уголовным преступлением, упомянутым в параграфе 1 настоящей Статьи.

4 Стороны, не выдвигающие в качестве условия выдачи наличие договора, в отношениях между собой признают уголовные преступления, упомянутые в параграфе 1 настоящей Статьи, в качестве преступлений, предполагающих выдачу.

5. Выдача осуществляется в соответствии с условиями, предусмотренными законодательством запрашиваемой Стороны или применимыми договорами о выдаче, включая основания, на которых запрашиваемая Сторона может отказывать в выдаче.

6. Если отказ в выдаче в связи с одним из уголовных преступлений, упомянутых в параграфе 1 настоящей Статьи, мотивируется исключительно гражданством искомого лица или тем, что, по мнению запрашиваемой Стороны, данное преступление относится к ее юрисдикции, запрашиваемая Сторона по просьбе запрашивающей Стороны передает это дело своим компетентным органам в целях осуществления судебного преследования и своевременно сообщает запрашивающей Стороне об окончательном результате. Эти

органы принимают свое решение и проводят свое расследование и судебное разбирательство так же, как и в случае любого другого правонарушения сопоставимого характера согласно законам этой Стороны.

7.a. Каждая Сторона при подписании или сдаче на хранение своего документа о ратификации, принятии, об одобрении или о присоединении, сообщает Генеральному Секретарю Совета Европы наименование и адрес каждого органа, ответственного за направление или получение запроса о выдаче или предварительном аресте при отсутствии договора.

b. Генеральный Секретарь Совета Европы составляет и постоянно обновляет реестр органов, назначенных Сторонами с этой целью. Каждая Сторона обеспечивает то, чтобы в этом реестре всегда содержались постоянные данные.

Подраздел 3 – Общие принципы взаимной помощи

Статья 25 – Общие принципы взаимной помощи

1. Стороны на взаимной основе оказывают друг другу по возможности максимально правовую помощь в целях проведения расследований или судебного разбирательства в связи с уголовными преступлениями, связанными с компьютерными системами и данными, или сбора доказательств по уголовному преступлению в электронной форме.

2. Каждая Сторона также принимает такие законодательные и иные меры, какие могут быть необходимы для выполнения обязательств, изложенных в Статьях 27 - 35.

3. Каждая Сторона может в экстренных ситуациях направлять запросы о взаимной помощи или сообщения, связанные с такими запросами, используя оперативные средства связи, включая факсимильную связь или электронную почту, в той мере, в какой такие средства обеспечивают соответствующие уровни безопасности и подтверждения подлинности (включая, если необходимо, использование шифрования), с последующим официальным подтверждением, если того требует запрашиваемая Сторона. Запрашиваемая Сторона принимает такой запрос и отвечает на него с помощью любых аналогичных оперативных средств связи.

4. За исключением случаев, когда положениями статей настоящей главы конкретно предусматривается иное, взаимная помощь оказывается на условиях, предусмотренных законодательством запрашиваемой Стороны или положениями применимых договоров о взаимной помощи, включая основания, на которых запрашиваемая Сторона может отказаться от сотрудничества. Запрашиваемая Сторона не осуществляет права на отказ во взаимной помощи в отношении правонарушений, предусмотренных Статьями 2 - 11, исключительно на том основании, что запрос касается правонарушения, которое она рассматривает как финансовое правонарушение.

5. Когда в соответствии с положениями настоящей главы запрашиваемой Стороне разрешается выдвигать в качестве условия оказания взаимной помощи требование о том, чтобы соответствующее деяние рассматривалось как преступное обеими Сторонами, это условие считается выполненным независимо от того, относят ли данное правонарушение ее

законы к преступлениям той же категории или использует ли она для обозначения этого преступления ту же терминологию, что и запрашивающая Сторона, если деяние, лежащее в основе преступления, в связи с которым запрашивается помощь, является уголовным преступлением согласно ее законам.

Статья 26 – Внеплановая информация

1. Сторона может в пределах норм своего внутригосударственного права направить без предварительного запроса другой Стороне информацию, полученную в рамках своего собственного расследования, когда, по ее мнению, раскрытие такой информации могло бы помочь Стороне - получателю этой информации начать или провести расследование или судебное разбирательство в отношении уголовных преступлений, установленных в соответствии с положениями настоящей Конвенции, или могло бы повлечь за собой направление этой Стороной просьбы о сотрудничестве в соответствии с положениями настоящей главы.

2. Прежде чем предоставить такую информацию, предоставляющая Сторона может просить о соблюдении ее конфиденциальности или поставить определенные условия для ее использования. Если получающая Сторона не может выполнить такую просьбу, она уведомляет об этом предоставляющую Сторону, которая определяет затем, следует ли тем не менее предоставить такую информацию. Если получающая Сторона принимает информацию на указанных условиях, они носят для нее обязательный характер.

Подраздел 4 – Процедуры направления запросов о взаимной помощи в отсутствие применимых международных соглашений

Статья 27 – Процедуры направления запросов о взаимной помощи в отсутствие применимых международных соглашений

1. В случаях, когда между запрашивающей и запрашиваемой Сторонами нет действующего договора или соглашения о взаимной помощи, основанного на единообразном или принятом на началах взаимности законодательства, применяются положения параграфов 2 - 9 настоящей Статьи. При наличии такого договора, соглашения или законодательства положения данной Статьи не применяются, если только заинтересованные Стороны не соглашается применять взамен любые или все последующие положения настоящей Статьи.

2.a. Каждая Сторона назначает центральный орган или органы, которые несут ответственность за направление запросов о взаимной помощи и ответов на них, выполнение таких запросов или их передачу органам, в компетенцию которых входит их выполнение;

b. Эти центральные органы поддерживают связь непосредственно друг с другом;

c. Каждая Сторона при подписании настоящей Конвенции или при сдаче на хранение своей ратификационной грамоты или своего документа о принятии, об одобрении или о присоединении сообщает Генеральному Секретарю

Совета Европы наименования и адреса органов, назначенных в соответствии с настоящим параграфом;

d. Генеральный Секретарь Совета Европы составляет и постоянно обновляет реестр центральных органов, назначенных Сторонами. Каждая Сторона обеспечивает, чтобы в этом реестре всегда содержались достоверные сведения;

3. Запросы о взаимной помощи, направляемые согласно положениям настоящей Статьи, исполняются в соответствии с процедурами, указанными запрашивающей Стороной, за исключением случаев, когда они несовместимы с законодательством запрашиваемой Стороны.

4. Запрашиваемая Сторона может в дополнение к основаниям для отказа, предусмотренным параграфом 4 Статьи 25, отказать в предоставлении помощи, если:

a. запрос касается правонарушения, рассматриваемого запрашиваемой Стороной как политическое преступление или как правонарушение, связанное с политическим преступлением;

b. по ее мнению, выполнение запроса, по всей вероятности, приведет к подрыву ее суверенитета, безопасности, общественного порядка или иных существенных интересов.

5. Запрашиваемая Сторона может отложить принятие мер по запросу, если такие меры препятствовали бы уголовным расследованиям или судебным разбирательствам, проводимым ее органами.

6. Прежде чем отказать в предоставлении помощи или отсрочить ее оказание, запрашиваемая Сторона по мере

необходимости после консультаций с запрашивающей Стороной рассматривает возможность удовлетворения запроса частично или на таких условиях, какие она сочтет необходимыми.

7. Запрашиваемая Сторона незамедлительно информирует запрашивающую Сторону о результатах выполнения запроса о помощи. В случае отказа в выполнении запроса или отсрочки такого выполнения сообщаются причины такого отказа или отсрочки. Запрашиваемая Сторона также сообщает запрашивающей Стороне о любых причинах, по которым выполнение запроса становится невозможным или, по всей вероятности, будет осуществлено со значительной задержкой.

8. Запрашивающая Сторона может просить запрашиваемую Сторону обеспечить конфиденциальность факта и предмета любого запроса, сделанного в соответствии с положениями настоящей главы, но лишь в той степени, которая согласуется с его выполнением. Если запрашиваемая Сторона не может выполнить просьбу о сохранении конфиденциальности, она незамедлительно сообщает об этом запрашивающей Стороне, которая затем принимает решение о том, следует ли тем не менее направить запрос.

9.a. В случае крайней необходимости запросы о взаимной помощи или сообщения, связанные с такими запросами, могут направляться непосредственно судебными органами запрашивающей Стороны соответствующим органам запрашиваемой Стороны. В любых таких случаях одновременно направляется копия центральным органам запрашиваемой Стороны через центральные органы запрашивающей Стороны.

b. Любой запрос или сообщение, упомянутые в настоящей части, могут быть направлены через Международную Организацию Уголовной Полиции (Интерпол).

c. Когда запрос делается в соответствии с положениями под параграфа a. настоящей Статьи, а его рассмотрение не входит в компетенцию получившего его органа, последний направляет этот запрос в компетентный национальный орган и сообщает об этом непосредственно запрашивающей Стороне.

d. Направляемые в соответствии с положениями настоящего параграфа запросы или сообщения, которые не предполагают принятия принудительных мер, могут передаваться компетентными органами запрашивающей Стороны непосредственно компетентным органам запрашиваемой Стороны.

e. Каждая Сторона может при подписании Конвенции или при сдаче на хранение ратификационной грамоты или документа о принятии, об одобрении или о присоединении сообщить Генеральному Секретарю Совета Европы, что в целях обеспечения эффективности запросы, направляемые в соответствии с положениями настоящего параграфа, должны быть адресованы ее центральным органам.

Статья 28 – Конфиденциальность и ограничения на использование информации

1. В случае отсутствия между запрашивающей и запрашиваемой Сторонами действующего договора или соглашения о взаимной правовой помощи, опирающегося на

единообразное или основанное на принципе взаимности законодательство, применяются положения настоящей Статьи. Положения настоящей Статьи при наличии такого договора, соглашения или законодательства не применяются, если только заинтересованные Стороны не соглашаются применять вместо последних любые или все последующие положения настоящей Статьи.

2. В ответ на просьбу запрашиваемая Сторона может выдвинуть следующие условия предоставления информации или материала:

a. сохранение их конфиденциальности, если без такого условия просьба о взаимной правовой помощи не могла бы быть выполнена;

b. неиспользование для других расследований или судебных разбирательств, которые не указываются в просьбе.

3. Если запрашивающая Сторона не может выполнить одно из условий, упомянутых в параграфе 2, она незамедлительно информирует об этом другую Сторону, которая затем решает, может ли быть предоставлена такая информация. Если запрашивающая Сторона соглашается выполнить эти условия, они приобретают для нее обязательную силу.

4. Любая Сторона, предоставляющая информацию или материал на упомянутых в параграфе2 условиях, может в связи с одним из условий потребовать от другой Стороны разъяснений относительно имевшего место использования такой информации или материала.

Часть 2 – Конкретные положения

Подраздел 1 – Взаимная помощь в связи с предварительными мерами

Статья 29 – Неотложное обеспечение сохранности хранящихся компьютерных данных

1. Любая Сторона может попросить другую Сторону дать указание или сделать это иным образом, неотложно обеспечить сохранность данных, которые хранятся в компьютерной системе, расположенной на территории этой другой Стороны, и в отношении которых запрашивающая Сторона намеревается в рамках взаимной помощи направить просьбу об обыске или аналогичных обеспечивающих доступ действиях, о выемке или об аналогичном обеспечении сохранности или разглашении этих данных.

2. В просьбе об обеспечении сохранности данных, направляемой в соответствии с параграфом 1, указываются:

a. lорган, добивающийся обеспечения сохранности;

b. правонарушение, которое подлежит расследованию или судебному разбирательству, и краткое изложение основных фактов;

c. хранимые компьютерные данные, подлежащие сохранению, и их связь с указанным правонарушением;

d. любая имеющаяся информация, идентифицирующая владельца компьютерных данных или местоположение компьютерной системы;

e. обоснование сохранности;

f. сообщение, что эта Сторона намеревается в рамках взаимной помощи направить просьбу об обыске или аналогичных обеспечивающих доступ действиях, о выемке или об аналогичном обеспечении сохранности или разглашении этих данных.

3. По получении такой просьбы от другой Стороны запрашиваемая Сторона принимает все надлежащие меры для неотложного обеспечения сохранности указанных данных в соответствии с внутригосударственным правом. Для удовлетворения такой просьбы в качестве условия не выдвигается требование о том, чтобы правонарушение квалифицировалось как уголовно наказуемое обеими Сторонами.

4. Сторона, которая выдвигает в качестве условия удовлетворения в рамках взаимной помощи просьбы об обыске или аналогичных обеспечивающих доступ действиях, о выемке или об аналогичном обеспечении сохранности или о раскрытии этих данных по правонарушениям, не перечисленным в Статьях 2 - 11 настоящей Конвенции, может оставить за собой право отказать в просьбе об обеспечении сохранности в соответствии с настоящей Конвенцией в случаях, если у нее есть основания полагать, что в момент раскрытия условие о квалификации правонарушения как уголовно наказуемого обеими Сторонами не будет выполнено.

5. Кроме того, в просьбе об обеспечении сохранности данных может быть отказано, если:

a. соответствующая просьба касается правонарушения, которое запрашиваемая Сторона квалифицирует как политическое преступление или правонарушение, связанное с политическим преступлением;

b. запрашиваемая Сторона полагает, что выполнение такой просьбы может нанести ущерб ее суверенитету, безопасности, общественному порядку или другим важным интересам.

6. Если запрашиваемая Сторона полагает, что такое обеспечение сохранности данных не обеспечит в будущем сохранности этих данных, или поставит под угрозу их конфиденциальность, или иным образом помешает расследованию запрашивающей Стороны, она незамедлительно информирует об этом запрашивающую Сторону, которая после этого решает, должна ли выполняться эта просьба.

7. Любое обеспечение сохранности данных, предпринятое в ответ на упомянутую в параграфе 1 просьбу, производится на срок не менее 60 дней, чтобы запрашивающая Сторона могла направить просьбу об обыске или аналогичных обеспечивающих доступ действиях, о выемке или аналогичном обеспечении сохранности или разглашении данных. После получения такой просьбы такие данные продолжают сохраняться до принятия решения в отношении этой просьбы.

Статья 30 – Неотложное раскрытие сохраненных данных о потоках информации

1. Если в ходе предпринятого в соответствии со Статьей 29 исполнения просьбы об обеспечении сохранности данных о потоках в связи с конкретным сообщением запрашиваемая Сторона установит, что поставщик услуг в другом государстве участвовал в передаче этого сообщения, она оперативно раскрывает запрашивающей Стороне

достаточный объем данных о потоках, чтобы идентифицировать этого поставщика услуг и путь, по которому было передано это сообщение.

2. Просьба о раскрытии данных потоков в соответствии с параграфом 1 может быть отозвана только в случаях, если:

a. она касается правонарушения, которое запрашиваемая Сторона квалифицирует как политическое преступление;

b. запрашиваемая Сторона полагает, что исполнение этой просьбы может нанести ущерб ее суверенитету, безопасности, общественному порядку или другим важным интересам.

Подраздел 2 – Взаимная помощь в связи со следственными полномочиями

Статья 31 – Взаимная помощь в отношении доступа к хранящимся электронным данным

1. Сторона может попросить другую Сторону произвести обыск или аналогичные обеспечивающие доступ действия, выемку или аналогичное обеспечение сохранности и раскрытие данных хранящихся с помощью компьютерной системы, которая находится на территории запрашиваемой Стороны, в том числе данных, сохраненных в соответствии со Статьей 29.

2. Запрашиваемая Сторона отвечает на эту просьбу в соответствии с международными документами, договоренностями и законами, упомянутыми в Статье 23 и согласно другим соответствующим положениям настоящей главы.

3. Ответ на просьбу дается оперативно, если:

a. есть основания полагать, что соответствующие данные особо уязвимы для потери или изменения;

b. документы, договоренности и законы, упомянутые в параграфе 2, предусматривают иное оперативное сотрудничество.

Статья 32 – Трансграничный доступ к хранящимся компьютерным данным с соответствующего согласия или к общедоступным данным

Сторона может без согласия другой Стороны:

a. получать доступ к общедоступным (открытому источнику) компьютерным данным независимо от их географического местоположения;

b. получать через компьютерную систему на своей территории доступ к хранящимся на территории другой Стороны компьютерным данным или получать их, если эта Сторона имеет законное и добровольное согласие лица, которое имеет законные полномочия раскрывать эти данные этой Стороне через такую компьютерную систему.

Статья 33 – Взаимная правовая помощь по сбору данных о потоках в режиме реального времени

1. Стороны оказывают взаимную правовую помощь друг другу в сборе данных о потоках информации в режиме реального времени, имеющих отношение к конкретным сообщениям на их территории с помощью компьютерной системы. При соблюдении параграфа 2 оказание такой

помощи регламентируется условиями и процедурами, предусмотренными внутригосударственным правом.

2. Каждая Сторона оказывает такую помощь по меньшей мере по уголовным преступлениям, для которых во внутригосударственном праве мог бы предусматриваться сбор данных о потоках в режиме реального времени.

Статья 34 – Взаимная помощь по перехвату данных

Стороны оказывают друг другу взаимную помощь по сбору или записи в режиме реального времени содержания данных конкретных сообщений, передаваемых с помощью компьютерной системы, если это допускается их действующими договорами и внутригосударственным правом.

Подраздел 3 – Сеть 24/7

Статья 35 – Сеть 24/7

1. Каждая Сторона назначает контактный центр, работающий 24 часа в сутки семь дней в неделю, чтобы обеспечить оказание неотложной помощи в целях расследований или судебных разбирательств уголовных преступлений, имеющих отношение к компьютерным системам и данным, или в целях сбора доказательств в электронной форме по уголовным преступлениям. Такая помощь включает содействие или, если это допускается внутригосударственным правом или практикой, непосредственное применение следующих мер:

a. оказание технической консультативной помощи;

b. обеспечение сохранности данных в соответствии со Статьями 29 и 30;

c. сбор доказательств, предоставление законной информации и установление нахождения подозреваемых лиц.

2.a. Контактный центр одной Стороны располагает возможностями для оперативного обмена сообщениями с контактным центром другой Стороны.

b. Если контактный центр, назначенный одной из Сторон, не входит в состав органа или органов этой Стороны, которым поручено оказание помощи или экстрадиция, этот контактный центр принимает меры для того, чтобы он мог оперативно координировать свою деятельность с деятельностью такого органа или органов.

3. Каждая Сторона принимает меры для предоставления квалифицированного персонала и оборудования с целью облегчить функционирование такой сети.

Глава IV – Заключительные положения

Статья 36 – Подписание и вступление в силу

1. Настоящая Конвенция открыта для подписания Государствами - членами Совета Европы и не являющимися его членами Государствами, которые участвовали в ее разработке.

2. Настоящая Конвенция подлежит ратификации, принятию или утверждению. Ратификационные грамоты или документы о принятии либо утверждении сдаются на хранение Генеральному Секретарю Совета Европы.

3. Настоящая Конвенция вступает в силу в 1-й день месяца, следующего за истечением трех месяцев после

даты, когда пять государств, включая по меньшей мере три государства - члена Совета Европы, выразят свое согласие на обязательное для них соблюдение Конвенции в соответствии с положениями параграфов 1 и 2.

4. В отношении любого подписавшего Конвенцию государства, которое в последующий период выразит согласие на обязательное для него соблюдение Конвенции, она вступает в силу в 1-й день месяца, наступающего по истечении трехмесячного срока, считая с даты, когда оно выразило свое согласие на обязательное для него соблюдение Конвенции в соответствии с параграфами 1 и 2.

Статья 37 – Присоединение к Конвенции

1. После вступления настоящей Конвенции в силу Комитет Министров Совета Европы, после консультаций и единодушного согласия Государств - участников Конвенции, может предложить любому Государству, не являющемуся членом Совета Европы и не участвовавшему в ее разработке, присоединиться к настоящей Конвенции. Такое решение принимается большинством, предусмотренным Статьей 20.d Устава Совета Европы, при условии единодушного согласия представителей Договаривающихся Сторон, имеющих право на членство в Комитете Министров.

2. В отношении любого Государства, присоединяющегося к Конвенции в соответствии с параграфом 1, Конвенция вступает в силу в 1-й день месяца, наступающего по истечении трехмесячного срока, считая с даты сдачи на хранение Генеральному Секретарю Совета Европы документа о присоединении.

Статья 38 – Территориальное применение

1. Любое Государство при подписании или в момент сдачи на хранение ратификационной грамоты или документа о принятии, об утверждении или о присоединении может указать территорию или территории, на которые распространяется действие настоящей Конвенции.

2. Любая Сторона в любой последующий момент может путем заявления, направленного на имя Генерального Секретаря Совета Европы, распространить действие настоящей Конвенции на любую другую территорию, указанную в заявлении. В отношении такой территории Конвенция вступает в силу в 1-й день месяца, наступающего по истечении трехмесячного срока, считая с даты получения заявления Генеральным Секретарем.

3. Любое заявление, сделанное в соответствии с положениями двух предыдущих параграфов в отношении любой указанной в таком заявлении территории, может быть отозвано путем уведомления, направленного на имя Генерального Секретаря Совета Европы. Отзыв вступает в силу в 1-й день месяца, наступающего по истечении трехмесячного срока, считая с даты получения уведомления Генеральным Секретарем.

Статья 39 – Последствия Конвенции

1. Цель настоящей Конвенции - дополнить соответствующие >многосторонние или двусторонние соглашения или договоренности между Сторонами, включая положения:

– Европейской Конвенции о Выдаче, открытой для подписания в Париже 13 декабря 1957 (ETS № 024);

– Европейской Конвенции о Взаимной Правовой Помощи по Уголовным Делам, открытой для подписания в Страсбурге 20 апреля 1959 (ETS № 030);

– Дополнительного Протокола к Европейской Конвенции о Взаимной Правовой Помощи по Уголовным Делам, открытого для подписания в Страсбурге 17 марта 1978 (ETS № 099).

2. Если две и более Сторон уже заключили соглашение или договор по вопросам, составляющим предмет настоящей Конвенции, или иным путем определили свои отношения по вопросам, или если они сделают это в будущем, они также имеют право применять указанные соглашение или договор или регулировать свои отношения в соответствии с ними. Однако если Стороны устанавливают отношения по иным вопросам, составляющим предмет настоящей Конвенции, чем те, которые регламентирует данный документ, они делают это, не нарушая целей и принципов Конвенции.

3. Ничто в настоящей Конвенции не затрагивает иных прав, ограничений, обязательств и обязанностей Сторон.

Статья 40 – Заявления

Путем письменного уведомления на имя Генерального Секретаря Совета Европы любое государство при подписании или в момент сдачи на хранение ратификационной грамоты или документа о принятии, об утверждении или о присоединении может заявить о том, что оно пользуется возможностью, чтобы потребовать включения дополнительных элементов, предусмотренных Статьями 2, 3 и 6 параграфа 1.b, Статьями 7 и 9 параграф 3, Статьей 27 параграф 9.e.

Статья 41 – Положение, касающееся федеративного государства.

1. Федеративное государство может сделать оговорку о сохранении за собой права принять на себя содержащиеся в Главе II настоящей Конвенции обязательства, которые соответствуют основным принципам, регулирующим отношения между центральным правительством и субъектами Федерации или иными аналогичными территориальными образованиями, при условии, что оно тем не менее способно осуществлять сотрудничество по Главе III.

2. Делая такую оговорку в соответствии с параграфом 1, федеративное Государство не может использовать положения данной оговорки, чтобы исключить или существенно сократить обязательства по обеспечению выполнения мер, предусмотренных Главой II. Оно должно предусмотреть широкие и эффективные правоохранительные возможности для обеспечения выполнения данных мер.

3. В том, что касается положений настоящей Конвенции, выполнение которых подпадает под юрисдикцию субъектов Федерации или иных аналогичных территориальных образований, которые в соответствии с конституционной системой Федерации не обязаны принимать законодательные меры, федеральное правительство информирует компетентные власти таких субъектов об упомянутых положениях и своем положительном мнении, побуждая их предпринимать необходимые действия для выполнения данных положений.

Статья 42 – Оговорки

Путем письменного уведомления на имя Генерального Секретаря Совета Европы любое Государство при

подписании или в момент сдачи на хранение ратификационной грамоты или документа о принятии, об утверждении или о присоединении может заявить, что оно воспользуется правом сделать оговорку (и), предусмотренную (ые) параграфом 2 Статьи 4, параграфом 3 Статьи 6, параграфом 4 Статьи 9, параграфом 3 Статьи 10, параграфом 3 Статьи 11, параграфом 3 Статьи 14, параграфом 2 Статьи 22, параграфом 4 Статьи 29 и параграфом 1 Статьи 41. Никакие другие оговорки не допускаются.

Статья 43 – Статус и снятие оговорок

1. Сторона, сделавшая оговорку в соответствии с положениями Статьи 42, может снять всю оговорку или ее часть путем уведомления, направленного на имя Генерального Секретаря Совета Европы. Такое снятие оговорки вступает всилу в день получения соответствующего уведомления Генеральным Секретарем. Если в уведомлении говорится, что снятие оговорки должно вступить в силу с момента указанной в нем даты, а такая дата наступает позже даты получения уведомления Генеральным Секретарем, снятие оговорки вступает в силу с момента указанной поздней даты.

2. Сторона, сделавшая, указанную в Статье 42 оговорку, снимает такую оговорку или ее часть, как только позволят обстоятельства.

3. Генеральный секретарь Совета Европы может периодически запрашивать Стороны, сделавшие одну или несколько оговорок, указанных в Статье 42, о возможностях снятия такой оговорки (оговорок).

Статья 44 – Поправки

1. Поправки к настоящей Конвенции могут предлагаться любой Стороной, и сообщаться через Генерального Секретаря Совета Европы Государствам - членам Совета Европы, Государствам не являющимся членами Совета Европы, которые участвовали в разработке этой Конвенции, а также любому Государству, присоединившемуся к настоящей Конвенции или получившему предложение присоединиться к ней в соответствии с положениями Статьи 37.

2. Любая поправка, предложенная одной из Сторон, направляется в Европейский Комитет по Проблемам Преступности, который представляет Комитету Министров свое заключение относительно предлагаемой поправки.

3. Комитет Министров рассматривает предлагаемую поправку и заключение, представленное Европейский Комитет по Проблемам Преступности, и после консультации сторонами настоящей Конвенции, не являющимися Государствами - Членами, может принять эту поправку.

4. Текст любой поправки, принятой Комитетом Министров в соответствии с положениями параграфа 3 настоящей Статьи, направляется Сторонам Конвенции для утверждения.

5. Любая поправка, принятая в соответствии с положениями параграфа 3 настоящей Статьи, вступает в силу на 13 день после того, как все Стороны сообщат Генеральному Секретарю о своем согласии с этой поправкой.

Статья 45 – Урегулирование споров

1. Европейский Комитет по Проблемам Преступности получает информацию о толковании и применении настоящей Конвенции.

2. В случае возникновения спора между Сторонами относительно толкования или применения настоящей Конвенции они стремятся к урегулированию спора путем переговоров или любыми другими мирными средствами по своему выбору, включая передачу этого спора с согласия заинтересованных Сторон в Европейский Комитет по Проблемам Преступности, в арбитражный суд, решения которого имеют для Сторон обязательную силу, или в Международный суд.

Статья 46 – Консультации Сторон

1. Стороны, в соответствующих случаях, периодически проводят консультации с целью содействовать:

a. эффективному применению и выполнению настоящей Конвенции, включая выявление любых относящихся к ней проблем, а также последствий любого заявления или оговорки, сделанных в соответствии с настоящей Конвенцией;

b. обмену информацией о важных изменениях в правовой, политической или технической сферах, имеющих отношение к преступности в сфере компьютерной информации, и сбору доказательств в электронной форме;

c. рассмотрению возможных дополнений или поправок к настоящей Конвенции.

2. Европейский Комитет по Проблемам Преступности периодически получает информацию о результатах консультаций, упомянутых в параграфе 1.

3. Европейский Комитет по Проблемам Преступности в соответствующих случаях оказывает содействие в проведении консультаций, упомянутых в параграфе 1, и принимает необходимые меры для оказания помощи Сторонам в их усилиях по внесению дополнений или поправок в Конвенцию. Не позднее чем через три года после вступления в силу настоящей Конвенции Европейский Комитет по Проблемам Преступности во взаимодействии со Сторонами проводит пересмотр всех положений Конвенции и в случае необходимости рекомендует принять любые соответствующие поправки.

4. За исключением случаев, когда расходы, понесенные в процессе выполнения положений параграфа 1, берет на себя Совет Европы, их несут сами Стороны на установленных ими условиях.

5. Секретариат Совета Европы оказывает помощь Сторонам в выполнении их обязанностей, вытекающих из положений настоящей Статьи.

Статья 47 – Денонсация

1. Любая Сторона может в любое время денонсировать настоящую Конвенцию путем уведомления, направленного на имя Генерального Секретаря Совета Европы.

2. Такая денонсация вступает в силу в 1-й день месяца, наступившего по истечении трехмесячного срока, считая с

даты получения указанного уведомления Генеральным Секретарем.

Статья 48 – Уведомление

Генеральный Секретарь Совета Европы уведомляет Государства - члены Совета Европы, не являющиеся его членами Государства, которые участвовали в разработке настоящей Конвенции, а также любое Государство, присоединившееся или получившее предложение присоединиться к настоящей Конвенции о:

a. любом подписании;

b. сдаче на хранение любой ратификационной грамоты или любого документа о принятии, об утверждении или о присоединении;

c. любой дате вступления в силу настоящей Конвенции в соответствии с положениями Статей 36 и 37;

d. любом заявлении, сделанным в соответствии с положениями Статьи 40 или оговорки, сделанной в соответствии с положениями Статьи 42;

e. любых других актах, уведомления или сообщения, относящихся к настоящей Конвенции.

В удостоверение чего нижеподписавшиеся, должным образом на то уполномоченные представители, подписали настоящую Конвенцию.

Совершено в Будапеште 23 ноября 2001 в одном экземпляре на английском и французском языках, причем оба текста имеют одинаковую силу. Этот экземпляр передается на

хранение в архивы Совета Европы. Генеральный Секретарь Совета Европы направляет заверенные копии данного документа каждому Государству - члену Совета Европы, не являющимся членами Совета Европы Государствам, которые участвовали в разработке настоящей Конвенции, и любому Государству, получившему предложение присоединиться к ней.

Пояснительный Доклад

I. Конвенция и Пояснительная записка были утверждены Комитетом министров Совета Европы на его 109-м заседании (8 ноября 2001 г.). Конвенция была открыта для подписания 23 ноября 2001 г. в Будапеште, на Международной конференции по киберпреступности.

II. Текст данной Пояснительной записки не является прецедентным толкованием Протокола, но может облегчить понимание содержащихся в нем положений.

I. Введение

1. Революция в области информационных технологий в корне изменила общество и, вероятно, эти изменения в обозримом будущем продолжатся. Стало проще решать многие задачи. Если раньше рабочие процедуры рационализировались с помощью информационных технологий лишь в отдельных областях, то ныне почти невозможно найти отрасль, которого этот процесс не коснулся бы. Информационные технологии в том или ином виде проникли почти в каждый аспект человеческой деятельности.

2. Яркая особенность информационных технологий – это влияние, которое они оказывают на развитие телекоммуникационных технологий. Классическая телефония – передача человеческого голоса – сменилась на обмен огромным количеством данных, в том числе голос, текст, музыка, статические и анимированные изображения. Этот обмен происходит уже не только между людьми, но и между людьми и компьютерами, а также только между компьютерами.

Соединения с коммутацией каналов сменились на сети с коммутацией пакетов. Уже не имеет значения, можно ли установить прямую связь. Достаточно ввести данные в сеть, указав адрес их назначения или предоставить к ним доступ для всех желающих.

3. Повсеместное использование электронной почты и доступ через Интернет к многочисленным веб-сайтам – примеры этих изменений. Они глубоко повлияли на наше общество.

4. Простота доступа и возможности поиска информации, содержащейся в компьютерных системах, в сочетании с практически неограниченными возможностями обмена данными и их распространения на любые расстояния, привели к резкому росту объема доступной информации и знаний, которые из нее можно почерпнуть.

5. Такое развитие событий породило беспрецедентные экономические и социальные изменения, но есть и оборотная сторона медали: появление новых видов преступлений, а также совершение обычных преступлений с помощью новых технологий. Кроме того, преступное поведение может иметь намного более далеко идущие последствия, чем раньше, так как они не ограничены географическими или национальными границами. Распространение по всему миру вредных компьютерных вирусов – доказательство этой проблемы. Технические меры защиты компьютерных систем должны внедряться параллельно правовым мерам по предотвращению преступных деяний.

6. Новые технологии бросают вызов существующим юридическим понятиям. Информационные и коммуникационные

потоки проще перемещаются по всему миру. Границы больше не являются преградами для этих потоков. Все чаще преступники географически находятся вдали от мест, где их деяния вызывают последствия. Однако внутригосударственные законы, как правило, действуют на определенной территории. Такие проблемы следует поэтому решать с помощью международного права, что требует создания адекватных международно-правовых инструментов. Настоящая Конвенция направлена на решение этой задачи с должным уважением к правам человека в новом информационном обществе.

II. Подготовительная работа

7. Решением № CDPC/103/211196 Европейского комитета по проблемам преступности – ЕКПП (European Committee on Crime Problems – CDPC) от ноября 1996 года была создана экспертная комиссия по проблемам киберпреступности. Свое решение ЕКПП обосновал следующим образом:

8. «Быстрое развитие в области информационных технологий отражается на всех областях современного общества. Интеграция телекоммуникационных и информационных систем, позволяющих хранение и передачу разных типов данных на любые расстояния, открывает целый ряд новых возможностей. Это развитие существенно ускорилось с появлением таких информационных супер-магистралей и сетей как Интернет, с помощью которых кто угодно может получить доступ к любой электронной информационной службе вне зависимости от того, где в мире она находится. Подключаясь к службам информации и связи, пользователи создают так называемое «киберпространство», которое

используется для законных целей, но может также использоваться и неправомерно. Эти «преступления в киберпространстве» совершаются против целостности, доступности и конфиденциальности компьютерных систем и телекоммуникационных сетей, либо заключаются в использовании таких сетей для совершения обычных преступлений. Международный характер преступлений, которые совершаются через Интернет, противоречит принципу территориальности государственных правоохранительных органов.

9. Поэтому уголовное законодательство должно иметь в виду эти технологические разработки, которые предоставляют изощренные возможности для злоупотребления киберпространством и нанесения ущерба законным интересам. Учитывая трансграничный характер информационных сетей, чтобы противостоять такому неправомерному использованию, нужны согласованные международные усилия. Несмотря на то, что Рекомендация № (89) 9 привела к уравниванию национальных представлений о некоторых формах неправомерного использования компьютеров, только обязательный международно-правовой документ может обеспечить необходимую эффективность борьбы с этими новыми явлениями. В рамках такого документа должны, в дополнение к положениями о международном сотрудничестве и вопросами материального и процессуального права, должны также рассматриваться проблемы, тесно связанные с использованием информационных технологий».

10. РКроме того, ЕКПП принял во внимание доклад, подготовленный по его просьбе профессором Касперсеном

(H.W.K. Kaspersen), который пришел к выводу, что «... должна быть рассмотрена другая форма правового документа с большей степенью обязательности, чем рекомендация. Например, конвенция. Такая конвенция должна охватывать не только вопросы уголовного материального права, но и уголовно-процессуальные вопросы, а также международные уголовно-правовые процедуры и соглашения»[1] Такой же вывод был сделан в Записке к Рекомендации № R (89) 9[2], в отношении материального права, а также в Рекомендации № R (95) 13[3], в отношении проблем процессуального права, связанного с информационными технологиями.

11. Конкретные положения, установленные новым Комитетом:

i. «В свете Рекомендации № R (89) 9 о преступлениях, совершенных при помощи компьютеров, а также Рекомендации № R (95) 13 по проблемам уголовно-процессуального права, связанного с информационными технологиями, рассмотреть, в частности, следующие моменты:

---

1. Применение Рекомендации № R (89) 9 по преступлениям, связанным с использованием компьютера, доклад подготовлен профессором, д-ром Касперсеном (документы ЕКПП (97) 5 и PC-CY (97) 5, страница 106).

2. См. «Преступления, совершенные с использованием компьютеров», доклад Европейского комитета по проблемам преступности, стр. 86

3. См. «Проблемы уголовно-процессуального законодательства, связанные с информационными технологиями», Рекомендация № R (95) 13, правило № 17

ii. преступления в киберпространстве, в частности, совершенные с использованием таких телекоммуникационных сетей, как Интернет. Например, незаконные денежные транзакции, предложение незаконных услуг, нарушение авторских прав, а также преступления, связанные с унижением человеческого достоинства и защитой несовершеннолетних;

iii. иные существенные вопросы уголовного права, по которым может быть необходимо международное сотрудничество, например, определения, санкции и ответственность субъектов киберпространства, в том числе поставщиков услуг Интернета;

iv. использование – в том числе международное – в технологической среде принудительных мер, например, перехват телекоммуникаций и электронное наблюдение за информационными сетями, например, через Интернет; поиск и изъятие систем обработки информации (в том числе интернет-сайтов), закрытие доступа к незаконным материалам, требование от поставщиков услуг соблюдения особых обязательств, принимая во внимание проблемы, связанные, например, с такими особыми мерами информационной безопасности, как шифрование;

v. вопрос юрисдикции в отношении преступлений, связанных с информационными технологиями. Например, определение locus delicti и, соответственно, применимого права. А также вопрос о двойной подсудности за одно и то же преступление в двух юрисдикциях, и вопрос, как разрешать позитивные и избегать негативных конфликтов юрисдикции;

vi. вопросы международного сотрудничества в расследовании преступлений в киберпространстве, в тесной кооперации с Комитетом экспертов, который контролирует выполнение европейских конвенций в уголовной сфере (PC-OC).

По возможности, Комитет должен подготовить юридически обязывающий документ по пунктам I) - V) с особым акцентом на международные вопросы и, в случае необходимости, дополнительные рекомендации. Комитет может вносить и другие предложения в свете технологических разработок».

12. В соответствии с решением ЕКПП, постановлением Комитета министров Совета Европы № CM/Del/Dec(97)583, принятым на его 583-м заседании на уровне заместителей 4 февраля 1997 г., был создан «Комитет экспертов по преступности в киберпространстве (PC-CY– Committee of Experts on Crime in Cyber-space)». Комитет PC-CY начал переговоры по проекту международной конвенции о киберпреступности в апреле 1997 года. Планировалось, что он закончит свою работу до 31 декабря 1999 г. Но к этому моменту Комитет еще не был в состоянии в полной мере провести переговоры по некоторым вопросам в проекте конвенции, поэтому его полномочия были продлены до 31 декабря 2000 г. постановлением № CM/Del/Dec(99)679, принятым на уровне заместителей министров. Европейские министры юстиции дважды выразили поддержку переговоров: Постановлением № 1, принятым на 21-й Конференции (Прага, июнь 1997 г.), которая рекомендовала Комитету министров поддержать работу ЕКПП по киберпреступности, с целью гармонизации положений внутригосударственного уголовного права и обеспечения

применения эффективных средств расследования в отношении таких преступлений. А затем Постановлением № 3, принятым на 23-й Конференции европейских министров юстиции (Лондон, июнь 2000 г.), которая призвала участвующие в переговорах стороны продолжать усилия по поиску решений, чтобы привлечь к участию в Конвенции как можно большее число государств. Была также подтверждена необходимость создания оперативной и эффективной системы международного сотрудничества, которая должным образом учитывает особые требования борьбы с киберпреступностью. Государства-члены Европейского Союза выразили поддержку работе PC-CY, выразив в мае 1999 г. Общую позицию.

13. В период с апреля 1997 г. по декабрь 2000 г., Комитет PC-CY провел 10 пленарных заседаний и 15 совещаний открытого состава редакционной группы. По истечении увеличенного срока полномочий эксперты провели под эгидой ЕКПП еще три встречи для завершения проекта Пояснительной записки и рассмотрения проекта Конвенции с учетом мнения Парламентской ассамблеи. В октябре 2000 года Комитет министров предложил Ассамблее дать заключение по проекту Конвенции. Конвенция была принята в ходе 2-й части пленарной сессии в апреле 2001 года.

14. В соответствии с решением, принятым Комитетом PC-CY, ранняя версия проекта конвенции был рассекречена и опубликована в апреле 2000 года. Следующие проекты выпускались после каждого пленарного заседания, чтобы позволить договаривающимся государствам провести консультации со всеми заинтересованными сторонами. Этот процесс оказался полезным.

15. Пересмотренный и уточненный проект Конвенции и Пояснительной записки к ней был представлен на утверждение ЕКПП на его 50-м пленарном заседании в июне 2001 года, после чего текст проекта Конвенции был передан в Комитет министров для рассмотрения и открытия для подписания.

III. Конвенция

16. Конвенция направлена, главным образом, на (1) гармонизацию элементов внутригосударственного уголовного права и смежных положений в области киберпреступности (2) обеспечение внутренних уголовно-процессуальных полномочий, необходимых для расследования и преследования как таких преступлений, так и других правонарушений, совершенных с помощью компьютера, а также правонарушений, доказательства которых хранятся в электронном виде (3) создание быстрого и эффективного режима международного сотрудничества.

17. Конвенция состоит из четырех глав:

(I) Терминология

(II) Меры, принимаемые на национальном уровне – материальное и процессуальное право

(III) Международное сотрудничество

(IV) Заключительные положения

18. Раздел 1 Главы II (вопросы материального права) охватывает как положения о криминализации, так и смежные положения в области компьютерной преступности либо преступности, связанной с компьютерами: сначала

определяются 9 преступлений, сгруппированных в 4 категории, затем рассматривается дополнительная ответственность и санкции. Конвенцией определены следующие преступления: незаконный доступ, незаконный перехват, воздействие на данные, вмешательство в работу системы, неправомерное использование устройств, подлог с использованием компьютеров, мошенничество с использованием компьютеров, преступления, связанные с детской порнографией и правонарушения, связанные с авторским правом и смежными правами.

19. Раздел 2 Главы II (вопросы процессуального права) охватывает преступления, которые выходят за рамки, определенные в Разделе 1 – правонарушения, совершенные при помощи компьютерных систем или правонарушения, доказательства которых существуют в электронном виде. Этот раздел определяет общие условия и средства защиты, применимые ко всем процессуальным полномочиям в этой главе. Затем он устанавливает следующие процессуальные полномочия: оперативное обеспечение сохранности хранимых данных; оперативное обеспечение сохранности и частичное раскрытие данных о трафике; запрос на предоставление данных; поиск и изъятие компьютерных данных; сбор данных о трафике в режиме реального времени; перехват данных об информационном наполнении. Глава II заканчивается положениями о юрисдикции.

20. Глава III содержит положения о взаимопомощи в делах о традиционной и компьютерной преступности, а также о правилах экстрадиции. Она охватывает традиционную взаимопомощь в двух ситуациях: когда между сторонами не существует правовой основы (договор, двустороннее

законодательство и т.п.) и применяются его положения, либо когда такая основа существует, и ее механизмы применяются и для оказания помощи в рамках настоящей Конвенции. Помощь в связи с компьютерными и другими преступлениями, совершенными при помощи компьютеров, относится к обеим ситуациям и охватывает тот же диапазон процессуальных полномочий, который определен в Главе II (при этом могут применяться дополнительные условия). Кроме того, Глава III содержит положение об особом виде не требующего взаимной помощи трансграничного получения хранимых компьютерных данных (доступных по согласованию либо общедоступных), предусматривающее создание Сторонами круглосуточно работающей сети оперативной помощи.

21. Наконец, Глава IV содержит заключительные положения, с некоторыми исключениями воспроизводящие стандартные условия договоров Совета Европы.

Комментарии к статьям Конвенции

Глава I – Терминология

Об определениях, содержащихся в Статье 1

22. Разработчики Конвенции подразумевали, что Стороны Конвенции не будут обязаны дословно воспроизводить в своих национальных законодательствах четыре понятия, определения которых содержатся в Статье 1, если в их законах имеются аналогичные положения, соответствующие принципам Конвенции и обеспечивающие равноценные средства для их осуществления.

Статья 1 (a) – Компьютерная система

23. В соответствии с Конвенцией, компьютерной системой называется устройство, состоящее из аппаратного и программного обеспечения, разработанного для автоматической обработки цифровых данных. Она может включать устройства ввода, вывода и хранения данных. Система может быть отдельной или объединенной в сеть с другими аналогичными устройствами. Термин «автоматический» означает без прямого вмешательства человека. Термин «обработка данных» означает, что данные в компьютерной системе обрабатываются путем исполнения компьютерной программы. «Компьютерная программа» представляет собой набор инструкций, которые могут выполняться компьютером для достижения желаемого результата. Компьютер может исполнять различные программы. Компьютерная система обычно состоит из различных устройств, которые делятся на центральный процессор и периферийные устройства. «Периферийным» называется устройство, выполняющее определенные функции во взаимодействии с центральным процессором: принтер, монитор, устройство записи и чтения компакт-дисков и иные устройства хранения данных.

24. Сеть – это взаимосвязь между двумя или более компьютерными системами. Соединения могут быть наземными (через провод или кабель), беспроводными (например, радио, инфракрасные, спутниковые), или их комбинация. Сеть может быть географически ограничена небольшой территорией (локальные сети) или может охватывать большую площадь (глобальные сети). Сети могут быть соединены между собой. Интернет представляет собой глобальную

сеть, состоящую из многих взаимосвязанных сетей, использующих один протокол связи. Существуют и другие типы подключенных или не подключенных к Интернету сетей, которые способны передавать данные между компьютерными системами. Компьютерные системы могут быть подключены к сети в качестве конечных точек, либо в качестве связующих звеньев сети. Существенно то, что по сети происходит обмен данными.

Статья 1 (b) – Компьютерные данные

25. Определение компьютерной информации опирается на определение ISO. Это определение содержит термин «подходящий для обработки». Это означает, что данные вводятся в такой форме, которая позволяет их обработку в компьютерной системе. Для четкого понимания факта, что данные в настоящей Конвенции следует понимать как данные в электронной или иной обрабатываемой форме, вводится понятие «компьютерные данные». Автоматически обрабатываемые компьютерные данные могут быть объектом одного из уголовных преступлений, определенных в настоящей Конвенции, а также объектом следственных мер, определенных в Конвенции.

Статья 1 (c) – Поставщик услуг

26. Термин «поставщик услуг» охватывает широкую категорию лиц, играющих особую роль в передаче или обработке данных при помощи компьютерных систем (см. также замечания к Разделу 2). Пункт (I) определения четко указывает, что термин охватывает как государственные, так и частные организации, предоставляющие пользователям

возможность обмена информацией. Таким образом, не имеет значения, образуют ли пользователи закрытую группу или поставщик предоставляет свои услуги широкому населению, бесплатно или за плату. Закрытой группой может быть, например, группа сотрудников частного предприятия, которой предоставляются услуги корпоративной сети.

27. 27. Пункт (II) определения четко указывает, что термин «поставщик услуг» распространяется и на лиц, которые хранят или обрабатывают данные от имени лиц, указанных в пункте (I). Кроме того, термин включает в себя те объекты, которые хранят или обрабатывают данные от имени пользователей услуг, упомянутых в пункте (I). Например, в соответствии с этим определением, поставщики услуг предлагают как услуги хостинга и кэширования, так и услуги подключения к сети. Тем не менее, поставщик информационного наполнения (например, человек, который заключает контракт с хостинговой компанией для размещения своего веб-сайта) не охватывается этим определением, если такой поставщик информационного наполнения не предлагает услуги обмена или смежные услуги обработки данных.

Статья 1 (d) – Данные о трафике

28. Для целей настоящей Конвенции – как определено в Статье 1, подпункт d – под трафиком понимается категория компьютерных данных, являющихся предметом особого правового режима. Эти данные генерируются компьютерами в сети связи для того, чтобы маршрутизировать сообщение от источника к месту назначения. По отношению к самой связи, трафик играет вспомогательную роль.

29. В случае расследования уголовного преступления, совершенного с использованием компьютерной системы, данные о трафике необходимы, чтобы проследить источник сообщения. Это отправная точка для сбора дополнительных доказательств или часть доказательной базы преступления. Иногда данные о трафике практически не хранятся, что делает необходимым требование об оперативном обеспечении их сохранности. Следовательно, быстрое раскрытие этих данных может быть необходимо, чтобы выявить маршрут сообщения, собрать дополнительные доказательства или выявить подозреваемого до того, как данные будут удалены. Поэтому обычная процедура сбора и раскрытия компьютерных данных может быть недостаточной. Кроме того, сбор таких данных считается менее инвазивным, поскольку не раскрывается содержание сообщения, которое считается конфиденциальным.

30. Определение дает исчерпывающий перечень категорий данных о трафике, которые обрабатываются с помощью особого режима Конвенции: источник сообщения, место назначения, маршрут, время (GMT), дата, размер, продолжительность и тип сетевого сервиса. Не все из этих категорий всегда технически доступны, могут выдаваться поставщиком услуг, или необходимы для конкретного уголовного расследования. «Источник» относится к номеру телефона, адресу интернет-протокола (Internet Protocol – IP), или аналогичному идентификатору объекта связи, которому поставщик оказывает услуги. Термин «Получатель» относится к сопоставимому указанию объекта связи, которому передаются сообщения. Термин «тип соответствующего сетевого сервиса» относится к типу сервиса, который

используется в сети, например, передача файлов, электронная почта или служба мгновенных сообщений.

31. Определение оставляет национальным законодательным органам возможность дифференцировать правовую охрану данных о трафике в соответствии с их уровнем конфиденциальности. В этом контексте Статья 15 обязывает Стороны предусмотреть условия и гарантии защиты прав и свобод человека. Это подразумевает, в частности, что основные критерии и процедуры, применимые для расследования, могут меняться в зависимости от уровня конфиденциальности данных.

Глава II – Меры для принятия на национальном уровне

32. Глава II (Статьи 2 – 22) состоит из трех разделов: материальное уголовное право (Статьи 2 – 13), процессуальное право (Статьи 14 – 21) и юрисдикции (Статья 22).

Раздел 1 – Материальное уголовное право

33. Цель Раздела 1 Конвенции (Статьи 2 – 13) – улучшение средств предупреждения и пресечения преступлений, связанных с компьютерами, путем создания общего минимального стандарта соответствующих преступлений. Такая гармонизация облегчает борьбу с правонарушениями как на национальном, так и на международном уровне. Соответствие в национальном законодательстве может предотвратить злоупотребления в результате смещения Стороны к предыдущему, более низкому стандарту. Как следствие, может быть улучшен обмен полезным общим

опытом в практической обработке таких случаев. Международное сотрудничество (особенно выдача преступников и взаимная правовая помощь) упрощается, например, при случаях двойной подсудности.

34. Указанный список правонарушений представляет минимальный консенсус и не исключает расширения во внутригосударственном законодательстве. Он основан в значительной степени на руководящих принципах, разработанных в связи с Рекомендацией № R(89)9 Совета Европы о преступлениях, связанных с компьютерами и о работе других государственных и частных международных организаций (ОЭСР, ООН, МАУП), но с учетом более современных случаев злоупотребления широкими телекоммуникационными сетями.

35. Раздел состоит из пяти подразделов. Подраздел 1 включает основу компьютерных преступлений, преступлений против конфиденциальности, целостности и доступности компьютерных данных и систем. Согласно дискуссиям о безопасности компьютеров и данных, он описывает основные угрозы, которым подвергаются системы электронной обработки и передачи данных. Обрисованы типы преступлений, а именно: несанкционированный доступ и незаконное вмешательство в системы, программы или данные. Подразделы 2 - 4 включают и другие типы преступлений, связанные с компьютерами, которые на практике играют важную роль. В этих случаях компьютерные и телекоммуникационные системы используются в качестве средства нападения на определенные правовые интересы, которые в большинстве случаев уже защищены традиционными мерами уголовного права. Подраздел 2: согласно

предложениям в руководящих принципах Совета Европы, Рекомендация № R(89)9, добавлены такие преступления, как мошенничество и подделка при помощи компьютерной техники. Подраздел 3 охватывает «преступления незаконного информационного наполнения, связанные с незаконным производством или распространением детской порнографии через компьютерные системы. Это в последнее время рассматривается как одно из самых вредных modi operandi (преступных деяний). Редакционный комитет Конвенции обсудил возможность включения других правонарушений, связанных с информационным наполнением, например, распространение через компьютерные системы расистской пропаганды. Однако Комитет не смог достичь консенсуса по вопросу подсудности такого поведения. Несмотря на то, что признание такой деятельности уголовным преступлением получило немалую поддержку, некоторые делегации выразили глубокую обеспокоенность по поводу включения этого положения в связи с соображениями о свободе выражения мнения. Отмечая сложность этого вопроса, было решено, что комитет поручит Европейскому комитету по проблемам преступности (ЕКПП) составление дополнительного Протокола к настоящей Конвенции.

Подраздел 4 определяет набор «преступлений, связанных с нарушением авторского права и смежных прав». Эта тема включена в Конвенцию, поскольку нарушение авторских прав является одной из наиболее распространенных форм компьютерной преступности. Быстрое и широкое распространение этой практики вызывает обеспокоенность международного сообщества. Наконец, Подраздел 5 включает дополнительные положения о попытках совершения преступления, пособни-

честве, подстрекательстве и санкциях. А также о корпоративной ответственности, в соответствии с недавно появившимися международными инструментами.

36. Хотя материально-правовые положения относятся к преступлениям с использованием информационных технологий, Конвенция использует нейтральный язык, с тем чтобы основные определения нарушений уголовного права могли применяться к современным и к будущим технологиям.

37. Разработчики Конвенции подразумевали, что Стороны могут освободить от уголовной ответственности, определенной в статьях 2-10, за мелкие или незначительные проступки.

38. Специфика перечисленных правонарушений заключается в правиле, что действия совершаются «без права». Она отражает понимание того факта, что действие не всегда наказуемо как таковое, оно может быть законным или оправданным не только в случаях, когда применимы классические средства юридической защиты, например согласие, самооборона или необходимость, но и в случаях, если другие принципы или соображения ведут к исключению уголовной ответственности. Выражение «без права» получает свое значение в зависимости от контекста использования. Таким образом, не внося ограничений в реализацию внутреннего законодательства Сторон, это выражение может относиться к действиям, совершенным без разрешения (будь оно законодательным, исполнительным, административным, судебным, договорным или по согласию), либо к поведению, на которое не распространяются способы установленной правовой защиты, оправдания, обоснования

или соответствующие принципы в соответствии с внутренним законодательством. Следовательно, Конвенция не касается действий, совершаемых законной государственной властью (например, действий правительства Стороны для поддержания общественного порядка, защиты национальной безопасности или расследования уголовных преступлений). Кроме того, законные и обычные действия, присущие конструкции сетей, либо законные и обычные эксплуатационные или коммерческие методы не должны преследоваться. Конкретные примеры исключений в отношении конкретных правонарушений представлены в тексте Пояснительной записки ниже. Сторонам предоставляется определить, как такие исключения реализуются во внутренних правовых системах (в рамках уголовного права или иным образом).

39. Все правонарушения, предусмотренные Конвенцией, должны быть совершены «намеренно», иначе уголовная ответственностью неприменима. В некоторых случаях наличие дополнительного конкретного умысла образует часть правонарушения. Например, в Статье 8 о компьютерном мошенничестве, намерение извлечь выгоду является составным элементом правонарушения. Составители Конвенции сошлись во мнении, что точное значение «намеренно» должно быть оставлено для толкования на национальном уровне.

40. Некоторые статьи в разделе позволяют добавлять определенные обстоятельства для применения Конвенции в национальном законодательстве. В других случаях предоставляется возможность оговорки (см. Статьи 40 и 42). Такие способы более ограничительного подхода к крими-

нализации отражают различные оценки степени опасности или необходимости использования уголовного права в качестве контрмеры. Такой подход обеспечивает для правительств и парламентов гибкость в определении собственной уголовной политики в этой области.

41. Законы, устанавливающие ответственность за эти правонарушения, должны быть разработаны с максимально возможной ясностью и конкретностью, чтобы обеспечить адекватную прогнозируемость того, какой тип поведения повлечет уголовное наказание.

42. В ходе редакционного процесса составители рассмотрели целесообразность криминализации поведения, на которое не распространяются Статьи 2 - 11, в том числе узурпацию доменов, т.е. факт регистрации доменного имени, которое идентично либо наименованию организации (как правило, хорошо известной), либо торговому наименованию или торговой марке продукта или компании. Кибер-узурпаторы не имеют намерения активно использовать доменные имена, а пытаются извлечь финансовую выгоду, заставляя заинтересованное – может быть, косвенно, лицо заплатить за передачу собственности на имя домена. В настоящее время такие действия рассматриваются как проблемы товарных знаков. Нарушения прав на товарные знаки не регулируются настоящей Конвенцией, поэтому составители не считают целесообразным обсуждать подсудность такого деяния.

Подраздел 1 – Преступления против конфиденциальности, целостности и доступности компьютерных данных и систем

43. Криминализация деяний, описанных в Статьях 2-6, преследует цель защиты конфиденциальности, целостности и доступности компьютерных систем или данных, а не наказания за законные и обычные мероприятия, присущие сетям, либо законные и обычные эксплуатационную или коммерческую практику.

Незаконный доступ (Статья 2)

44. Понятие «незаконный доступ» подразумевает основное правонарушение, представляющее серьезную угрозу в отношении безопасности (т.е. конфиденциальности, неприкосновенности и доступности) компьютерных систем и данных. Необходимость в защите отражает потребность организаций и частных лиц контролировать свои системы и управлять ими без внешнего вмешательства. Само несанкционированное вторжение, т.е. «взлом», «вскрытие» или «компьютерное проникновение» должно быть незаконно. Оно может помешать легальному использованию систем и данных, а также вызвать изменение или уничтожение данных, что сопряжено с высокими расходами на их восстановление. Подобное вторжение может обеспечить доступ к конфиденциальным данным (включая пароли и информацию о системе), к секретной информации, к бесплатному использованию системы, или даже подтолкнуть компьютерных взломщиков к более серьезным правонарушениям, таким как мошенничество и подделка документов с применением компьютера.

45. Самыми эффективными средствами предотвращения неавторизованного вторжения являются, разумеется, внедрение и развитие эффективных мер безопасности. Однако всесторонняя защита должна также включать в себя использование уголовно-правовых мер. На ранней стадии запрет уголовного характера на несанкционированный доступ может обеспечить дополнительную защиту системы и данных от вышеописанных угроз.

46. 46. Термин «доступ» означает проникновение в компьютерную систему или любую ее часть (аппаратное обеспечение, компоненты компьютера, данные установленной системы, каталоги, трафик и данные, относящиеся к информационному наполнению). Однако в это понятие не входит отправление файла или электронного сообщения системе. «Доступ» подразумевает вход в другую компьютерную систему в том случае, если он производится через общедоступные телекоммуникационные сети, такие как LAN (локальная сеть), или через внутреннюю сеть организации. Способ связи (например, удаленный, в том числе, беспроводное соединение, или с небольшого расстояния) не имеет значения.

47. Действие также должно быть совершено «неправомерно». Помимо пояснения выше следует отметить, что доступ, авторизованный владельцем или другим правомочным обладателем системы или ее части, не является преступным (например, доступ в целях авторизованного тестирования или защиты такой компьютерной системы). Более того, не является преступным доступ к компьютерной системе, которая предоставляет бесплатный и свободный публичный доступ: такой доступ считается «правомерным».

48. Статья 2 может распространяться на применение специальных технических инструментов, например, на доступ к веб-странице напрямую или через гипертекстовые ссылки, включая глубокие ссылки (deep links), или использование файлов «cookie» и «ботов» для поиска и извлечения информации. Применение таких инструментов само по себе не является «неправомерным». Публикация публичного веб-сайта подразумевает согласие владельца на предоставление доступа для любого пользователя Интернета. Использование стандартных инструментов, предусмотренных распространенными протоколами и программами, не является само по себе «неправомерным», в частности тогда, когда считается, что правообладатель системы, к которой осуществляется доступ, согласился на их использование (как, например, в случае с файлами «cookie», если от их использования не отказались на исходном этапе установки и позднее они не были отключены).

49. В законодательстве многих стран уже содержатся меры предотвращения правонарушений, связанных со «взломом» компьютеров, однако эти меры существенно различаются. Широкое толкование незаконности, приведенное в первом предложении Статьи 2, не является неоспоримым. В случаях, когда само вторжение не несет опасности, или же когда акт взлома приводит к выявлению слабых мест в безопасности системы, это толкование вызывает возражения. В результате некоторые страны принимают более узкое толкование, требующее дополнительных уточнений (этот подход был также принят в Рекомендации № (89) 9 и предложен рабочей группой ОЭСР в1985 г.).

50. Стороны могут принять широкое толкование и объявить незаконным сам акт взлома в соответствии с первым

предложением Статьи 2. В качестве альтернативы, они могут принять уточнения, перечисленные во втором предложении (нарушение мер безопасности, специальный умысел, направленный на получение компьютерных данных или иной умысел, подразумевающий уголовную ответственность). Также они могут постановить, что правонарушение должно быть совершено в отношении компьютерной системы, связанной удаленно с другой компьютерной системой. Последний вариант позволяет сторонам исключить ситуацию, когда лицо физически получает доступ к отдельному компьютеру без использования другой компьютерной системы. Стороны могут принять за правонарушение исключительно незаконный доступ в сетевые компьютерные системы (включая публичные сети, предоставляемые телекоммуникационными службами и частные сети, такие как интранет или экстранет).

Незаконный перехват (Статья 3)

51. Это положение защищает право на конфиденциальность при передаче данных. Данное правонарушение нарушает конфиденциальность при передаче данных таким же образом, как перехват и запись телефонных разговоров. Право на тайну переписки закреплено в Статье 8 Европейской Конвенции Прав человека. Правонарушение, определенное Статьей 3, применяет тот же принцип ко всем формам электронной передачи данных, будь то телефон, факс, электронная почта или пересылка файлов.

52. Основная часть текста положения взята из определения правонарушения, названного «незаконным перехватом» (см. Рекомендацию (89) 9). В Конвенции разъяснено,

что речь может идти как о «передаче компьютерных данных», так и об электромагнитном излучении при указанных ниже обстоятельствах.

53. Перехват с помощью «технических устройств» подразумевает прослушивание, контроль или наблюдение за содержимым передаваемых данных, а также получение данных либо напрямую, с использованием компьютерной системы, либо опосредованно, с использованием устройств электронного прослушивания. Перехват может включать в себя и запись данных. К техническим средствам относятся устройства, подключенные к линиям передачи, а также устройства для перехвата и записи беспроводного обмена данными. При этом также может быть использовано программное обеспечение, пароли и коды. Использование технических средств – ограничительное условие, помогающее избежать чрезмерной криминализации.

54. Правонарушение связано с «непубличной» передачей компьютерных данных. Понятие «непубличный» определяет характер процесса передачи (обмена), но не характер передаваемых данных. Данные могут быть информацией, доступной публично, однако стороны пожелали обмениваться ими конфиденциально. Или же данные могут держаться в тайне в коммерческих целях, пока услуга не оплачена (как, например, в Pay-TV). Следовательно, само понятие «непубличный» не исключает обмен данными через публичные сети. В соответствии со Статьей 3 (см. решение ЕСПЧ по делу «Халфорд против Соединенного Королевства» от 25 июня 1997 г, 20605/92) также защищен от незаконного перехвата обмен данными между наемными сотрудниками в

деловых или иных целях, в том числе «непубличная передача компьютерных данных».

55. Передача компьютерных данных может происходить в пределах одной компьютерной системы (например, поток данных от процессора к экрану или принтеру); между двумя компьютерными системами, принадлежащими одному лицу; между двумя компьютерами, обменивающимися данными друг с другом; или между компьютером и человеком (например, через клавиатуру). Тем не менее, в качестве дополнительного определяющего признака Стороны могут принять передачу данных между компьютерными системами, связанными удаленно.

56. Несмотря на то, что понятие «компьютерной системы» может также подразумевать радиосвязь, это не означает, что одна из Сторон обязана подвергнуть криминализации перехват радиопередач. Даже будучи «непубличной», радиопередача происходит в относительно открытой форме, и, следовательно, может быть перехвачена, к примеру, радиолюбителями.

57. Учет правонарушений, связанных с «электромагнитным излучением», расширяет сферу действия данного положения. Электромагнитное излучение может исходить от компьютера во время его работы. Такое излучение не рассматривается как «данные» в соответствии с определением в Статье 1. Однако данные могут быть восстановлены при использовании такого излучения. Следовательно, перехват данных из электромагнитного излучения компьютерной системы считается правонарушением в соответствии с данным положением.

58. Чтобы перехват данных можно было отнести к правонарушениям, он должен быть совершен «намеренно» и «неправомерно». Перехват правомерен, если совершающее его лицо имеет на это право; например, если оно действует согласно указаниям или с разрешения участников передачи (включая санкционированное тестирование или мероприятия по защите, на которые участники дали свое согласие). Наблюдение может производиться на законных основаниях следственными органами, в интересах национальной безопасности, а также в целях выявления правонарушений. Кроме того, было решено, что использование общераспространенных торговых практик, например, применение файлов «cookie», не должно считаться правонарушением, поскольку оно не является «неправомерным» перехватом данных. Если говорить о непубличном обмене информацией между сотрудниками, защищенном Статьей 3 (см. пункт 54 выше), то в этом случае внутреннее законодательство может предоставить основания для законного перехвата такого обмена. Согласно Статье 3, перехват при таких обстоятельствах считается осуществленным «правомерно».

59. В некоторых странах перехват данных может быть тесно связан с незаконным доступом к компьютерной системе. Чтобы обеспечить согласованность в запрете и преследовании подобных действий, страны, в которых в соответствии со Статьей 2 для криминализации требуется наличие злого умысла или совершение правонарушения в отношении компьютерной системы, связанной с другой компьютерной системой, могут также установить другие уточнения. Эти уточнения должны интерпретироваться и применяться вместе с другими понятиями, определяющими деяние, такими как «намеренное» и «неправомерное».

Вмешательство в данные (Статья 4)

60. Целью данного положения является обеспечение защиты компьютерных данных и программ от намеренного повреждения, аналогичной защите материальных объектов. В данном случае защищаемый правовой интерес – целостность и правильное функционирование или использование хранимых компьютерных данных, либо программ.

61. В пункте 1 определяются частично совпадающие термины «повреждение» и «ухудшение качества»: негативные изменения в целостности или в информационном наполнении данных и программ. «Удаление» данных приравнивается к уничтожению материального объекта. Оно уничтожает данные и делает их неузнаваемыми. Под блокировкой компьютерных данных подразумевается любое действие, ограничивающее или перекрывающее доступ к ним лицу, пользующемуся компьютером, или носителю, на котором эти данные хранились. Термин «изменение» означает видоизменение существующих данных. Следовательно, ввод вредоносных программ, таких как вирусы и трояны, подпадает под действие данного пункта, равно как и вызванные ими изменения в данных.

62. Вышеупомянутые действия подлежат наказанию только в том случае, если совершаются «неправомерно». Общепринятые действия, связанные с разработкой компьютерных сетей, как и обычные эксплуатационные или коммерческие методы практики являются правомерными, и, следовательно, не могут быть признаны незаконными в соответствии с этой статьей. К таким методам относятся,

в частности, тестирование и защита безопасности компьютерной системы с разрешения ее владельца или оператора, или изменение конфигурации операционной системы компьютера в случае, если оператору системы нужно новое программное обеспечение (например, установка программного обеспечения для доступа в Интернет и удаление ранее установленных подобных программ). Изменения информации о трафике в целях обеспечения анонимного обмена информацией (например, работа анонимных транзитных почтовых узлов) или изменение данных в целях безопасности обмена информацией (например, шифрование), должны рассматриваться как обоснованная защита конфиденциальности, и, следовательно, считаться правомерными. Однако по решению Сторон незаконными могут быть объявлены определенные злоупотребления, связанные с анонимным обменом информацией – например, такие, при которых информация о заголовках пакетов изменяется для того, чтобы скрыть личность преступника.

63. В дополнение к этому правонарушитель должен действовать «умышленно».

64. Пункт 2 позволяет Сторонам сделать оговорку, приняв обязательным условием правонарушения причинение значительного ущерба. Интерпретация понятия значительного ущерба предоставляется внутреннему законодательству, однако Стороны должны уведомить Генерального Секретаря Совета Европы о своей интерпретации, если такая оговорка используется.

Вмешательство в работу системы (Статья 5)

65. В рекомендации № (89) 9 это правонарушение обозначено термином «компьютерный саботаж». Цель данного положения – привлечение к уголовной ответственности за умышленное воспрепятствование законному использованию компьютерных систем, в том числе, телекоммуникационного оборудования, путем использования или модификации компьютерных данных. Под защитой данного положения находится право операторов и пользователей на нормальную работу компьютерных или телекоммуникационных систем. Текст положения сформулирован нейтрально для того, чтобы защита распространялась на все виды функций.

66. Термин «воспрепятствование» обозначает действия, мешающие нормальной работе компьютерной системы. Оно должно происходить путем ввода, передачи, повреждения, удаления, изменения или блокировки компьютерных данных.

67. Более того, воспрепятствование должно также быть «существенным», чтобы повлечь за собой уголовное преследование. Каждая из Сторон самостоятельно определяет критерии для признания воспрепятствования существенным. К примеру, Сторона может установить уровень минимального причиненного ущерба. Составители документа сочли «существенным» ущербом пересылку данных системе в такой форме, размере, или с такой частотой, что она будет отрицательным образом сказываться на возможности владельца или оператора пользоваться системой или обмениваться информацией с другими системами. К подобным

видам пересылки данных относятся программы, вызывающие отказ в обслуживании; вредоносные программы, например, вирусы, ухудшающие работу системы; или программы, отправляющие получателю большое количество электронных сообщений с целью блокировки коммуникационных возможностей системы.

68. Воспрепятствование должно производиться «неправомерно». Общепринятые действия, применяемые при разработке сетей, и обычные эксплуатационные или коммерческие методы являются правомерными. К ним относятся, в частности, тестирование компьютерной системы или защита ее безопасности, разрешенные ее владельцем или оператором, а также изменение конфигурации системы, которое происходит, если оператор устанавливает новое программное обеспечение и удаляет ранее установленные подобные программы. Следовательно, даже если в результате таких действий происходит существенное затруднение в работе системы, в соответствии с этой статьей они не считаются правонарушением.

69. Отправка несогласованных с получателем электронных сообщений в коммерческих или иных целях может доставить неудобства получателю, в частности, если подобные сообщения отправляются часто или в больших количествах («спам»). По мнению составителей документа, такие действия имеют состав преступления только в случае, если они умышленно и существенно препятствуют обмену информацией. Тем не менее, Стороны могут выбрать иной законодательный подход и придать определенным видам вмешательства статус административного правонарушения или действия, подлежащего иным видам ответственности.

Текст документа предоставляет Сторонам право определять степень затруднения работы системы (частичное или полное, временное или постоянное), чтобы установить порог ущерба, начиная с которого, в соответствии с их законодательством, будет применяться административное или уголовное наказание.

70. Правонарушение должно быть совершено умышленно, то есть правонарушитель должен действовать с намерением затруднить работу системы.

Незаконное использование устройств (Статья 6)

71. Согласно этому положению независимым уголовным преступлением объявляются умышленные незаконные действия в отношении определенных устройств и незаконное использование данных для совершения описанных выше правонарушений против конфиденциальности, целостности и доступности компьютерных систем или данных. Поскольку совершение таких правонарушений часто требует владения средствами доступа («хакерскими инструментами»), или другими инструментами, существует серьезное побуждение приобретения их в преступных целях, что впоследствии может привести к появлению черного рынка по их производству и распространению. Для более эффективной борьбы с подобной угрозой уголовное, законодательство должно категорически запрещать определенные потенциально опасные действия, предотвращая тем самым правонарушения, описанные в Статьях 2 – 5. Данное положение основывается на выводах, сделанных недавно Советом Европы (Европейская Конвенция по правовой защите

услуг условного доступа или услуг, основывающихся на нем – ETS № 178) и Евросоюзом (Директива 98/84/ЕС Европарламента и Совета Европы от 20 ноября 1998 года по правовой защите услуг, основывающихся на условном доступе), а также на соответствующих положениях законодательства некоторых стран. Подобный подход уже применялся в 1929 году в Женевской Конвенции по подделке денежных знаков.

72. Пункт 1(a)1 объявляет незаконным производство, продажу, поставку, импорт, распространение устройств или иное предоставление доступа к ним. Под его действие подпадают также компьютерные программы, созданные или измененные с целью совершения любых правонарушений, описанных в Статьях 2–5 Конвенции. «Распространение» подразумевает активные действия по отправке данных другим лицам, в то время как «предоставление доступа» подразумевает размещение таких устройств в Интернете для использования другими лицами. Этот термин также включает в себя создание или компиляцию гиперссылок, облегчающих доступ к таким устройствам. Под «компьютерными программами» подразумеваются программы, созданные для изменения или уничтожения данных, либо для вмешательства в работу систем, а также программы, созданные или измененные для получения доступа к компьютерным системам.

73. Составители документа долго не могли прийти к соглашению относительно того, не следует ли ограничить устройства только теми, которые специально созданы для совершения правонарушений, исключив устройства, имеющие двойное назначение. Такое ограничение было сочтено

слишком узким. Оно могло бы создать существенные помехи при предоставлении доказательств во время уголовных процессов, что сделало бы данное положение практически неприменимым, или применимым в редких случаях. Альтернативный вариант с включением всех типов устройств, даже если они произведены и распространяются на законных основаниях, также был отвергнут. В этом случае решающим фактором для привлечение к ответственности за компьютерное правонарушение стал бы субъективный признак умысла. Этот подход не был применен в области подделки дензнаков. В качестве разумного компромисса Конвенция ограничивает область действия статьи теми случаями, когда устройства объективно созданы или изменены в целях совершения правонарушения. Такое ограничение в большинстве случаев исключит устройства двойного назначения.

74. Пункт 1(a)2 объявляет незаконным использование, продажу, поставку, импорт, распространение или иное предоставление доступа к компьютерному паролю, коду доступа или иным подобным данным, с помощью которых может быть получен доступ ко всей компьютерной системе или ее части.

75. Пункт 1(b) объявляет незаконным владение объектами, описанными в пунктах 1(a)1 и 1(a)2. Последнее предложение пункта 1(b) позволяет Сторонам законодательно определять количество таких объектов, которое используется в качестве прямого доказательства преступного умысла. Каждая Сторона вправе решать, какое количество объектов ведет к уголовной ответственности.

76. Необходимо, чтобы правонарушение было совершено умышленно и неправомерно. Чтобы избежать опасности чрезмерной криминализации в тех случаях, когда устройства производятся и выпускаются на рынок в законных целях – например, для отражения атак на компьютерные системы – вводятся иные ограничивающие признаки правонарушения. Помимо общего умысла, должен существовать особый (т.е. прямой) умысел использования устройства в целях совершения любых правонарушений, описанных в Статьях 2–5 Конвенции.

77. Пункт 2 четко устанавливает, что инструменты, созданные для авторизованной проверки или защиты компьютерной системы, не подпадают под действие данного положения. Это понятие уже содержится в определении термина «неправомерный». К примеру, тестовые устройства («устройства взлома») и устройства анализа системы, промышленно созданные для тестирования надежности информационных технологий или для проверки безопасности систем, производятся для законных целей и рассматриваются как применяемые «правомерно».

78. Поскольку необходимость распространения положения о «Незаконном использовании устройств» на все виды компьютерных правонарушений, описанных в Статьях 2–5, оценивается по-разному, пункт 3 позволяет на основании оговорки (сравн. со Статьей 42), ограничить данное правонарушение во внутреннем законодательстве. Каждая из Сторон, однако, обязана объявить незаконными по крайней мере продажу, распространение или предоставление компьютерного пароля и данных для доступа, в соответствии с пунктом 1(a)2.

Подраздел 2 – Правонарушения, связанные с использованием компьютерных средств

79. Статьи 7–10 описывают обычные преступления, которые часто совершаются с использованием компьютерных систем. Большинство стран уже придали таким действиям статус незаконных, и их законодательства могут как широко, так и частично охватывать ситуации, в которых задействованы компьютерные сети (к примеру, существующие в некоторых странах законы о детской порнографии могут не касаться электронных изображений). Следовательно, принимая эти статьи, страны должны изучить существующие законодательства, чтобы определить, применимы ли они к ситуациям, в которых задействованы компьютерные системы или сети. Если существующее законодательство подразумевает подобные действия, то вносить в него поправки или вводить новые законы не требуется.

80. «Подлог и фальсификация, связанные с использованием компьютерных средств» – это правонарушения, совершенные с использованием компьютера, т.е. две особые разновидности манипуляций с компьютерными системами или данными. Включение их в документ является признанием того факта, что во многих странах некоторые традиционные правовые интересы недостаточно защищены от новых форм вмешательств и атак.

Подлог с использованием компьютерных технологий (Статья 7)

81. Целью данной статьи является создание понятия правонарушения, сходного с подлогом вещественных

документов. Ее действие направлено на устранение пробелов в уголовном законодательстве, рассматривающем обычный подлог. Текущее законодательство требует, чтобы показание или заявление, включенное в документ, можно было прочесть; оно неприменимо к данным, хранящимся в электронном виде. Однако манипулирование подобными данными, имеющими доказательную силу, может привести к столь же серьезным последствиям, что и обычный подлог, если при их помощи третья сторона вводится в заблуждение. К подлогу с использованием компьютерных технологий относится несанкционированное создание или изменение хранимых данных, которые в результате приобретают иную доказательную силу в суде, полагающемся на подлинность информации и таким образом основывающемся на обмане. Защищаемый правовой интерес – безопасность и надежность электронных данных, которые могут повлиять на правовые отношения.

82. Следует отметить, что понятие подлога в разных странах существенно различается. В одних оно основывается на подлинности авторства документа, в других – на правдивости содержащихся в документе фактов. Однако было решено, что подделка подлинности должна касаться как минимум источника данных, независимо от правильности или достоверности содержимого. Стороны могут пойти дальше и включить в термин «подлинность» правдивость данных.

83. Это положение касается данных, которые равноценны общедоступному или частному документу и имеют юридическую силу. Несанкционированный ввод верных или неверных данных приводит к ситуации, приравнивающейся к изготовлению фальшивого документа. Последующие

изменения (модификация, варьирование, частичное изменение), уничтожение (удаление данных с носителя) и блокировка (утаивание и сокрытие данных) в целом соответствуют фальсификации подлинного документа.

84. Термин «в правовых целях» распространяется также на юридически обоснованные законные действия и документы.

85. Последнее предложение данного положения позволяет Сторонам, учитывающим такие правонарушения во внутреннем законодательстве, сделать наличие преступного умысла необходимым условием для привлечения лица к уголовной ответственности.

Мошенничество с использованием компьютерных технологий (Статья 8)

86. В результате технологической революции стали более распространены такие экономические преступления, как мошенничество, и, в частности, мошенничество с использованием кредитных карт. Имущество, которое управляется при помощи компьютерных систем или представлено в них (электронные деньги, депозиты), стало такой же мишенью для мошенников, как и традиционные формы собственности. Подобные преступления заключаются главным образом во вводе поддельных данных: в компьютер вводится неверная информация, либо происходит вмешательство в процессе обработки данных при помощи программ и иных средств. Цель настоящей статьи – криминализация неправомерного манипулирования данными в процессе их обработки для осуществления незаконной передачи имущества.

87. Чтобы предусмотреть все возможные виды мошенничества, его основные признаки – «ввод», «изменение», «уничтожение» и «блокирование» (Статья 8(a)) – были дополнены общим определением «вмешательства в работу компьютерной программы или системы» (Статья 8 (b)). Понятия «ввод, изменение, уничтожение или блокирование» имеют то же значение, что и в предыдущих статьях. Статья 8 (b) предусматривает манипуляции с компьютерным оборудованием, действия, препятствующие выводу данных на печать, и действия, влияющие на запись или поток данных, или на последовательность работы программ.

88. Мошеннические действия с использованием компьютерных технологий считаются незаконными, если они наносят прямой экономический убыток или утерю собственности другого лица, и если правонарушитель действует с целью получения незаконной экономической выгоды для себя или иного лица. Термин «материальные убытки» является широким понятием, включающим в себя потерю денег, материальных и нематериальных благ, имеющих экономическую ценность.

89. Правонарушение должно быть совершено «неправомерно», и экономическая выгода должна быть также получена неправомерно. Разумеется, законные общепринятые торговые практики, направленные на получение экономической выгоды, не входят в понятие правонарушения, установленного в данной статье, поскольку производятся правомерно. К примеру, действия, произведенные в соответствии с действующим договором между потерпевшими сторонами, являются правомерными (например, прекращение работы веб-сайта, произведенное по условиям договора).

90. Правонарушение должно быть совершенно «умышленно». Общий признак умысла касается манипуляций с компьютером или вмешательства в его работу, которое приводит к материальным убыткам для другого лица. Правонарушение подразумевает также наличие особого мошеннического или иного преступного умысла, направленного на получение экономической или иной выгоды для себя или другого лица. Таким образом, торговые практики рыночной конкуренции, которые могут привести к экономическому ущербу для одного лица и к выгоде для другого, но не применяются с мошенническим или нечестным умыслом, не подпадают под понятие правонарушения, установленное данной статьей. К примеру, использование программ для сравнения магазинов в Интернете («ботов»), даже если оно не санкционировано сайтом, который посещает «бот», не является незаконным.

Подраздел 3 – Правонарушения, связанные с содержанием данных

Правонарушения, связанные с детской порнографией (Статья 9)

91. Цель Статьи 9 о детской порнографии – укрепление защитных мер по отношению к детям и борьба с их сексуальной эксплуатацией. Статья модернизирует положения уголовного права, более эффективно описывая использование компьютерных систем при совершении преступлений сексуального характера в отношении детей.

92. Это положение является ответом на озабоченность глав государств и правительств Совета Европы, которую они

выразили во время 2 саммита (Страсбург, 10–11 октября 1997 г.) в Плане действий (пункт III.4). Оно также соответствует международной тенденции к запрету детской порнографии, о чем свидетельствуют принятый недавно Дополнительный протокол к Конвенции ООН о правах детей, торговле детьми, детской проституции и детской порнографии, и недавняя инициатива Европейской Комиссии по борьбе с сексуальной эксплуатацией детей и детской порнографией (COM2000/854).

93. Данное положение относит к незаконным различные аспекты электронного производства, владения и распространения детской порнографии. Большинство государств уже считают преступлением обычное производство и физическое распространение детской порнографии. Однако из-за широкого использования Интернета в качестве основного инструмента торговли подобными материалами, появилась необходимость принятия специальных положений международных правовых актов, направленных на борьбу с новой формой эксплуатации детей и с угрозой их жизни и здоровью. Широко распространено мнение, что подобные материалы и такие действия в Интернете, как обмен идеями, фантазиями и советами в среде педофилов, поддерживают и поощряют людей в совершении сексуальных преступлений против детей.

94. Пункт 1(a) объявляет незаконным производство детской порнографии для распространения через компьютерные системы. Это положение стало необходимым для борьбы с источниками вышеописанных угроз.

95. Пункт 1 (b) объявляет незаконным «предложение» детской порнографии через компьютерные системы.

«Предложение» подразумевает рекомендации другим лицам по приобретению детской порнографии. Это означает, что лицо, предлагающее подобный материал, фактически может его предоставить. «Обеспечение доступа» подразумевает размещение детской порнографии в Интернете для использования другими лицами, например, путем создания порнографических сайтов. Данный пункт также подразумевает создание или компиляцию гиперссылок на сайты с детской порнографией, что облегчает доступ к таким материалам.

96. Пункт 1 (c) объявляет незаконным распространение или передачу детской порнографии через компьютерные системы. Под «распространением» понимается активное размещение подобных материалов. Пересылка детской порнографии через компьютерную систему другому лицу считается незаконной «передачей» детской порнографии.

97. Термин «приобретение для себя или другого лица» в пункте 1 (d) означает активное получение детской порнографии, например, путем ее скачивания.

98. 98. Хранение детской порнографии в компьютерной системе или на носителе данных, например, на дискете или компакт-диске, объявляется незаконным в пункте 1 (e). Владение детской порнографией стимулирует спрос на такого рода материалы. Эффективным способом сокращения производства детской порнографии является обеспечение уголовного преследования всех участников этой цепи от производства до хранения.

99. Термин «порнографические материалы» в пункте 2 обусловлен национальными стандартами, классифицирующими

материалы как непристойные и не соответствующие общественной морали. Соответственно, материалы, имеющие художественную, медицинскую, научную или другую подобную ценность, не рассматриваются как порнографические. Визуальное изображение включает в себя данные, сохраненные на дискете или других электронных устройствах хранения, которые могут трансформироваться в визуальные изображения.

100. Под «откровенными сексуальными действиями» поднимаются следующие реальные или инсценированные действия: a) половой акт, включая генитальный, орально-генитальный, анально-генитальный или орально-анальный акт между несовершеннолетними лицами, между взрослым и несовершеннолетним лицом одного или противоположного пола; b) скотоложство; c) мастурбация; d) сексуальные действия садистского или мазохистского характера; или e) демонстрация гениталий или интимных зон несовершеннолетним лицом, носящая развратный характер. Не имеет значения, реальны подобные действия или инсценированы.

101. Три типа материалов, определенные в пункте 2 и связанные с правонарушениями, описанными в пункте 1, включают в себя: изображения сексуального насилия по отношению к реальному ребенку (2a); порнографические изображения лица, кажущегося несовершеннолетним и выполняющего откровенные сексуальные действия (2b); и, наконец, изображения, которые, будучи «реалистичными», в действительности не показывают реального ребенка, совершающего откровенно сексуальные действия (2c). Последний вид материалов включает в себя видоизменен-

ные изображения, к примеру, графически обработанные изображения реальных людей, или же полностью созданные компьютером материалы.

102. В трех случаях, предусмотренных пунктом 2, защищаемые правовые интересы несколько различаются. Пункт 2(a) концентрируется непосредственно на защите детей от насилия. Пункты 2(b) и 2(c) имеют своей целью обеспечение защиты от поведения, которое не всегда причиняет вред «ребенку», изображенному в материалах, поскольку реального ребенка может и не существовать, однако может быть использовано для совращения или поощрения детей к участию в подобных действиях. Такое поведение является частью субкультуры, поддерживающей насилие по отношению к детям.

103. Термин «неправомерный» не исключает возможности правовой защиты, наличия освобождающих от ответственности обстоятельств и других принципов, снимающих ответственность с лица при определенных обстоятельствах. Таким образом, термин «неправомерный» позволяет Стороне принять во внимание основные права: свободу мысли, свободу самовыражения и право на частную жизнь. Кроме того, Сторона может обеспечить защиту от действий, связанных с «порнографическими материалами», имеющими художественную, медицинскую, научную или иную подобную ценность. В отношении пункта 2(b), ссылка на «неправомерные» действия может также позволить Стороне снять с лица уголовную ответственность, если установлено, что лицо, изображенное в материалах, не является несовершеннолетним в смысле, предусмотренном данным положением.

104. В соответствии с Пунктом 3, «несовершеннолетним» применительно к детской порнографии является любое лицо, не достигшее 18 лет (см. определение «ребенка» в Конвенции ООН о Правах ребенка (Статья 1)). Установление единого международного возрастного стандарта было сочтено необходимым. Следует отметить, что возраст касается использования реальных или несуществующих детей в качестве сексуальных объектов, и рассматривается отдельно от возраста, в котором допускаются сексуальные отношения. Тем не менее, с учетом того факта, что в некоторых государствах внутреннее законодательство предусматривает более низкий возрастной порог в отношении детской порнографии, последняя фраза пункта 3 позволяет Сторонам установить другой возрастной порог, если не ниже 16 лет.

105. В данной статье перечислены различные типы незаконных действий, связанных с детской порнографией, которые, как и в статьях 2–8, Стороны обязаны признавать преступными, если они совершаются «умышленно». В соответствии с этим стандартом лицо не несет ответственности, если у него не было умысла предлагать, предоставлять доступ, распространять, передавать, производить детскую порнографию или хранить ее. Стороны могут принять более точный стандарт, который в таком случае будет иметь приоритетное значение (см., например, применяемый Европейским Сообществом закон об ответственности поставщиков услуг). К примеру, ответственность может быть возложена при наличии «знания и контроля» над хранимой и передаваемой информацией. Того факта, что поставщик, предоставляющий услугу, служил каналом передачи

информации или предоставлял хостинг сайту или новостной странице, содержащей подобного рода материалы, недостаточно для уголовного преследования без наличия в каждом конкретном случае умысла, подпадающего под внутреннее законодательство. Более того, провайдер не обязан проверять деятельность сайта, чтобы избежать уголовной ответственности.

106. Пункт 4 позволяет Сторонам вносить поправки по пунктам 1(d) и (e), и пунктам 2(b) и (c). Право не применять данные разделы положения может использоваться частично или полностью. Любая подобная поправка должна быть представлена Генеральному Секретарю Совета Европы в момент подписания или при сдаче на хранение ратификационных грамот, документов о принятии, одобрении или присоединении, в соответствии со Статьей 42.

Подраздел 4 – Правонарушения, связанные с нарушением авторских и смежных прав

Правонарушения, связанные с нарушением авторского права и смежных прав (Статья 10)

107. Нарушение права интеллектуальной собственности, в частности авторского права, относится к наиболее распространенным правонарушениям в Интернете, что вызывает озабоченность как у правообладателей, так и у тех, кто профессионально занимается компьютерными сетями. Воспроизведение и распространение в Интернете защищенных авторским правом произведений без согласия правообладателя происходит чрезвычайно часто. К таким защищенным произведениям относятся литературные,

фотографические, музыкальные, аудиовизуальные и другие работы. Легкость, с которой благодаря цифровым технологиям могут создаваться несанкционированные копии, а также масштаб их распространения в электронных сетях привели к необходимости включения в уголовное законодательство соответствующих положений. Необходимо также расширить международное сотрудничество в этой сфере.

108. В соответствии с соглашениями, перечисленными в данной статье, каждая Сторона обязана признать незаконным умышленное нарушение авторского права, когда таковое совершается с использованием компьютерной системы и в промышленном масштабе. Пункт 1 предусматривает уголовную ответственность за нарушение авторского права с использованием компьютерной системы. Нарушение авторского права уже является преступлением почти во всех странах. Пункт 2 касается нарушения смежных прав с использованием компьютерной системы.

109. Нарушение авторского права и смежных прав определяется законодательством каждой Стороны и согласуется с обязательствами, принятыми Стороной в отношении определенных международных актов. Каждая Сторона обязуется считать подобные нарушения незаконными, однако способ определения таких нарушений во внутреннем законодательстве может различаться в зависимости от страны. Обязательства по признанию действий незаконными в соответствии с Конвенцией не касаются нарушений права на интеллектуальную собственность, за исключением случаев, прямо указанных в Статье 10. Следовательно, нарушения, связанные с патентами и торговыми наименованиями, не рассматриваются.

110. Пункт 1 ссылается на Парижский Акт от 24 июля 1971 г. Бернской конвенции о защите литературных и художественных произведений, Соглашение о торговых аспектах права на интеллектуальную собственность (TRIPS), и Договор об авторских правах Всемирной организации интеллектуальной собственности (WIPO). Пункт 2 основан на международной Конвенции о защите исполнителей, создателей фонограмм и транслирующих организаций (Римская конвенция), Соглашении о торговых аспектах права на интеллектуальную собственность (TRIPS), и Договоре об исполнителях и фонограммах Всемирной организации интеллектуальной собственности (WIPO). Использование выражения «в соответствии с принятыми обязательствами» в обоих пунктах говорит о том, что участвующая в Конвенции Сторона не обязана применять условия указанных соглашений, если она в них не участвует. Более того, если Сторона приняла поправку или заявление в соответствии с одним из этих соглашений, такая поправка может ограничить степень обязательств Стороны по данной Конвенции.

111. Договор об авторских правах Всемирной организации интеллектуальной собственности (WIPO) и Договор об исполнителях и фонограммах Всемирной организации интеллектуальной собственности (WIPO) не вступили в силу на момент заключения настоящей Конвенции. Тем не менее, эти договоры крайне важны, так как они существенно совершенствуют международную защиту интеллектуальной собственности (особенно в отношении нового права «предоставления доступа» к защищенным материалам «по запросу» через Интернет) и улучшают средства борьбы с нарушениями

прав интеллектуальной собственности во всем мире. Однако следует понимать, что нарушения прав, оговоренные в данных документах, не должны признаваться правонарушениями по Конвенции, пока эти договоры не вступят в силу в отношении какой-либо Стороны.

112. Обязательство признать незаконными нарушения авторских и смежных прав согласно принятым международным актам, не распространяется на моральное право, обеспеченное упомянутыми актами (такими как Статья 6bis Бернской конвенции и Статья 5 Договора об авторских правах WIPO).

113. Для применения уголовной ответственности нарушение авторских и смежных прав должно совершаться «умышленно». В противоположность всем остальным положениям материально-правового законодательства в данной Конвенции, понятие «умышленно» используется вместо «преднамеренно» в пунктах 1 и 2, поскольку это понятие применяется в Договоре TRIPS (Статья 61), имеющем приоритетную силу при признании нарушений авторских прав незаконными.

114. Данные положения обеспечивают уголовное преследование за нарушение прав «в промышленном масштабе» и с использованием компьютерной системы. Это согласуется со Статьей 61 Договора TRIPS, требующей уголовного наказания в вопросах авторского права только в случаях «пиратства в промышленном масштабе». Однако Стороны могут пожелать перешагнуть порог «промышленного масштаба» и признать незаконными иные виды нарушения авторских прав.

115. Термин «неправомерно» был опущен в тексте данной статьи как излишний, поскольку понятие «нарушение авторских прав» уже подразумевает несанкционированное использование авторских материалов. Однако отсутствие термина «неправомерно», не исключает возможности защиты, учета оправдывающих обстоятельств и принципов уголовного законодательства, обуславливающего исключение уголовной ответственности, связанной с термином «неправомерно» где-либо еще в тексте данной Конвенции.

116. Пункт 3 позволяет Сторонам не применять уголовное наказание в соответствии с пунктами 1 и 2 в «ограниченных обстоятельствах» (например, при параллельном импорте, правах на прокат), при условии доступности других эффективных средств, в том числе, гражданских и/или административных мер. Данное положение допускает частичное освобождение Сторон от обязательств налагать уголовную ответственность, при условии, что Стороны не отменяют обязательств, принятых в соответствии со Статьей 61 Договора TRIPS. Эта статья является уже существующим минимальным требованием в отношении признания действий незаконными.

117. Данная статья ни в коей мере не подразумевает распространения защиты, которая предоставляется авторам, продюсерам фильмов, исполнителям, создателям фонограмм, транслирующим организациям или другим правообладателям на лиц, не обладающих этим правом в соответствии с внутренним законодательством или международными соглашениями.

Подраздел 5 – Дополнительные виды ответственности и санкции

Покушение, соучастие или подстрекательство к совершению преступления (Статья 11)

118. Данная статья определяет дополнительные правонарушения, связанные с покушением, соучастием или подстрекательством к совершению определенных в Конвенции преступлений. Как указано ниже, от Стороны не требуется считать незаконной попытку совершения каждого из преступлений, установленных данной Конвенцией.

119. Пункт 1 требует от Сторон признавать уголовным преступлением соучастие или подстрекательство к совершению любых правонарушений, описанных в Статьях 2–10. Уголовная ответственность за соучастие и подстрекательство возникает случаях, если лицу, совершившему описанное в Конвенции преступление, умышленно содействует другое лицо. Пример: передача вредоносных данных или программ через Интернет требует содействия поставщика услуг, который служит в качестве канала коммуникации. Однако поставщик, не имеющий преступного умысла, не может нести уголовную ответственность. Следовательно, на поставщика не возлагается обязанность активно проверять информационное наполнение ресурса, чтобы избежать уголовной ответственности.

120. Что касается пункта 2 о попытке преступления, некоторые правонарушения, определенные в Конвенции, как и их части, были сочтены сложными для совершения (например, предложение или предоставление доступа к детской порнографии). Кроме того, некоторые правовые системы

ограничивают список правонарушений, попытка совершения которых подлежит наказанию. В связи с этим требуется, чтобы попытка правонарушения, установленная Статьями 3, 4, 5, 7, 8, 9(1)(a) и(1)(c), была признана незаконной.

121. Как в случае всех правонарушений, установленных в Конвенции, покушение, соучастие, и подстрекательство должны быть умышленными.

122. Пункт 3 был добавлен для разрешения трудностей, которые могут возникнуть у Сторон в отношении пункта 2, несмотря на предпринятую в пункте 2 попытку исключить определенные аспекты из положения о покушении. Он учитывает широту спектра понятий в различных законодательных системах. Сторона может заявить, что сохраняет за собой право не применять пункт 2 или его часть. Это означает, что любая Сторона, делающая оговорку по поводу данного положения, не обязана считать покушение преступлением, либо же она может выбрать правонарушения или их части, за покушение на которые возникнет уголовная ответственность. Цель такой оговорки – сделать как можно более широкой ратификацию Конвенции, в то же время позволяя Сторонам сохранить некоторые из своих фундаментальных юридических принципов.

Корпоративная ответственность (Статья 12)

123. Статья 12 посвящена ответственности юридических лиц. Она следует юридической тенденции признания корпоративной ответственности. Ее цель – привлечение к ответственности корпораций, ассоциаций и подобных юридических лиц за преступления, совершенные

руководителем, если последний действовал в интересах юридического лица. Статья 12 также рассматривает возможность привлечения к ответственности в тех случаях, когда руководящее лицо не осуществляет наблюдение или контроль над сотрудником или представителем юридического лица, и это способствует совершению ими одного из правонарушений, установленных Конвенцией.

124. В соответствии с пунктом 1, для возникновения ответственности должны быть соблюдены четыре условия. Во-первых, должно быть совершено одно из правонарушений, описанных в Конвенции. Во-вторых, это правонарушение должно быть совершено в интересах юридического лица. В-третьих, совершить правонарушение (включая соучастие и подстрекательство) должно лицо, занимающее руководящий пост. Под термином «лицо, занимающее руководящий пост» подразумевается реальное лицо, занимающее высокий пост в организации, например, директор. В-четвертых, лицо, занимающее руководящий пост, должно действовать на основании одного из следующих прав: права представлять юридическое лицо или права принимать решения и осуществлять контроль. Последнее условие говорит о том, что физическое лицо действовало в рамках своих полномочий. В целом, пункт 1 обязывает Стороны привлечь юридическое лицо к ответственности только за правонарушения, совершенные такими руководящими лицами.

125. Кроме того, пункт 2 обязывает Стороны иметь возможность привлечь юридическое лицо к ответственности в тех случаях, когда преступление совершается не руководителем, как это описано в пункте 1, а иным лицом,

действующим от имени юридического лица, т.е. одним из его сотрудников или представителей, действующих в рамках своих полномочий. Для возникновения уголовной ответственности должны быть соблюдены следующие условия: (1) Правонарушение совершено сотрудником или представителем юридического лица; (2) Правонарушение совершено в интересах юридического лица; (3) Совершение правонарушения стало возможным из-за того, что руководящее лицо не осуществляло контроль над сотрудником или представителем. В данном контексте неосуществление контроля означает непринятие соответствующих мер для предотвращения преступлений, совершенных сотрудниками или представителями от имени юридического лица. Подобные меры могут определяться различными факторами, такими как род деятельности компании, ее размер, стандарты, принятые в ней деловые практики, и т.д. Это понятие не следует интерпретировать как требование установления слежки за общением сотрудников (см. также пункт 54). Поставщик не несет ответственности, если преступление было совершено в его системе клиентом, пользователем или иным третьим лицом, поскольку термин «действующий на основании полномочий» применяется исключительно к сотрудникам и представителям, действующим в рамках своих полномочий.

126. Ответственность, возникающая по данной Статье, может быть уголовной, гражданско-правовой или административной. Каждая Сторона вольна выбрать любую или все формы ответственности в соответствии со своими законодательными принципами. Кроме того, выбор должен соответствовать критериям, приведенным в Статье 13, пункт 2,

т.е. санкции или меры должны быть «эффективными, соразмерными и оказывающими сдерживающее воздействие» и включать денежные взыскания.

127. Пункт 4 разъясняет, что корпоративная ответственность не исключает индивидуальной ответственности.

Санкции и меры (Статья 13)

128. Данная статья тесно связана со Статьями 2–11, определяющими различные уголовно наказуемые правонарушения, совершенные с использованием компьютера или связанные с таким использованием. В соответствии с обязательствами, налагаемыми этими статьями, данное положение требует от Сторон юридически преследовать такие серьезные правонарушение и обеспечивать уголовные санкции, являющиеся «эффективными, соразмерными и оказывающими сдерживающее воздействие». В случае применения к реальным лицам, к ним может относиться наказание в виде тюремного заключения.

129. Юридические лица, чья ответственность устанавливается в соответствии со Статьей 12, также подвергаются санкциям, являющимся «эффективными, соразмерными и оказывающими сдерживающее воздействие», которые могут носить уголовный, административный или гражданско-правовой характер. Стороны договора обязаны согласно пункту 2 обеспечить возможность наложения денежного взыскания с юридических лиц.

130. Статья оставляет открытой возможность применения других санкций или мер, соответствующих серьезности правонарушения; например, может применяться судебный

запрет или имущественное наказание. Создание системы уголовных правонарушений и санкций, которая соответствовала бы их внутреннему законодательству, остается на усмотрении Сторон.

Часть 2 – Процессуальное законодательство

131. Статьи данной части описывают процессуальные меры, принимаемые на государственном уровне для уголовного расследования правонарушений, предусмотренных в Части 1, других уголовных преступлений, совершенных с использованием компьютерной системы, и сбора доказательств в электронной форме. В соответствии со Статьей 36, пунктом 3, никакая часть Конвенции не требует от Сторон введения полномочий и процедур сверх описанных в данной Конвенции, равно как и не препятствует таковому.

132. Технологическая революция привела к появлению «электронной магистрали», на которой пересекаются многочисленные формы услуг и обмена информацией, а также происходит совместное использование средств передачи и носителей информации. Все это изменило сферу уголовного права и Процессуальных действий. Расширяющаяся коммуникационная сеть открывает новые возможности для преступной деятельности. Это касается как традиционных правонарушений, так и новых технологических преступлений. Материально-уголовное право, уголовно-процессуальный кодекс и методы расследования преступлений не должны отставать от новых форм преступности. В равной степени должны развиваться и изменяться и меры предосторожности, чтобы соответствовать новой технологической среде и новым процессуальным методам.

133. Одной из основных трудностей борьбы с преступностью в сетевой среде является установление личности преступника и оценка уровня ущерба от преступления. Другая проблема – эфемерность электронных данных, которые могут быть изменены, перемещены или удалены в считанные секунды. Лицо, контролирующее данные, может использовать компьютерную систему для их удаления, если они являются объектом уголовного расследования, и таким образом уничтожить улики. Залогом успешного расследования часто являются быстрота и секретность.

134. Конвенция адаптирует к новой технологической среде такие традиционные процессуальные действия, как обыск и изъятие. Кроме того, созданы новые меры (например, оперативное сохранение данных) для поддержания эффективности традиционных методов сбора доказательств в постоянно меняющейся технологической среде. Поскольку данные в этой среде не всегда стабильны, и могут поступать в процессе коммуникации, для их сбора применяются другие процедуры, например, сбор данных о трафике в реальном времени и перехват данных об информационном наполнении. Некоторые из этих методов описаны в Рекомендации Совета Европы № (95)13 по проблемам уголовно-процессуального законодательства, связанным с информационными технологиями.

135. Все положения данного раздела разрешают сбор и получение данных в целях специального уголовного расследования или процессуальных действий. Составители Конвенции обсуждали возможность включения в нее налагаемых на поставщиков обязательств по регулярному сбору и сохранению данных о трафике на определенный

фиксированный период времени. Однако соглашение по этому вопросу не было достигнуто, и такие обязательства не были включены в текст Конвенции.

136. В целом, процедуры касаются всех видов данных, включая три особых вида компьютерных данных (данные о трафике, данные об информационном наполнении и сведения об абонентах), которые могут существовать в двух формах – сохраненные либо находящиеся в процессе передачи. Определения некоторых из этих терминов приведены в Статьях 1 и 18. Возможность применения процедур к одному из видов электронных данных зависит от характера и формы данных, а также от характера процедуры, как указано в каждой статье.

137. При использовании традиционного процессуального законодательства в новой технологической среде возникает вопрос о соответствующей терминологии. Применяются как традиционные формулировки («обыск», «изъятие»), так и новые, технически ориентированные компьютерные термины («доступ», «копирование»), использованные в текстах других международных комиссий по данной тематике (например, Подгруппа G8 по преступлениям в сфере высоких технологий), а также смешанные термины («обыск или аналогичный доступ», «изъятие или аналогичное обеспечение безопасности»). В связи с необходимостью не только отражать развитие понятий в электронной среде, но и устанавливать и сохранять их традиционные истоки, применяется гибкий подход, позволяющий странам использовать либо старые термины «обыск и изъятие», либо новые – «доступ и копирование».

138. Все статьи данного Раздела касаются «уполномоченных органов» и их прав на проведение специальных уголовных расследований и процедур. В некоторых странах только судьи имеют право предписывать и санкционировать сбор и предоставление доказательств. В других странах теми же или подобными полномочиями наделены прокуроры или другие сотрудники правоохранительных органов. Следовательно, термин «уполномоченные органы» относится к судебным, административным или иным правоохранительным органам, которые, согласно внутреннему законодательству, имеют право предписывать, санкционировать или совершать процессуальные действия по сбору и предоставлению доказательств при проведении специальных уголовных расследований и процедур.

Подраздел 1 – Общие положения

139. Данный Раздел начинается с двух положений общего характера, которые применяются ко всем статьям, касающимся процессуального законодательства.

Сфера применения процессуальных норм (Статья 14)

140. Каждая Сторона (Государство) обязана принять необходимые законодательные и иные меры, соответствующие внутреннему законодательству и правовой системе, для установления полномочий и процедур, описанных в данном Разделе и необходимых для «специальных уголовных расследований».

141. С учетом двух исключений, все Стороны должны применять установленные в данном Разделе полномочия и

процедуры к: (I) уголовным преступлениям, совершенным как описано в Статье 1 данной Конвенции; (II) другим уголовным преступлениям, совершенным с использованием компьютерной системы; (III) к сбору доказательств уголовного преступления в электронной форме. Таким образом, полномочия и процедуры, описанные в данном Разделе, должны применяться к правонарушениям, установленным в данной Конвенции, к прочим правонарушениям, совершенным с использованием компьютерной системы, и к сбору доказательств уголовного преступления в электронной форме. Это гарантирует, что доказательства любого уголовного преступления в электронной форме могут быть получены и собраны с использованием полномочий и процедур, указанных в данном Разделе. Это также гарантирует возможность получения компьютерных данных, эквивалентную или аналогичную той, что существует в традиционных процедурах для неэлектронных данных. Конвенция ясно указывает, что Стороны должны сделать законным использование информации, существующей в цифровой или иной электронной форме, в качестве доказательства в суде во время процессуальных действий, независимо от характера уголовного преступления.

142. В сфере применения данных положений существует два исключения. Во-первых, Статья 21 устанавливает, что полномочия на перехват данных об информационном наполнении должны быть ограничены рядом серьезных правонарушений, определенных внутренним законодательством. Многие Государства ограничивают полномочия на перехват устного или телекоммуникационного общения рядом серьезных правонарушений, поскольку признают

конфиденциальность такого общения и интрузивность подобного метода расследования. Подобным же образом Конвенция требует от Сторон лишь установления полномочий и процедур по перехвату данных о содержимом компьютерных коммуникаций в отношении ряда серьезных правонарушений, предусмотренных внутренним законодательством.

143. Во-вторых, Сторона может оставить за собой право применять меры, указанные в Статье 20 (сбор данных о трафике в реальном времени) только к правонарушениям или категориям правонарушений, указанным в оговорках. При этом ряд таких правонарушений или их категорий не должен быть более ограниченным, чем ряд правонарушений, к которым применяются меры перехвата, указанные в Статье 21. Некоторые страны считают сбор данных о трафике не менее интрузивным, чем сбор данных об информационном наполнении. Право на оговорки позволит таким странам ограничить применение мер по сбору данных о трафике в реальном времени тем же рядом правонарушений, к которым они применяют полномочия и процедуры по перехвату в реальном времени данных об информационном наполнении. Однако многие страны не считают перехват данных об информационном наполнении и сбор данных о трафике одинаковыми по степени интрузивности, поскольку сам по себе сбор данных о трафике не собирает и не раскрывает содержание общения. Сбор данных о трафике в реальном времени может играть важную роль в отслеживании источника или получателя компьютерной коммуникации и содействовать установлению личности преступника. Поэтому Конвенция предлагает Сторонам,

использующим право на оговорку, ограничить количество таких оговорок, чтобы как можно шире применять полномочия и процедуры в отношении сбора данных о трафике в реальном времени.

144. Пункт (b) вносит оговорку для стран, которые из-за ограничений, существующих во внутреннем законодательстве на момент принятия Конвенции, не могут перехватывать обмен информацией в компьютерных системах, работающих в интересах закрытой группы пользователей, не использующих публичные коммуникационные сети и не связанных с другими системами. Термин «закрытая группа пользователей» обозначает, например, группу пользователей, использующую одного поставщика услуг – такую как сотрудники компании, которым она дает возможность общаться друг с другом через компьютерную сеть. Термин «не связанная с другими компьютерными системами» подразумевает, что в момент издания распоряжения в соответствии со Статьями 20 или 21 система, по которой передавались данные, не имеет физической или логической связи с другой компьютерной сетью. Термин «не использующая другие публичные коммуникационные сети» исключает системы, которые используют публичные компьютерные сети (включая Интернет), публичные телефонные сети или другие публичные телекоммуникационные средства для передачи информации, независимо от того, является ли это использование очевидным для пользователей.

Условия и гарантии (Статья 15)

145. Введение, осуществление и применение полномочий и процедур, оговоренных в данном Разделе Конвенции,

должно подчиняться условиям и гарантиям, предусмотренным внутренним законодательством каждой из Сторон. Несмотря на обязанность Сторон вводить определенные положения во внутреннее процессуальное законодательство, методы введения и осуществления полномочий и процедур в конкретных случаях оставлены на усмотрение внутреннего законодательства каждой из Сторон. Такие внутренние законы и процедуры, как подробно описано ниже, должны включать в себя условия или гарантии, оговоренные конституционно, законодательно, в судебном или ином порядке. Методы должны включать в себя добавление в качестве условий или гарантий определенных элементов, обеспечивающих баланс между необходимостью исполнения законов и защитой прав и свобод. Поскольку Конвенция касается Сторон, имеющих различные культуры и юридические системы, не представляется возможным детально определить применимые условия и гарантии для каждого полномочия или процедуры. Стороны должны обеспечить этими условиями и гарантиями соблюдение прав и свобод человека. Существуют общепринятые стандарты или минимальные гарантии, которых Стороны Конвенции должны придерживаться. К ним относятся стандарты и минимальные гарантии, возникающие согласно обязательству, принятому на себя Стороной в соответствии с международными правовыми актами, применяемыми в сфере прав человека. Эти акты включают в себя Европейскую Конвенцию 1950 г. по защите прав человека и основных свобод и ее дополнительные Протоколы № 1, 4, 6, 7 и 12 (ETS № 005[4], 009, 046,

4. В текст конвенции были внесены поправки в соответствии с положениями Протокола № 3 (СЕД № 45), вступившего в силу 21

114, 117 и 177), применительно к подписавшим их европейским Государствам. К ним также относятся другие правовые акты, применяемые Государствами-участниками этих соглашений в других регионах (например, Американская Конвенция 1969 г. о правах человека и Африканская Хартия 1981 г. о правах человека и народов). Применяется также Международный пакт 1966 г. о гражданских и политических правах, а также подобные виды защиты, предусмотренные законодательством большинства Государств.

146. Еще одной гарантией в Конвенции является требование, что полномочия и процедуры должны «следовать принципу соразмерности». Этот принцип применяется каждой Стороной в соответствии с действующими нормами внутреннего законодательства. Для европейских стран источником таких норм должны стать принципы Конвенции Совета Европы 1950 г. о защите прав и основных свобод человека, а также применяемые правовые нормы и внутреннее законодательство. Полномочия и процедуры должны быть соразмерны характеру и обстоятельствам правонарушения. Другие страны должны применять соответствующие нормы своего законодательства, например,

---

сентября 1970 г.; Протокола № 5 (СЕД № 55), вступившего в силу 20 декабря 1971 г.; и Протокола № 8 (СЕД № 118), вступившего в силу 1 января 1990 г. В нее вошел также текст Протокола № 2 (СЕД № 44), который, согласно пункту 3 Статьи 5, стал неотъемлемой частью Конвенции с момента ее вступления в силу 21 сентября 1970 г. Все положения, в которые этими Протоколами были внесены поправки или дополнения, заменены. Протоколом №11 (СЕД № 155) с момента его вступления в силу 1 ноября 1998 г. С этой даты Протокол №9 (СЕД № 140), вступивший в силу 1 октября 1994 г., аннулирован, а Протокол №10 (СЕД № 146) утратил свою силу.

ограничение порядка представления доказательств и требование разумной необходимости в обыске и конфискации. Кроме того, приведенное в Статье 21 четкое ограничение (обязательства по мерам перехвата касаются ряда серьезных правонарушений, установленных внутренним законодательством) является ясным примером применения принципа соразмерности.

147. Не ограничивая виды применяемых условий и гарантий, Конвенция требует, чтобы они включали в себя (если это соответствует характеру полномочия или процедуры) судебный или иной независимый надзор, основания для применения полномочия или процедуры, и ограничение сферы и сроков их действия. При использовании юридически обязывающих международных и внутригосударственных принципов внутреннее законодательство определяет, какие из полномочий и процедур имеют достаточно интрузивный характер, чтобы потребовалось применение определенных условий и гарантий. Как указано в Пункте 215, Стороны должны прямо применять такие условия и гарантии в отношении перехвата, если он является интрузивным. В то же время подобные гарантии не следует тем же образом применять к сохранению данных. Другие гарантии, применяемые в соответствии с внутренним законодательством, включают в себя право не свидетельствовать против себя, правовой иммунитет и специфику лиц и мест, к которым применяются меры.

148. Самым важным из вопросов, обсуждаемых в пункте 3, является внимание к «интересам общества», в частности к потребности в «надежном применении законодательства». В той мере, насколько это согласуется с интересами

общества, Стороны должны принимать во внимание другие факторы, такие как воздействие полномочий и процедур на «права, ответственность и законные интересы» третьих сторон, включая провайдеров, ставшее результатом применения принудительных мер, и предпринимать необходимые шаги для смягчения такого воздействия. В целом, в первую очередь должно рассматриваться надежное применение законодательства и прочие общественные интересы (например, общественная безопасность, общественное здоровье, интересы пострадавших, уважение к частной жизни, и др.). Если это согласуется с интересами общества, рассматриваться должны и такие вопросы, как минимизация проблем в бытовом обслуживании, защита от привлечения к ответственности за раскрытие информации или помощь в ее раскрытии, или защита права собственности.

Подраздел 2 – Оперативное обеспечение сохранности хранимых компьютерных данных

149. Меры, указанные в Статьях 16 и 17, применяются к сохраненным данным, которые уже собраны и хранятся у держателей данных – например, у поставщиков услуг. Эти меры не применяются к сбору данных в реальном времени, сбору будущих данных о трафике и к доступу в реальном времени к содержанию информационного обмена. Перечисленные вопросы освещены в Подразделе 5.

150. Описанные меры действуют лишь там, где уже существуют и в данный момент хранятся компьютерные данные. По многим причинам данные, имеющие значение для уголовного расследования, могут более не существовать. Например, если точные данные не были собраны или

сохранены. Законы о защите данных могут требовать удаления важных данных до того, как становится ясна их важность для уголовно-процессуальных действий. В некоторых случаях может не быть коммерческих соображений для сбора и сохранения данных. Например, в случае внесения клиентом фиксированной суммы за услугу, или при предоставлении бесплатных услуг. Статьи 16 и 17 не касаются этих вопросов.

151. Следует различать термины «хранение данных» и «сохранение данных». В обычной речи эти понятия имеют схожее значение, однако в отношении компьютерных данных значения разнятся. Хранить данные означает держать уже имеющиеся данные в записанной форме, защищенной от любых воздействий, способных изменить или повредить их нынешнее качество или состояние. Сохранять данные означает записывать данные, производимые в текущий момент, для владения ими в будущем. Сохранение данных подразумевает сбор данных в настоящем для владения ими в будущем. Хранение данных, напротив, подразумевает действия по содержанию имеющихся данных в сохранности и безопасности.

152. Статьи 16 и 17 касаются лишь хранения данных. Они не дают полномочий на сбор и сохранение всех или части данных, собранных провайдером или иным объектом в процессе его деятельности. Меры по хранению применяются к компьютерным данным, «хранящимся с использованием компьютерной системы», что предполагает, что данные уже существуют, собраны и хранятся. Более того, как указано в Статье 14, все полномочия и процедуры, требуемые в Разделе 2 данной Конвенции, применяются «для

определенных уголовных расследований или процедур», что ограничивает применение таких мер в расследовании конкретного дела. Кроме того, если Сторона вводит в действие меры по хранению в приказном порядке, этот приказ относится к «конкретным хранимым компьютерным данным, находящимся во владении и под контролем лица» (пункт 2). Следовательно, по этим статьям предусматривается только возможность хранения существующих данных вплоть до их последующего раскрытия в соответствии с прочими законными полномочиями в конкретных уголовных расследованиях и процедурах.

153. Обязанность обеспечить хранение данных не требует от Сторон ограничивать работу служб, которые в рамках своей законной деловой деятельности не осуществляют регулярный сбор и сохранение данных (например, данные о трафике или об абонентах). Не требуется также использование новых технических возможностей для подобных действий, например, для хранения данных, существующих в системе так недолго, что их невозможно сохранить по просьбе или по распоряжению.

154. Законы некоторых стран требуют, чтобы определенные виды данных, например личные сведения, находящиеся у частных держателей, не сохранялись и удалялись при отсутствии долгосрочных служебных оснований для их сохранения. В Евросоюзе применяется общий принцип Директивы 95/46/ЕС, а в контексте телекоммуникационного сектора – Директива 97/66/ЕС. Согласно этим директивам, данные должны быть обязательно удалены, если необходимость в их хранении отпадает. Однако страны-участницы могут принять закон, предусматривающий исключения,

когда это необходимо для предотвращения, расследования или привлечения к уголовной ответственности. Эти директивы не препятствуют странам Евросоюза устанавливать полномочия и процедуры для хранения конкретных данных во время конкретных расследований.

155. Для большинства стран хранение данных – совершенно новый вид полномочий и процедур во внутреннем законодательстве. Это важный инструмент расследования преступлений, совершенных с использованием компьютера, особенно преступлений, совершенных через Интернет. Во-первых, по причине своей эфемерности, компьютерные данные легко подвергаются изменению и воздействию. Следовательно, важные доказательства преступления могут быть легко утеряны из-за небрежного обращения и хранения, в результате намеренных действий, удаления, направленного на уничтожение улик, либо рутинного удаления данных, которые больше не требуют хранения. Один из методов сохранения их целостности, применяемый уполномоченными органами, заключается в обыске или подобном доступе, и конфискации или подобном обеспечении безопасности данных. Однако если обладатель данных заслуживает доверия (например, предприятие с хорошей репутацией), целостность данных можно быстрее обеспечить путем распоряжения о хранении данных. Такое распоряжение может быть менее разрушительным для нормальной деятельности и репутации законного бизнеса, чем обыск и конфискация на его территории. Во-вторых, преступления, совершенные с использованием компьютера, чаще всего совершаются в результате передачи материалов через компьютерную систему. Эти материалы могут иметь

незаконное содержание (например, детская порнография), компьютерные вирусы или иные команды, имеющие негативное воздействие на данные или на нормальную работу системы. Они также могут содержать доказательства совершения других преступлений, таких как наркоторговля или мошенничество. Определение источника или получателя таких информационных материалов может содействовать в установлении личности правонарушителя. Для отслеживания подобного обмена информацией, его источника и получателя, требуются данные о трафике (более подробно важность данных о трафике объясняется в Статье 17). В-третьих, если обмен информацией имеет незаконное содержание или доказательства преступной деятельности, а копии материалов сохраняются провайдерами (например, электронная почта), хранение этих материалов является важным для обеспечения сохранности важных доказательств. Копии таких материалов (например, полученные или отправленные сообщения электронной почты) могут послужить доказательствами совершения преступления.

156. Для решения этих проблем существуют полномочия по оперативному обеспечению сохранности компьютерных данных. От Сторон требуется введение полномочия на выпуск распоряжения о хранении конкретных компьютерных данных в качестве временной меры. Таким образом, данные будут храниться в течение необходимого периода, не превышающего 90 дней. Сторона может впоследствии продлить действие такого распоряжения. Это не означает, что данные раскрываются правоохранительным органам во время хранения. Для этого требуется приказ на применение дополнительной меры по раскрытию данных или

обыск. Правила раскрытия хранимых данных правоохранительным органам описаны в пунктах 152 и 160.

157. Также важно принимать меры по хранению данных на государственном уровне: это позволит Сторонам оказывать друг другу международное содействие, если оперативное обеспечение сохранности данных происходит на их территории. Таким образом, важные данные не будут утеряны во время длительных традиционных процедур юридической взаимопомощи, и запрашиваемая Сторона сможет получить данные и предоставить их запрашивающей Стороне.

Оперативное обеспечение сохранности хранимых компьютерных данных (Статья 16)

158. Статья 16 позволяет уполномоченным органам оперативно обеспечивать сохранность определенных компьютерных данных в связи с конкретным уголовным расследованием или преследованием путем издания распоряжений или иным подобным образом.

159. «Обеспечение сохранности» требует, чтобы данные, которые уже существуют в сохраненной форме, были защищены от воздействий, способных изменить или ухудшить их качество или состояние. Данные следует обезопасить от изменений, деградации или удаления. Обеспечение сохранности не означает, что данные должны быть «заморожены» (т.е. доступ к ним закрыт), и что они или их копии не могут использоваться законными пользователями. В зависимости от конкретных указаний, лицо, которому отдано распоряжение, может иметь доступ к данным. Статья не уточняет способ хранения данных. Каждая Сторона принимает

соответствующие меры по обеспечению сохранности данных и решает, следует ли их «заморозить».

160. Термин «путем выпуска распоряжений или иным подобным образом» позволяет использовать иные законные методы обеспечения сохранности данных, помимо судебного или административного решения (например, распоряжение полиции или прокурора). В некоторых странах распоряжения по обеспечению сохранности в процессуальном законодательстве отсутствуют, и данные могут быть получены только путем обыска и конфискации, либо по судебному приказу. Использование фразы «или иным подобным образом» обеспечивает гибкость, позволяющую странам задействовать данную статью, используя такие средства. Однако странам рекомендуется рассмотреть возможность установления полномочий и процедур, которые обязывают получателя распоряжения обеспечить сохранность данных. В определенных случаях результатом быстрых действий такого лица может быть более оперативное применение мер по обеспечению сохранности.

161. Полномочие на запрос оперативного обеспечения сохранности компьютерных данных касается любых хранимых компьютерных данных. Сюда относятся любые данные, которые в распоряжении указаны как подлежащие хранению. Это могут быть записи делового, медицинского, личного или иного характера. Стороны должны определить меры, используемые «в тех случаях, если есть основания считать компьютерные данные особо уязвимыми для утери или изменения». Это могут быть ситуации, в которых данные хранятся недолго – например, если политикой фирмы является удаление данных по истечении определенного

периода, или данные удаляются обычным путем, если их носитель используется для записи другой информации. Это может касаться также характера обладателя данных, или ненадежного способа их хранения. Однако если обладатель является ненадежным, возможно, более эффективно обеспечить сохранность данных путем обыска и конфискации, а не путем распоряжения, которое может быть проигнорировано. Отдельная ссылка на «данные о трафике» в пункте 1 предупреждает об особом применении положения к этому типу данных. Даже если они собираются и сохраняются провайдером, то обычно лишь на короткое время. Ссылка на «данные о трафике» обеспечивает также связь между мерами, описанными в Статьях 16 и 17.

162. Пункт 2 устанавливает, что в случаях, если Сторона обеспечивает сохранность данных путем выпуска распоряжения, такое распоряжение касается «конкретных хранимых компьютерных данных, находящихся под контролем или во владении указанного лица». Таким образом, хранимые данные могут фактически находиться во владении лица, либо храниться в ином месте, но находиться под контролем этого лица. Лицо, получившее такое распоряжение, обязано «хранить компьютерные данные и обеспечивать их целостность в течение необходимого периода времени, не превышающего 90 дней, чтобы уполномоченные органы могли получить к ним доступ». Внутреннее законодательство Сторон должно определять максимальный период времени, в течение которого данные, указанные в распоряжении, должны храниться. Период времени не должен превышать 90 дней, чтобы позволить уполномоченным органам предпринять другие законные меры, такие как обыск и изъятие, либо подобный доступ

и обеспечение сохранности, либо выпуск судебного приказа для раскрытия данных. Сторона может продлить действие судебного приказа. В данном контексте следует сослаться на Статью 29, которая касается запроса о взаимопомощи для оперативного обеспечения сохранности данных, хранимых с использованием компьютерной системы. Данная статья устанавливает, что сохранение, произведенное по запросу о взаимопомощи, «длится не менее 60 дней, чтобы запрашивающая Сторона могла подать запрос на обыск или подобный доступ, изъятие или подобное обеспечение сохранности, или на раскрытие данных».

163. Согласно пункту 3, обладатель или другое лицо, которому поручено обеспечивать сохранность компьютерных данных, обязан сохранять конфиденциальность этих процедур в течение срока, предусмотренного внутригосударственным правом. В связи с этим Стороны обязаны принять меры по сохранению конфиденциальности и ввести ограниченный срок ее соблюдения. Таким образом, интересы правоохранительных органов (не ставить подозреваемого в известность о расследовании) согласуются с правом человека на частную жизнь. Для правоохранительных органов оперативное обеспечение сохранности данных является частью предварительного расследования, поэтому на данном этапе важна конфиденциальность. Хранение данных – предварительная мера, необходимая до принятия других законных мер по их получению или раскрытию. Конфиденциальность требуется для того, чтобы другие лица не пытались изменить или удалить данные. Существует четкое временное ограничение этой меры для лица, получившего распоряжение, для субъекта данных или для иных лиц,

упомянутых в данных. Двойное обязательство хранить данные в безопасности и сохранять конфиденциальность помогает защитить частную жизнь субъекта данных или иных лиц, упомянутых в данных.

164. Помимо описанных выше ограничений, полномочия и процедуры, описанные в Статье 16, подчиняются условиям и гарантиям, предусмотренным Статьями 14 и 15.

Оперативное обеспечение сохранности и частичное раскрытие данных о трафике (Статья 17)

165. Данная статья устанавливает особые обязательства в отношении хранения данных о трафике согласно Статье 16, и предусматривает оперативное раскрытие некоторых таких данных для того, чтобы определить, были ли другие провайдеры вовлечены в передачу конкретной информации. Определение «данных о трафике» приведено в Статье 1.

166. Получение хранимых данных о трафике, связанных с информационным обменом, может оказаться решающим в определении источника и получателя такого обмена. Это играет ключевую роль при поиске лиц, которые, к примеру, распространяли детскую порнографию либо фальсифицированные данные в рамках мошеннической схемы; лиц, распространявших компьютерные вирусы; лиц, пытавшихся получить или получивших незаконный доступ к компьютерным системам; либо лиц, передававших системе информацию, которая негативно отразилась на данных или нормальной работе системы. Такие данные часто хранятся короткое время, поскольку законы, защищающие частную жизнь, могут запрещать их длительное хранение. Хранение может

также не поощряться рыночной ситуацией. Следовательно, важно предпринять действия по обеспечению целостности таких данных (см. выше дискуссию о хранении).

167. В передаче информации часто участвуют несколько провайдеров. Каждый из них может обладать некоторыми данными о трафике, относящимися к передаче конкретной информации. Такие данные либо создаются и сохраняются провайдером при передаче информации через его систему, либо получены от других провайдеров. Иногда, в коммерческих и технических целях или в целях безопасности, данные о трафике (или некоторые их виды) являются общими для нескольких провайдеров, участвующих в передаче информации. В таких случаях любой из провайдеров может обладать важными данными о трафике, которые нужны для определения источника или получателя обмена информацией. Каждый владеет одним звеном цепи, и каждое из звеньев должно быть проверено, чтобы определить источник или цель.

168. Согласно Статье 17, в случаях, если передача информации осуществляется одним или несколькими провайдерами, оперативное обеспечение сохранности данных о трафике может производиться среди всех провайдеров. Статья не определяет средства такого обеспечения, предоставляя внутреннему законодательству выбор средства в соответствии с правовой и экономической системой. Одним из таких средств является оперативный выпуск уполномоченными органами отдельных распоряжений по сохранению данных для каждого провайдера. Тем не менее, получение отдельных распоряжений может занять слишком много времени. Предпочтительной альтернативой будет

получение единого распоряжения, действие которого распространяется на всех провайдеров, чье участие в передаче информации установлено. Подобное распоряжение широкого охвата может последовательно применяться для каждого установленного провайдера. Другие альтернативы могут включать участие самих провайдеров. К примеру, можно потребовать, чтобы провайдер, получивший распоряжение, уведомил о существовании и условиях распоряжения по хранению данных следующего провайдера в цепочке. В зависимости от внутреннего законодательства, такое уведомление может либо разрешать другим провайдерам добровольно хранить важные данные о трафике, несмотря на любые обязательства по их удалению, либо требовать хранения этих данных. Второй провайдер может таким же образом уведомить следующего провайдера в цепочке.

169. Данные о трафике не раскрываются правоохранительным органам с момента вручения провайдеру распоряжения о хранении данных; доступ к ним или их раскрытие осуществляется позднее, после принятия других законных мер. Таким образом, правоохранительные органы не знают, обладает ли провайдер всеми важными данными о трафике, и вовлечены ли другие провайдеры в цепочку передачи информации. Следовательно, данная статья требует, чтобы провайдер, получивший распоряжение о хранении данных, оперативно раскрыл уполномоченным органам или иному специально назначенному лицу достаточное количество данных о трафике, которое поможет установить других провайдеров и определить маршрут передачи информации. Уполномоченные органы должны четко определить

вид данных о трафике, который требуется раскрыть. Получение такой информации поможет им в принятии мер по хранению данных в отношении других провайдеров. Таким образом, следственные органы могут проследить обмен информацией до его источника или получателя, и установить лицо, совершившее расследуемое преступление. На меры, предусмотренные данной статьей, также распространяются ограничения, условия и гарантии, указанные в Статьях 14 и 15.

Подраздел 3 – Распоряжение о предъявлении данных

Распоряжение о предъявлении данных (Статья 18)

170. В соответствии с пунктом 1 данной статьи, Стороны обеспечивают уполномоченным органам либо возможность обязать лицо, находящееся на их территории, представить конкретные сохраненные компьютерные данные, либо обязать провайдера, предлагающего услуги на их территории, представить сведения об абоненте. Речь идет о хранимых или существующих данных; сюда не входят еще не созданные данные, например, данные о трафике или об информационном наполнении, относящиеся к будущему обмену информацией. Важно, чтобы во внутреннем законодательстве Государств имелись альтернативные возможности обеспечить менее интрузивные средства получения информации по уголовным расследованиям, нежели систематические принудительные меры в отношении третьих сторон (такие как обыск и изъятие данных).

171. «Распоряжение о предъявлении данных» – гибкая мера, которую правоохранительные органы могут

применять во многих случаях, особенно вместо более интрузивных или подавляющих мер. Такой процессуальный механизм будет также полезным для третьих сторон – обладателей данных, к примеру, для Интернет-провайдеров. Они зачастую готовы оказывать добровольное содействие правоохранительным органам, предоставляя подконтрольные им данные, но при этом предпочитают иметь законные основания для такого содействия, освобождающие их от договорной или внедоговорной ответственности.

172. Распоряжение о предъявлении данных касается компьютерных данных или сведений об абонентах, находящихся во владении или под контролем лица или поставщика услуг. Эта мера применяется лишь в том случае, если такие данные или информация имеются у лица или провайдера. К примеру, некоторые провайдеры не ведут учет своих абонентов.

173. Согласно пункту 1(a), Сторона предоставляет правоохранительным органам полномочия отдать находящемуся на ее территории лицу распоряжение о предъявлении конкретных компьютерных данных, хранящихся в компьютерной системе или на носителе, находящемся во владении или под контролем этого лица. Термин «во владении или под контролем» подразумевает физическое владение данными на территории Стороны, выпускающей такое распоряжение. Этот термин также подразумевает ситуации, если данные не находятся в физическом владении лица, однако оно может свободно контролировать их предъявление с территории Стороны, выпускающей такое распоряжение. Например, в соответствии с применяемыми полномочиями, лицо, получившее распоряжение о предъявлении информации, которая

хранится в его учетной на удаленном сервисе хранения, должно предъявить такую информацию. В то же время сама техническая возможность получить удаленный доступ к хранимым данным не обязательно означает «контроль» в понимании данного положения (например, возможность пользователя через сетевую ссылку получить удаленный доступ к данным, не находящимся под его/ее контролем). В некоторых странах понятие, определенное в законе как «владение», достаточно широко распространяется на физическое и подразумеваемое владение, чтобы соответствовать требованию «владения и контроля».

Согласно пункту 1 (b), Сторона также предоставляет полномочия на выпуск распоряжения в отношении провайдера, предлагающего услуги на ее территории. Согласно распоряжению он должен «предоставить сведения об абонентах, находящиеся в его владении или под его контролем». Как и в пункте 1(a), термин «владение или контроль» подразумевает как сведения об абонентах, находящиеся в физическом владении провайдера, так и хранимую удаленно информацию, находящуюся под его контролем (например, на удаленном устройстве хранения данных, предоставляемом другой компанией). Термин «относящийся к подобным услугам» означает, что полномочия действуют в целях получения сведений об абонентах, имеющих отношение к услугам, которые предлагаются на территории Стороны, выпускающей распоряжение.

174. Условия и гарантии в пункте 2 могут исключать конфиденциальные данные или информацию, в зависимости от внутреннего законодательства каждой Стороны. Сторона может назначить иные условия, иные уполномоченные

органы и иные гарантии в отношении предъявления конкретного вида компьютерных данных или сведений об абонентах, хранящихся у конкретных категорий лиц или провайдеров. Например, в отношении некоторых видов данных, таких как общедоступные сведения об абонентах, Сторона сможет позволить правоохранительным органам издать такое распоряжение, хотя иначе потребовался бы судебный приказ. С другой стороны, в некоторых ситуациях Сторона может потребовать, чтобы распоряжение о предъявлении определенного вида данных было выпущено исключительно судебными органами, если это продиктовано гарантиями прав человека. Стороны могут ограничить раскрытие этих данных для правоохранительных целей ситуациями, когда распоряжение о раскрытии выпускается судебными органами. Принцип соразмерности также обеспечивает некоторую гибкость в применении этой меры – например, во многих Государствах он исключает ее применение в делах о незначительных правонарушениях.

175. Стороны могут рассмотреть возможность включения мер, касающихся конфиденциальности. Данное положение не содержит особого определения конфиденциальности. Это призвано сохранить соответствие неэлектронной среде, в которой конфиденциальность обычно не является обязательной для распоряжений о предъявлении данных. Однако в электронной среде, в частности в среде онлайн, распоряжение о предъявлении данных иногда может применяться в качестве предварительной меры расследования, за которой следуют дальнейшие меры, например, обыск и изъятие или перехват данных в реальном времени. Конфиденциальность может оказаться крайне важной для успешного расследования.

176. Что касается условий предъявления, Стороны могут установить требование предъявлять конкретные компьютерные данные или сведения об абонентах в определенной форме, указанной в распоряжении. Может быть указан период, в который данные должны быть предоставлены, либо форма предоставления данных или информации (например, в виде простого текста, в режиме онлайн, на бумажном носителе или дискете).

177. Определение «сведений об абонентах» дано в пункте 3. В принципе оно относится к любой информации, находящейся у администрации провайдера и касающейся его абонента. Сведения об абонентах могут храниться в форме компьютерных данных или любой другой форме, например, на бумаге. Поскольку сведения об абонентах помимо компьютерных включают и другие формы данных, в статью добавлено специальное положение, относящееся к этому виду информации. Термин «абонент» относится к широкому ряду клиентов провайдера, от обладателей платной подписки до тех, кто платит за услуги по факту использования или тех, кто пользуется бесплатными услугами. Он также включает информацию о лицах, имеющих право пользования учетной записью абонента.

178. В процессе уголовного расследования сведения об абонентах в первую очередь требуются в двух специфических ситуациях. Во-первых, эти сведения нужны для установления служб и связанных с ними технических средств, которые использует абонент. Это может быть тип телефонной связи (мобильная), тип связанных с ней услуг (переадресация звонков, голосовая почта, и т.д.), телефонный номер или иной технический адрес (например, адрес

электронной почты). Во-вторых, когда известен технический адрес, сведения об абоненте нужны для установления личности заинтересованного лица. Прочие сведения об абоненте, например, коммерческая информация о выставлении счетов и записи о платежах, может также оказаться значимой для уголовного расследования, особенно в случаях, когда расследуется компьютерное мошенничество или другие экономические преступления.

179. Следовательно, сведения о подписчике включают различные виды информации об использовании услуги и ее пользователе. В отношении использования услуги этот термин означает любую информацию (помимо данных о трафике и об информационном наполнении), с помощью которой можно установить тип используемой коммуникационной услуги, связанное с ней техническое обеспечение, и период, в течение которого лицо было подписано на услугу. Термин «техническое обеспечение» обозначает все средства, дающие абоненту возможность пользоваться предложенной услугой. К ним относится резервирование технического номера или адреса (номер телефона, адрес сайта, имя домена, адрес электронной почты, и т.д.), а также обеспечение и регистрация коммуникационного оборудования, используемого абонентом (телефонные иустройства, телефонные центры или локальные сети LAN).

180. Сведения об абоненте не ограничиваются информацией, напрямую связанной с использованием компьютерных услуг. К ним относится любая информация (помимо данных о трафике и об информационном наполнении), с помощью которой можно установить личность пользователя, его почтовый или географический адрес, номер

телефона или иной номер доступа, а также информация о счетах и платежах, которая доступна на основании пользовательского соглашения или договоренности между абонентом и поставщиком услуг. Сюда также входит любая другая информация (помимо данных о трафике и об информационном наполнении), относящаяся к сайту или месту установки коммуникационного оборудования, и доступная на основании пользовательского соглашения или договоренности. Последний вид информации может оказаться практически важным в тех случаях, когда оборудование нетранспортабельно, а сведения о его транспортабельности или предполагаемом местонахождении (на основании информации, предоставленной в соответствии с пользовательским соглашением) могут быть полезными для расследования.

181. Данную статью не следует понимать как обязывающую провайдеров вести записывать сведения об абонентах, либо убеждаться в достоверности таких сведений. Соответственно, провайдер не обязан регистрировать информацию о личности пользователей так называемых предоплаченных карт мобильной связи. Он также не обязан подтверждать личность абонентов или препятствовать использованию псевдонимов.

182. Поскольку полномочия и процедуры, описанные в данном Разделе, относятся к специфическим уголовным расследованиям и процессуальным действиям (Статья 14), распоряжения о предъявлении данных следует использовать в индивидуальных случаях, обычно касающихся конкретных абонентов. Например, если в распоряжении упомянуто имя, может быть запрошен связанный с ним номер

телефона или адрес электронной почты. На основании такого номера или адреса может быть запрошено имя и адрес абонента. Это положение не дает Сторонам право издавать приказ, требующий раскрытия имеющейся у провайдера широкой информации о группах абонентов, например, в целях извлечения данных.

183. Ссылку на «пользовательское соглашение или договоренность» следует интерпретировать в широком смысле, и понимать под ними любые виды отношений, на основании которых клиент пользуется услугами провайдера.

Подраздел 4 – Обыск и изъятие хранимых компьютерных данных

Обыск и изъятие хранимых компьютерных данных (Статья 19)

184. Цель данной статьи – модернизация и урегулирование внутреннего законодательства по обыску и изъятию хранимых компьютерных данных, которые могут быть использованы для получения доказательств при конкретных уголовных расследованиях и процессуальных действиях. Любое внутреннее уголовно-процессуальное законодательство содержит указания по обыску и изъятию материальных объектов. Однако правоохранительные органы многих стран не считают хранимые компьютерные данные материальными объектами. Следовательно, невозможно обеспечить безопасность таких данных в интересах уголовного расследования тем же способом, что и безопасность материальных объектов. Поэтому единственной мерой остается обеспечение безопасности носителя, на котором хранятся

данные. Целью Статьи 19 является установление равнозначных мер в отношении хранимых данных.

185. Традиционно обыск, имеющий отношение к документам или записям, включает в себя сбор доказательств, которые были записаны ранее в материальной форме, например, при помощи чернил и бумаги. Следователи изучают такие данные и изымают их, т.е. физически забирают материальные записи. Сбор данных происходит во время обыска и касается данных, существующих в этот момент. Предварительное условие для получения законных полномочий на проведение обыска (как это предусматривается внутренним законодательством и гарантиями прав человека) – это обоснованное предположение, что данные, которые могут послужить доказательством уголовного преступления, действительно существуют в определенном месте.

186. На поиск доказательств в новой технологической среде, в частности, компьютерных данных, распространяются многие характеристики традиционного поиска. Например, сбор данных осуществляется во время, отведенное на их поиск, и в отношении данных, существующих в этот момент. Предварительные условия для получения законного права на проведение обыска остаются неизменными. Уровень подозрения, требуемый для получения этого права, не зависит от того, являются ли данные материальными или электронными. Точно так же убежденность и обыск касаются уже существующих данных, которые могут стать доказательством определенного правонарушения.

187. Однако для обыска, связанного с компьютерными данными, требуются дополнительные процессуальные нормы,

обеспечивающие получение данных столь же эффективным способом, как поиск и изъятие материального носителя. На это есть несколько причин. Во-первых, данные имеют нематериальную форму – например, электромагнитную. Во-вторых, хотя данные можно прочесть с помощью компьютерного оборудования, их нельзя изъять в том же смысле, что и бумажные записи. Физический носитель, на котором хранятся нематериальные данные (жесткий диск или дискета), должен быть изъят, либо должна быть сделана материальная копия данных (распечатка) или их нематериальная копия на материальном носителе (дискета), который будет изъят. В последних двух случаях, если делаются копии данных, копия остается в компьютерной системе или на устройстве хранения. Внутреннее законодательство должно предусматривать создание таких копий. В-третьих, из-за возможности подключения компьютерных систем друг к другу, данные могут храниться не на том компьютере, на котором ведется их поиск, но при этом к ним легко получить доступ. Они могут храниться на соединенном с системой устройстве, напрямую подключенном к компьютеру или связанном с ним через коммуникационные системы, например, через Интернет. В этом случае могут потребоваться новые законы, разрешающие расширение поиска с охватом мест, где фактически хранятся данные, или загрузку данных с сайта на компьютер, в котором ведется поиск, или более оперативное и координированное использование традиционных процедур в обоих местах хранения данных.

188. Пункт 1 требует, чтобы Стороны предоставили правоохранительным органам возможность обыска и доступа к компьютерным данным, содержащимся в компьютерной

системе или ее части (например, на соединенном с ней устройстве хранения), или на независимом устройстве хранения данных (компакт-диск или дискета). Поскольку определение «компьютерная система» в Статье 1 обозначает любое устройство или группу взаимосвязанных или смежных устройств, пункт 1 относится к обыску в компьютерной системе и связанных с ней компонентах, которые вместе рассматриваются как единая компьютерная система (например, компьютер с принтером, устройствами хранения или локальной сетью). Иногда к данным, физически хранящимся в другой системе или устройстве, можно получить законный доступ через компьютерную систему, на которой производится обыск, при помощи соединения с другими компьютерными системами. Такая ситуация, включающая связь с другими компьютерными системами через телекоммуникационные сети (региональная сеть или Интернет), рассматривается в пункте 2.

189. Хотя обыск и изъятие «устройства хранения, на котором могут содержаться компьютерные данные» (пункт 1 (b)) может происходить с использованием традиционных законных полномочий, поиск компьютерных данных часто требует обыска как в компьютерной системе, так и в связанных с ней устройствах хранения, находящихся рядом. В этой связи пункт 1 предусматривает широкие законные полномочия, охватывающие обе ситуации.

190. Статья 19 применяется к хранимым компьютерным данным. В этом отношении возникает вопрос: рассматривается ли непрочитанное электронное сообщение, ожидающее в почтовом ящике Интернет-провайдера загрузки в систему пользователя, как хранимые данные или как данные

в процессе передачи. Согласно законам некоторых Сторон, такое сообщение является частью информационного обмена, и его содержимое может быть получено только при наличии полномочий на перехват; другие же правовые системы рассматривают такое сообщение как хранимые данные, к которым применима Статья 19. Следовательно, Стороны должны пересмотреть свои законы в отношении данного вопроса и определить, что является приемлемым в рамках внутреннего законодательства.

191. Упоминается термин «обыск или подобный доступ». Использование традиционного слова «обыск» выражает идею силового применения полномочий страной, и означает, что полномочия, описанные в данной статье, аналогичны традиционному обыску. «Обыскивать» означает искать, читать, изучать или просматривать данные. В этот термин входят понятия поиска данных и их осмотра. С другой стороны, слово «доступ» имеет нейтральное значение, но более точно отражает компьютерную терминологию. Для соединения традиционных понятий с современной терминологией используются оба термина.

192. Ссылка на «нахождение на территории Стороны» напоминает, что данное положение, как и все статьи этого Раздела, касается только мер, принимаемых на уровне страны.

193. Пункт 2 позволяет следственным органам расширять сферу обыска или подобного доступа к другой компьютерной системе или ее части, если у них есть основания полагать, что требуемые данные хранятся в такой системе. Однако эта система или ее часть должны также находиться на территории Стороны.

194. Конвенция не определяет, каким образом должен предприниматься расширенный обыск. Это оставлено на усмотрение внутреннего законодательства. Вот некоторые примеры возможных условий: если есть основания полагать, что связанная компьютерная система может содержать разыскиваемые данные (в степени, требуемой внутренним законодательством и гарантиями прав человека), можно уполномочить судебные или иные органы, санкционировавшие обыск в компьютерной системе, разрешить расширение обыска или иного доступа, чтобы охватить связанную систему; можно уполномочить следственные органы расширить обыск или подобный доступ в конкретной компьютерной системе, до связанной с ней системы, если существуют такие же основания считать, что разыскиваемые данные находятся в этой системе. Можно также произвести координированный и оперативный обыск или подобный доступ в обоих местах. В любом случае к необходим законный доступ к разыскиваемым данным с исходной компьютерной системы.

195. Данная статья не предписывает «трансграничного обыска и изъятия», при котором Стороны могут искать и изымать данные на территории других государств без использования традиционных каналов юридической взаимопомощи. Этот вопрос обсуждается ниже, в Главе о международном сотрудничестве.

196. Пункт 3 касается предоставления компетентным органам полномочий на изъятие или подобное обеспечение сохранности компьютерных данных, в отношении которых производился обыск или подобный доступ, описанный в пунктах 1 или 2. К таким полномочиям относится право на

изъятие деталей компьютера и устройств хранения компьютерных данных. В определенных случаях – например, когда данные хранятся в уникальных операционных системах, которые невозможно скопировать, – неизбежно изъятие всего носителя данных. Это может также потребоваться в случаях, когда носитель требуется изучить для получения старых данных, которые были замещены новыми, но тем не менее оставили следы на носителе.

197. В данной Конвенции «изъять» означает забрать физический носитель, на котором записаны данные или информация, либо сделать и сохранить копии этих данных. «Изъятие» включает в себя использование или изъятие программ, требуемых для доступа к изымаемым данным. Помимо традиционного термина «изъять», используется термин «подобным образом обеспечить сохранность», чтобы отразить другие методы, с помощью которых нематериальные данные перемещаются, становятся недоступными, или возникает иной контроль над ними в компьютерной среде. Поскольку эти методы относятся к нематериальным хранимым данным, от уполномоченных органов требуются дополнительные меры по обеспечению их сохранности. Требуется «сохранить целостность данных», или «поддерживать порядок передачи и хранения» данных, то есть копируемые или перемещаемые данные должны находиться в стране, в которой они были обнаружены в момент изъятия, и оставаться неизменными во время уголовного разбирательства. Это касается получения контроля над данными или их изъятия.

198. Обеспечение недоступности данных может включать в себя их шифрование или иное технологическое предотвращение доступа к ним. Эту меру полезно применять

в ситуациях, когда существует опасность или общественный вред (вирусные программы или инструкции по изготовлению вирусов или бомб), либо когда данные или их содержимое незаконны (детская порнография). Термин «перемещение» означает, что данные не уничтожаются и продолжают существовать, пока их перемещают или обеспечивают их недоступность. Данные на время изымают у подозреваемого, но их можно вернуть по результатам уголовного расследования или процессуальных действий.

199. Таким образом, изъятие или подобное обеспечение сохранности выполняет две функции: 1) собрать доказательства, например, при помощи копирования данных; или 2) конфисковать данные, например, при помощи копирования и последующего блокирования оригинала или его перемещения. Изъятие не подразумевает окончательного удаления конфискованных данных.

200. Пункт 4 вводит силовые меры по обеспечению обыска и изъятия компьютерных данных. Он обращается к практической проблеме трудностей с доступом и выявлением данных, разыскиваемых в качестве доказательств, принимая во внимание большое количество обрабатываемых и хранимых данных, меры компьютерной безопасности и характер компьютерных операций. Данный пункт признает, что может потребоваться консультация системных администраторов, имеющих определенные знания о компьютерных системах, на предмет лучшего способа поиска данных. Следовательно, данное положение позволяет правоохранительным органам привлекать системных администраторов в разумных пределах оказывать содействие в проведении обыска и изъятия данных.

201. Данное полномочие полезно не только следственным органам. Без такого сотрудничества следственные органы могут подолгу оставаться на территории, где производится обыск, и ограничивать доступ к компьютерной системе. Это может оказаться экономическим бременем для законного бизнеса и абонентов, которым в это время отказано в доступе. Возможность привлечения специалистов поможет сделать поиск более эффективным и экономически выгодным для правоохранительных органов и невиновных лиц, которых он затрагивает. Законное требование помощи системного администратора также освобождает его от договорных и иных обязательств по неразглашению данных.

202. Информация, предоставления которой можно потребовать в приказном порядке, должна быть необходимой для проведения обыска или изъятия или подобного доступа и обеспечения сохранности данных. Предоставление такой информации, однако, ограничивается «разумными» пределами. В некоторых обстоятельствах может потребоваться раскрытие правоохранительным органам пароля или иной меры безопасности. В других обстоятельствах это может не быть разумным – например, когда раскрытие пароля или иной меры безопасности неоправданно угрожает частной жизни других пользователей или другим данным, поиск которых не санкционирован. В таких случаях предоставление «необходимой информации» может оказаться раскрытием, в доступной для понимания и прочтения форме, фактических данных, которые разыскиваются уполномоченными органами.

203. Согласно пункту 5 данной статьи, меры подчиняются условиям и гарантиям, предписанным внутренним

законодательством на основании Статьи 15 данной конвенции. Эти условия могут включать в себя положения, относящиеся к привлечению свидетелей и экспертов и к выплате им финансовой компенсации.

204. В рамках пункта 5 составители обсуждали, следует ли уведомлять заинтересованные стороны о проведении процедуры обыска. Обыск и изъятие (копирование) данных в онлайн среде может оказаться менее очевидным, нежели в реальном мире, где изъятые объекты физически отсутствуют. Законы некоторых Сторон не предусматривают обязанность уведомления в случае традиционного обыска. Требование Конвенции производить такое уведомление в отношении компьютерного обыска создало бы противоречие в законодательстве таких Сторон. С другой стороны, некоторые из Сторон могут рассматривать уведомление как неотъемлемую часть данной меры, чтобы разграничить компьютерный поиск хранимых данных (который, как правило, не является тайной мерой), и перехват данных о трафике (который является тайной мерой, см. Статьи 20 и 21). Выпуск уведомления, таким образом, определяется внутренним законодательством. Если Стороны решают уведомлять заинтересованных лиц, следует иметь в виду, что это может нанести ущерб расследованию. Если существует такой риск, стоит рассмотреть возможность отсрочки уведомления.

Подраздел 5 – Сбор компьютерных данных в режиме реального времени

205. Статьи 20 и 21 предусматривают сбор данных о трафике и перехват данных об информационном наполнении в реальном времени, связанные с определенным информационным

обменом в компьютерной системе. Положения описывают сбор и перехват таких данных в реальном времени как уполномоченными органами, так и провайдерами, а также обязательства по сохранению конфиденциальности.

206. Перехват дистанционной передачи данных обычно относится к традиционным телекоммуникационным сетям. Такие сети могут иметь оптическую или кабельную инфраструктуру, а также соединения с беспроводными сетями, включая мобильные телефонные системы и системы микроволновой передачи. Сегодня мобильная связь осуществляется также через систему особых спутниковых сетей. Компьютерные сети могут состоять из независимой фиксированной кабельной инфраструктуры, но чаще работают как виртуальная сеть с соединениями через телекоммуникационные инфраструктуры, что делает возможным создание глобальных компьютерных или связанных между собой сетей. Из-за постепенного сближения телекоммуникационных и информационных технологий стираются различия между дистанционной передачей данных и компьютерным обменом информацией, а также отличительные характеристики их инфраструктур. Таким образом, термин «компьютерная система» в Статье 1 не ограничивает способы взаимосвязи между устройствами или группами устройств. Статьи 20 и 21 применяются к конкретному обмену информацией, осуществленному при помощи компьютерной системы. Это может включать передачу информации по телекоммуникационным сетям, прежде чем она будет получена другой компьютерной системой.

207. Статьи 20 и 21 не делают различий между общественной или частной телекоммуникационной или компьютерной

системой, а также между использованием систем и коммуникационных услуг, предлагаемых публично или лишь закрытым группам пользователей и частным лицам. Определение «поставщика услуг» в Статье 1 относится к публичным и частным организациям, предоставляющим своим пользователям возможность обмениваться информацией при помощи компьютерной системы.

208. Данный подраздел регламентирует сбор доказательств, содержащихся в текущем информационном обмене, и собираемых во время этого обмена (т.е. «в реальном времени»). Данные нематериальны по форме (т.е. содержатся в форме голосовой передачи или электронных импульсов). Поток данных не подвергается значительному вмешательству в процессе сбора, и информация достигает предполагаемого получателя. Вместо физического изъятия передаваемых данных делается их запись (т.е. копия). Сбор таких доказательств происходит в определенный период времени. Для разрешения сбора в отношении будущих событий (т.е. передачи данных в будущем) требуется юридическое основание.

209. Собираемые данные могут быть двух типов: данные о трафике и данные об информационном наполнении. Термин «данные о трафике» определен в Статье 1(d) и обозначает любые компьютерные данные, относящиеся к информационному обмену при помощи компьютерной системы, созданные компьютерной системой, и составляющие часть цепочки информационного обмена, указывая на его происхождение, место назначения, путь, время, дату, размер и длительность, или на вид услуг. Термин «данные об информационном наполнении» не определен в Конвенции, но

относится к содержанию информационного обмена (т.е. к смыслу или сути обмена, либо к передаваемому сообщению или информации, помимо данных о трафике).

210. Во многих странах проводится различие между перехватом в реальном времени данных об информационном наполнении и сбором в реальном времени данных о трафике, как в отношении законных предпосылок для авторизации такого следственного метода, так и в отношении правонарушений, к которым может быть применен этот метод. Признавая, что оба вида данных могут быть связаны с частными интересами, многие страны считают, что частные интересы в отношении данных об информационном наполнении стоят выше из-за характера содержания информационного обмена или характера сообщений. В отношении сбора данных об информационном наполнении могут налагаться более строгие ограничения по сравнению со сбором данных о трафике. Чтобы способствовать признанию этого различия такими странами, Конвенция в заголовках статей называет сбор данных о трафике «сбором в реальном времени», а сбор данных об информационном наполнении «перехватом в реальном времени». Тем не менее, в рабочем порядке признается, что данные могут собираться и записываться в обоих случаях.

211. Существующее законодательство некоторых стран не различает сбор данных о трафике и перехват данных об информационном наполнении. Это происходит либо потому, что в законе не определены различия в плане личных сведений, либо потому, что технические методы сбора в обоих случаях очень похожи. Таким образом, юридические предпосылки для санкционированного применения этих

мер, и правонарушения, в отношении которых эти меры применяются, одинаковы. Конвенция признает эту ситуацию в тексте Статей 20 и 21 общим рабочим употреблением термина «собирать или записывать».

212. Закон часто предписывает, что перехват в реальном времени данных об информационном наполнении применим только в отношении расследования серьезных правонарушений или их категорий. Местное законодательство относит правонарушения к серьезным, если они включены в список или категорию с упоминанием применимого к ним определенного максимального срока тюремного заключения. Следовательно, Статья 21 особо оговаривает, что перехват данных об информационном наполнении должен применяться Сторонами лишь «в отношении ряда серьезных правонарушений, определенных внутренним законодательством».

213. С другой стороны, Статья 20, касающаяся сбора данных о трафике, не так узка и в принципе применима к любому правонарушению, предусмотренному Конвенцией. Однако пункт 3 Статьи 14 предусматривает, что Сторона может сохранить за собой право применять эту меру лишь к правонарушениям или их категориям, указанным в оговорке, при условии, что ряд правонарушений или их категорий не короче ряда правонарушений, к которым применяется перехват данных об информационном наполнении. Тем не менее, если такая оговорка принимается, Сторона должна ограничить ее применение, чтобы обеспечить как можно большую сферу действия меры по сбору данных о трафике.

214. Во многих странах правонарушения, предусмотренные Конвенцией, обычно рассматриваются как недостаточно серьезные для перехвата данных об информационном наполнении или, в некоторых случаях, даже для сбора данных о трафике. Тем не менее, такие методы часто бывают решающими при расследовании предусмотренных Конвенцией правонарушений, например, включающих незаконный доступ к компьютерным системам, распространение вирусов и детской порнографии. Источник вмешательства или распространения в некоторых случаях не может быть установлен без сбора данных о трафике в реальном времени. В некоторых случаях характер информационного обмена не может быть раскрыт без перехвата данных об информационном наполнении в реальном времени. Такие правонарушения по своему характеру или по средствам передачи данных подразумевают использование компьютерных технологий. Следовательно, для их расследования должно допускаться использование технологических средств. Однако из-за сложности вопроса о перехвате данных об информационном наполнении Конвенция оставляет определение сферы применения этой меры на усмотрение внутреннего законодательства. Поскольку некоторые страны юридически приравнивают сбор данных о трафике к перехвату данных об информационном наполнении, допустима оговорка, ограничивающая применение первой меры, однако не в большей степени, нежели ограничение меры по перехвату данных об информационном наполнении. Тем не менее, Стороны должны рассмотреть возможность применения обеих мер к правонарушениям, предусмотренным Конвенцией в Разделе 1 Главы II, для обеспечения эффективных методов

расследования таких правонарушений, связанных с применением компьютера.

215. Условия и гарантии в отношении полномочий и процедур, связанных с перехватом данных об информационном наполнении и сбором данных о трафике, подчиняются Статьям 14 и 15. Поскольку перехват данных об информационном содержании является весьма интрузивной мерой по отношению к частной жизни, требуются серьезные гарантии для обеспечения соответствующего равновесия между интересами правосудия и основными правами человека. В области перехвата сама Конвенция не предусматривает конкретных гарантий, за исключением ограничения санкций на перехват данных расследованиями серьезных уголовных преступлений, как это определено во внутреннем законодательстве. Тем не менее, важными условиями и гарантиями, применяемыми в этой сфере внутренним законодательством, являются: юридический или иной независимый надзор; специфика лиц или информационного обмена, подлежащего перехвату; принцип необходимости, подчиненности и соразмерности (например, существуют юридические предпосылки, оправдывающие принятие меры; другие, менее интрузивные меры, неэффективны); ограничение длительности перехвата; право на компенсацию. Многие из этих гарантий отражены в Европейской Конвенции о Правах человека и ее последующей правоприменительной практике (см. решения суда по делам Klass[5], Kruslin[6],

5. Постановление ЕСПЧ по делу «Класс и др. против Германии», A28, 06/09/1978

6. Постановление ЕСПЧ по делу «Крюстен против Франции», 176-A, 24/04/1990

Huvig[7], Malone[8], Halford[9] y Lambert[10]). Некоторые из этих гарантий применимы также к сбору данных о трафике.

Сбор данных о трафике в реальном времени (Статья 20)

216. Часто данные за прошедшие периоды могут быть недоступны или потерять свою важность, поскольку нарушитель изменил путь информационного обмена. Следовательно, сбор данных о трафике в реальном времени является важной следственной процедурой. Статья 20 касается сбора и записи данных о трафике в реальном времени в целях особых уголовных расследований или процессуальных действий.

217. Традиционно сбор данных о потоках информации в отношении телекоммуникаций (например, телефонных разговоров) является полезным следственным инструментом для определения отправителя или получателя информации (например, телефонных номеров); относящихся к ним данных (например, времени, даты и длительности); различных видов незаконного информационного обмена (преступных угроз и домогательств, преступного сговора, введения в заблуждение в мошеннических целях); а также информационного обмена, представляющего собой доказательства

7. Постановление ЕСПЧ по делу «Хьювиг против Франции», 176-B, 24/04/1990

8. Постановление ЕСПЧ по делу «Мелон против Соединенного Королевства», A82, 02/08/1984

9. Постановление ЕСПЧ по делу «Хальфорд против Соединенного Королевства», доклады 1997 – III, 25/06/1997

10. Постановление ЕСПЧ по делу «Ламбер против Франции», доклады 1998 – V, 24/08/1998

прошлых или будущих преступлений (наркоторговля, убийство, экономические преступления, и т.д.).

218. Компьютерный обмен информацией может содержать в себе или представлять доказательства тех же видов преступной деятельности. Однако способность компьютерных технологий передавать большое количество данных, включая текст, визуальные образы и звук, предоставляет большие возможности для совершения преступлений, связанных с распространением материалов незаконного содержания (например, детской порнографии). Поскольку компьютеры могут хранить большие объемы данных, часто личного характера, потенциальный экономический, социальный или личный вред может быть весьма велик, если целостность этих данных нарушена. Кроме того, компьютерные технологии основаны на обработке данных, как в виде конечного продукта, так и части рабочих функций (например, использование компьютерных программ), поэтому любое вмешательство в эти данные может иметь катастрофические последствия для нормальной работы компьютерной системы. Когда происходит незаконное распространение детской порнографии, незаконный доступ к компьютерной системе, нарушение нормальной работы системы или целостности данных, особенно дистанционно (например, через Интернет), крайне важно отследить путь информационного обмена от жертвы к правонарушителю. Следовательно, возможность собирать данные о трафике при компьютерном обмене информации не меньше (если не больше) важна, чем в обычных телекоммуникациях. Этот следственный метод может установить соотношение времени, даты, источника и назначения информации,

передаваемой подозреваемым, со временем вмешательства в системы жертв, а также установить другие жертвы или показать связи между сообщниками.

219. Согласно этой статье, данные о трафике должны быть связаны с конкретными информационными транзакциями на территории Стороны. «Транзакции» указаны во множественном числе, поскольку может потребоваться сбор данных о трафике в отношении нескольких взаимодействий, чтобы определить отправителя или получателя. Например, в доме, где несколько разных людей пользуются одним и тем же телекоммуникационным оборудованием, может потребоваться обнаружить несколько взаимодействий для того, чтобы соотнести их с возможностью людей пользоваться компьютерной системой. Однако информационный обмен, при котором могут собираться и записываться данные о трафике, должен быть конкретным. Таким образом, Конвенция не требует и не санкционирует всеобщий и неизбирательный надзор и сбор большого количества данных о трафике. Она не санкционирует «предварительный сбор фактов», когда предпринимаются попытки обнаружить преступную деятельность, в противоположность конкретным эпизодам расследования такой деятельности. Судебный или иной приказ, санкционирующий сбор данных, должен указать, в отношении какого информационного обмена производится сбор данных о трафике.

220. Согласно пункту 2, Стороны обязаны в соответствии с пунктом 1 (a) обеспечить своим уполномоченным органам возможность сбора или записи данных о трафике при помощи технических средств. Статья не указывает конкретных технических методов сбора и не определяет обязательств в отношении этих методов.

221. Кроме того, согласно пункту (b), Стороны должны предоставить своим уполномоченным органам возможность обязать провайдера производить сбор и запись данных о трафике или оказывать помощь и содействие уполномоченным органам в сборе и записи этих данных. Провайдер обязан производить сбор или запись, а также помощь и содействие только в пределах его технических возможностей. Статья не обязывает провайдеров обеспечивать технические возможности для сбора и записи данных, помощи и содействия в этих процедурах. Они не обязаны приобретать или разрабатывать новое оборудование, привлекать помощь экспертов или заниматься дорогостоящим переоборудованием своих систем. Однако если их системы и персонал имеют возможность обеспечить сбор, запись, помощь и сотрудничество, статья требует, чтобы они приняли необходимые для этого меры. Например, настройки системы или имеющиеся во владении провайдера программы могут позволить принять подобные меры, но обычно они не используются в процессе обычной работы. Статья требует, чтобы провайдер задействовал или включил эти возможности в соответствии с законом.

222. Поскольку данная мера применяется на государственном уровне, сбор и запись конкретного информационного обмена производится на территории Стороны. Таким образом на практике обязательства применяются в случаях, когда провайдер располагает инфраструктурой или оборудованием на этой территории, дающими возможность принять данные меры, хотя это не обязательно должно быть место расположения основной деятельности или органов управления. В целях соблюдения Конвенции считается, что

информационный обмен произошел на территории Стороны, если одна из сторон обмена (люди или компьютеры) находится на ее территории, или если там находится компьютерное или телекоммуникационное оборудование, через которое производился обмен.

223. Как правило, две возможности сбора данных о трафике в пункте 1(a) и (b) не являются альтернативами. За исключением предписаний пункта 2, Сторона должна обеспечить применение обеих мер. Это необходимо, поскольку если провайдер не имеет технической возможности для сбора или записи данных о трафике (1(b)), Сторона должна предоставить правоохранительным органам возможность выполнить эту задачу самостоятельно (1(a)). Таким же образом, в соответствии с пунктом 1(b)(II), обязательство оказывать уполномоченным органам помощь и содействие в сборе и записи данных о трафике не имеет смысла, если эти органы не уполномочены собирать и записывать данные самостоятельно. Кроме того, в ситуациях с некоторыми локальными сетями (LAN), единственный способ произвести сбор и запись данных без участия провайдера – это предоставить выполнение задачи самим следственным органам. Обе меры в пункте 1 (a) и (b) не обязательно использовать каждый раз, но статья требует обеспечить возможность применения обоих методов.

224. Это двойное обязательство создало трудности для некоторых стран, в которых правоохранительные органы могли перехватывать данные в телекоммуникационных системах лишь с помощью поставщика услуг, либо негласно, без его ведома. Пункт 2 регулирует такую ситуацию. В случаях, когда Сторона из-за «принципов, установленных

внутренней правовой системой», не может применять меры, упомянутые в пункте 1 (a), она может использовать другой подход – например, обязать провайдеров предоставить необходимое техническое оборудование для обеспечения сбора данных о трафике правоохранительными органами. В таком случае применяются все остальные ограничения в отношении территории, специфики информационного обмена и использования технических средств.

225. Как и перехват данных об информационном наполнении, сбор данных о трафике эффективен только в случаях, если он предпринимается без ведома лиц, в отношении которых ведется следствие. Перехват является негласным и должен происходить так, чтобы стороны, осуществляющие информационный обмен, не знали о его проведении. Провайдеры и их сотрудники, знающие о перехвате, должны соблюдать секретность, чтобы принятые меры были эффективными.

226. Пункт 3 обязывает Стороны принимать юридические или иные меры, обязывающие провайдера сохранять в тайне действия по сбору данных о трафике. Это положение не только обеспечивает конфиденциальность расследования, но и освобождает провайдера от любых договорных или иных обязательств уведомлять абонентов о сборе их данных. Пункт 3 может быть исполнен путем создания четких обязательств в законе. С другой стороны, Сторона может обеспечить конфиденциальность мер на основании других положений внутреннего законодательства, таких как уголовное преследование за препятствование правосудию тех лиц, которые сообщают преступникам об этих мерах. Хотя особое требование конфиденциальности (с эффективными санкциями в случае утечки информации) является

предпочтительной процедурой, преследование за препятствование правосудию может быть альтернативным способом предотвратить неуместное раскрытие информации и, следовательно, его достаточно для применения этого пункта. В случаях, когда существует четкое обязательство по соблюдению конфиденциальности, оно должно подчиняться условиям и гарантиям, предусмотренным в Статьях 14 и 15. Эти условия и гарантии должны устанавливать разумный период времени для действия обязательств, с учетом негласного характера этой следственной меры.

227. Как указано выше, частные интересы обычно считаются менее значимыми в отношении сбора данных о трафике, нежели в отношении перехвата данных об информационном наполнении. Данные о трафике, касающиеся времени, длительности и размеров информационного обмена раскрывают мало личных сведений о лице или его/ее мыслях. Однако может существовать более серьезная проблема нарушения частных интересов при сборе данных об источнике или получателе информационного обмена (например, посещенные веб-сайты). В некоторых случаях сбор таких данных может подразумевать составление сведений об интересах лица, его помощниках и социальной среде. Стороны должны иметь это в виду, устанавливая соответствующие гарантии и юридические предпосылки для принятия подобных мер в соответствии со Статьями 14 и 15.

Перехват данных об информационном наполнении (Статья 21)

228. Как правило, сбор данных об информационном наполнении в отношении телекоммуникаций (например,

телефонных разговоров) является полезным следственным инструментом для определения незаконного характера общения (преступная угроза, домогательство, преступный сговор или введение в заблуждение в мошеннических целях) и для сбора доказательств прошлых или будущих преступлений (наркоторговля, убийство, экономические преступления, и т.д.). Компьютерный обмен информацией может содержать или представлять доказательства таких видов преступной деятельности. Поскольку компьютерные технологии позволяют передавать большое количество данных, включая текст, визуальные образы и звук, они предоставляют большие возможности для совершения преступлений, связанных с распространением материалов незаконного содержания (например, детской порнографии). Частью многих компьютерных преступлений является передача или обмен данными – например, информация, отправленная для получения незаконного доступа к компьютерной системе, или распространение компьютерных вирусов. Без перехвата содержимого такого сообщения невозможно в реальном времени определить пагубный и незаконный характер подобного информационного обмена. Не имея возможности определять и предотвращать преступную деятельность в ее процессе, правоохранительным органам оставалось бы лишь расследовать прошлые и уже совершенные преступления, вред от которых уже нанесен. Следовательно, перехват данных об информационном наполнении в реальном времени важен не меньше, если не больше, чем перехват телекоммуникационного общения.

229. Термин «данные об информационном наполнении» обозначает содержимое информационного обмена, т.е. его

смысл и суть, или сообщение и информацию, передаваемую таким обменом. Это любая передаваемая часть информационного обмена, за исключением данных о трафике.

230. Большинство элементов данной статьи идентичны элементам Статьи 20. Следовательно, приведенные выше комментарии к сбору и записи данных о трафике, к обязательствам оказывать помощь и содействие, и обязательствам соблюдать конфиденциальность, в равной степени применяются к перехвату данных об информационном наполнении. Поскольку частные интересы, связанные с информационным наполнением имеют приоритет, следственная мера ограничена «рядом серьезных правонарушений, определяемых внутренним законодательством».

231. Кроме того, как описано в комментариях к статье 20, условия и гарантии, применяемые к перехвату данных об информационном наполнении, могут быть более строгими, нежели те, что применяются к сбору данных о трафике, или к обыску и изъятию или подобному доступу и обеспечению сохранности хранимых компьютерных данных.

Часть 3 – Юрисдикция

Юрисдикция (Статья 22)

232. Данная Статья предусматривает ряд критериев, согласно которым Договаривающиеся Стороны должны устанавливать юрисдикцию в отношении правонарушений, перечисленных в Статьях 2–11 Конвенции.

233. Пункт 1 (a) основывается на принципе территориальности. Каждая Сторона должна наказывать за преступления,

предусмотренные данной Конвенцией и совершенные на ее территории. Например, Сторона устанавливает территориальную юрисдикцию, если и лицо, совершившее атаку на компьютерную систему, и подвергшаяся атаке система находятся на ее территории, а также в случае, если на ее территории находится атакованная компьютерная система, но не лицо, совершившее атаку.

234. Рассматривалось включение положения, требующего от каждой из Сторон установления юрисдикции в отношении правонарушений, включающих в себя спутники, зарегистрированные на имя Стороны. Составители решили, что такое положение не является необходимым, поскольку незаконный информационный обмен с использованием спутников неизбежно имеет источник и место назначения на земле. Таким образом, будет доступно одно из оснований, описанных в пунктах 1(a) – (c), для установления Стороной юрисдикции, если передача данных начинается или заканчивается в одном из указанных мест. В случаях, когда правонарушение с использованием спутниковой связи совершается гражданином Стороны за пределами территориальной юрисдикции любой страны, процессуальная основа соответствует пункту 1(d). Составители задавались вопросом, является ли регистрация основанием для установления уголовной юрисдикции, поскольку во многих случаях не существует значимой связи между совершенным правонарушением и страной регистрации, поскольку спутник служит лишь средством передачи данных.

235. Пункты 1(b) и (c) основываются на одном из вариантов принципа территориальности. Эти подпункты требуют,

чтобы каждая из Сторон устанавливала уголовную юрисдикцию в отношении правонарушений, совершенных на борту судна, действующего под ее флагом, или на борту самолета, зарегистрированного по ее законам. В большинстве случаев в законах многих стран уже применяется это обязательство, так как корабли и воздушные судна часто считаются продолжением территории страны. Этот вид юрисдикции наиболее полезен в случаях, когда корабль или воздушное судно не находится на территории Стороны в момент совершения преступления, в результате чего Пункт 1 (a) не может служить основанием для установления юрисдикции. Если преступление совершено на корабле или воздушном судне, находящемся за пределами территории Стороны регистрации, ни одна другая страна не сможет установить свою юрисдикцию в соответствии с данным требованием. Кроме того, если преступление совершено на борту корабля или воздушного судна, проходящего через водное или воздушное пространство другой страны, последняя может столкнуться с серьезными практическими препятствиями в установлении своей юрисдикции, поэтому стране регистрации полезно также иметь юрисдикцию.

236. Пункт 1 (d) основывается на принципе национальной принадлежности. Этот мотив наиболее часто используется странами, применяющими традицию гражданского законодательства. Она предписывает гражданам страны соблюдать внутреннее законодательство, даже если они находятся за пределами ее территории. Согласно подпункту d, если гражданин совершает преступление за границей, Сторона обязана иметь возможность наказать его,

если деяние является правонарушением по законам государства, в котором оно было совершено, или если оно произошло за пределами территориальной юрисдикции каких-либо стран.

237. Пункт 2 позволяет Сторонам внести оговорку в отношении оснований для юрисдикции, изложенных в пункте 1 (b), (c) и (d). Однако оговорки не допускаются в отношении установления территориальной юрисдикции согласно подпункту (a), или в отношении обязательства устанавливать юрисдикцию в случаях, подпадающих под принцип «выдать или наказать» согласно пункту 3, т.е. когда Сторона отказывается выдать предполагаемого правонарушителя на основании его национальной принадлежности, и он находится на ее территории. Юрисдикция, установленная на основании пункта 3, необходима для того, чтобы Стороны, которые отказываются выдавать гражданина, имели законную возможность провести расследование и процессуальные действия на своей территории, если этого требует Сторона, запрашивающая выдачу согласно требованиям пункта 6 Статьи 24 данной Конвенции.

238. Основания для установления юрисдикции, указанные в пункте 1, не являются исключительными. Пункт 4 данной Статьи позволяет Сторонам устанавливать другие виды уголовной юрисдикции в соответствии со своим внутренним законодательством.

239. При совершении преступлений с использованием компьютерных систем бывают случаи, когда несколько Сторон имеют юрисдикцию в отношении всех или некоторых правонарушителей. Например, многие вирусные атаки, случаи

мошенничества и нарушения авторского права, совершенные с использованием Интернета, направлены на жертв, находящихся во многих странах. Чтобы избежать дублирования усилий, создания лишних неудобств для свидетелей, или конкуренции между представителями правоохранительных органов заинтересованных стран, а также для того, чтобы иным образом способствовать эффективности и справедливости процессуальных действий, затронутые Стороны должны провести консультации и определить надлежащее место для судебного преследования. В некоторых случаях наиболее эффективным для заинтересованных стран будет выбор единого места. В других случаях может оказаться наилучшим преследование некоторых участников одной страной, в то время как другая/другие страны преследуют остальных. Согласно данному пункту, разрешены оба варианта. Обязательство проводить консультации не является абсолютным, но должно происходить «в случае необходимости». Таким образом, если одна из Сторон знает, что консультация не является необходимостью (например, она получила подтверждение того, что другая Сторона не планирует предпринимать действия), или если Сторона считает, что консультация может повредить следствию или процессуальным действиям, она может отложить или отклонить консультацию.

Глава III – Международное сотрудничество

240. Глава III содержит положения, относящиеся к выдаче преступников и юридической взаимопомощи между Сторонами.

Часть 1 – Общие принципы

Подраздел 1 – Общие принципы международного сотрудничества

Общие принципы международного сотрудничества (Статья 23)

241. Статья 23 устанавливает три общих принципа в отношении международного сотрудничества согласно Главе III.

242. Сначала статья разъясняет, что международное сотрудничество должно осуществляться Сторонами «максимально широко». Этот принцип требует от Сторон обеспечить широкое сотрудничество друг с другом и минимизировать препятствия быстрой и бесперебойной передаче информации и доказательств между государствами.

243. Далее в Статье 23 устанавливается общая сфера обязательств по сотрудничеству. Сотрудничество должно распространяться на все уголовные правонарушения, относящиеся к компьютерным системам и данным (т.е. к правонарушениям, предусмотренным пунктом 14 a-b Статьи 14), а также на сбор доказательств уголовных правонарушений в электронной форме. Это означает, что положения Главы III применяются в случаях, когда преступление совершено с использованием компьютерной системы, а также если не связанное с использованием компьютера преступление (например, убийство) имеет доказательства в электронной форме. Однако следует заметить, что Статьи 24 (Выдача преступников), 33 (Взаимопомощь в отношении сбора данных о трафике в реальном времени) и 34 (Взаимопомощь в отношении перехвата данных об информационном наполнении) позволяют Сторонам предусмотреть иную сферу применения этих мер.

244. Сотрудничество должно происходить «в соответствии с положениями данной Главы» и «с помощью применения соответствующих международных соглашений по международному сотрудничеству в уголовных вопросах, договоренностей, достигнутых на основании единообразного или двустороннего законодательства, и внутреннего законодательства». Последняя часть устанавливает, что положения Главы III не замещают положения международных соглашений по юридической взаимопомощи и выдаче преступников, двусторонних договоренностей между сторонами (описанных более детально в обсуждении Статьи 27 ниже), или соответствующие положения внутреннего законодательства, относящиеся к международному сотрудничеству. Этот основополагающий принцип четко закреплен в Статьях 24 (Выдача преступников), 25 (Общие принципы взаимопомощи), 26 (Внеплановая информация), 27 (Процедуры направления запросов о взаимопомощи в отсутствие применимых международных соглашений), 28 (Конфиденциальность и ограничения на использование информации), 31 (Взаимопомощь в отношении доступа к хранимым электронным данным), 33 (Взаимопомощь в отношении сбора данных о трафике в реальном времени) и 34 (Взаимопомощь в отношении перехвата данных об информационном наполнении).

Подраздел 2 – Принципы в отношении выдачи преступников

Выдача преступников (Статья 24)

245. Пункт 1 указывает, что обязательство по выдаче применяется только в отношении правонарушений,

предусмотренных Статьями 2–11 настоящей Конвенции, наказуемых по законам обеих Сторон лишением свободы на срок не менее одного года или более серьезным взысканием. Составители решили ввести порог наказания, поскольку, согласно Конвенции, Стороны могут наказывать некоторые правонарушения относительно коротким сроком заключения (например, Статья 2 – незаконный доступ и Статья 4 – вмешательство в данные). Принимая это во внимание, составители не сочли уместным требовать, чтобы каждое из предусмотренных Статьями 2–11 правонарушений рассматривалось как основание для выдачи. Было достигнуто соглашение о том, чтобы считать правонарушение поводом для выдачи, если – как в Статье 2 Европейской Конвенции об экстрадиции (ETS № 24) – максимальной формой наказания за правонарушение, в отношении которого запрошена выдача, является тюремное заключение сроком не менее одного года. Определение того, является ли правонарушение основанием для выдачи, зависит не от фактического наказания, примененного в конкретном случае, а от максимального срока, предусмотренного для правонарушения, по поводу которого запрошена выдача.

246. В то же время, в соответствии с общим принципом, согласно которому на основании действующих между Сторонами документов (см. Главу III) осуществляется международное сотрудничество, пункт 1 также предусматривает следующие меры. В случае если между Сторонами действует договор о выдаче или иное соглашение на основании единообразного или двустороннего законодательства (см. описание этого термина в обсуждении Статьи 27 ниже), и если оно предусматривает иное пороговое наказание для выдачи,

применяется тот порог, который предусмотрен таким договором или соглашением. Например, многие договоры о выдаче между европейскими странами предусматривают, что правонарушение подразумевает выдачу только в том случае, когда максимально возможное наказание превышает тюремное заключение сроком на один год, или когда существует более суровое наказание. В таких случаях специалисты будут применять обычный порог, предусмотренный практикой договора, чтобы определить, предусматривает ли правонарушение выдачу. Даже согласно Европейской Конвенции о выдаче (ETS № 24), оговорки могут определять иное минимальное наказание для выдачи. Если среди Сторон, подписавших Конвенцию ETS № 24, запрос на выдачу поступает от той Стороны, которая ввела подобную оговорку, то наказание, предусмотренное оговоркой, применяется при решении вопроса, является ли правонарушение основанием для выдачи.

247. Пункт 2 предписывает, чтобы правонарушения, описанные в пункте 1, считались имеющими основание для выдачи нарушителя в любом договоре о выдаче между Сторонами, и включались в будущие договоры, которые они могут заключить между собой. Это не означает, что выдача должна производиться при каждом запросе; скорее, должна существовать возможность выдачи лиц, совершивших такие правонарушения. Согласно пункту 5, Стороны могут предусмотреть другие требования для выдачи.

248. Согласно пункту 3, Сторона, отказывающая в выдаче по причине отсутствия договора о выдаче с запрашивающей Стороной или в связи с тем, что существующие договоры не предусматривают этого в отношении правонарушений,

установленных в Конвенции, может использовать саму Конвенцию как основание для выдачи запрошенного лица, хотя и не обязана этого делать.

249. В случае если Сторона не полагается на договоры о выдаче и использует обычную предусмотренную законом схему, пункт 4 требует включать правонарушения, описанные в пункте 1, в список тех, для которых возможна выдача.

250. Пункт 5 устанавливает, что запрашиваемой Стороне не нужно производить выдачу, если она не удовлетворена выполнением всех сроков и условий, предусмотренных применяемым договором или законом. Это еще один пример того, что сотрудничество должно осуществляться в соответствии с условиями международных документов, действующих между сторонами, двусторонних соглашений, или внутреннего законодательства. Например, условия и ограничения, изложенные в Европейской Конвенции о выдаче (ETS № 24) и ее Дополнительных Протоколах (ETS № 86 и №98) применяются к Сторонам этих соглашений, и в выдаче может быть отказано на этих основаниях. Например, Статья 3 Европейской конвенции о выдаче предусматривает отказ в выдаче, если правонарушение считается политическим, или если запрос о выдаче считается произведенной в целях преследования или наказания лиц, в том числе по причине его расовой, религиозной, национальной принадлежности или политических взглядов.

251. Пункт 6 применяет принцип «выдать или наказать». Поскольку многие страны отказываются выдавать своих граждан, правонарушители, находящиеся на территории Стороны, гражданами которой они являются, могут

избежать ответственности за совершенное на территории другой Стороны правонарушение, если местные власти не примут меры. Согласно пункту 6, если другая Сторона запросила выдачу правонарушителя, и в выдаче было отказано на основании того, что правонарушитель является гражданином запрашиваемой Стороны, то запрашиваемая Сторона должна по просьбе запрашивающей Стороны передать дело своим уполномоченным органам. Если Сторона получила отказ на запрос о выдаче, и не просит передать дело местным следственным органам, запрашиваемая Сторона не обязана предпринимать никаких действий. Более того, если не был подан запрос о выдаче, или в выдаче было отказано по другим причинам, кроме гражданства, этот пункт не обязывает запрашиваемую Сторону передавать дело для местного уголовного преследования. Кроме того, пункт 6 требует, чтобы следствие и уголовное преследование на местном уровне производились тщательно. Стороне, передающей дело на рассмотрение, следует относиться к этому так же серьезно, «как в случае любого другого правонарушения сопоставимого характера». Сторона должна сообщить о результатах расследования и процессуальных действий запрашивающей Стороне.

252. Для того, чтобы каждая Сторона знала, кому следует направлять запросы о временном задержании или выдаче, пункт 7 требует, чтобы Стороны сообщили Генеральному Секретарю Совета Европы наименование и адрес их органов, ответственных за направление и получение запросов на выдачу или временное задержание в отсутствие договора. Данное положение ограничено ситуациями, когда между заинтересованными Сторонами нет действующего

договора о выдаче, поскольку если между Сторонами существует двусторонний или многосторонний договор о выдаче (такой как ETS № 24), Стороны знают, кому следует направлять запросы на выдачу или временное задержание, без необходимости их регистрировать. Сведения должны быть переданы Генеральному Секретарю в момент подписания или сдачи документа о ратификации, принятии, одобрении или присоединении. Следует заметить, что назначение уполномоченного органа не исключает возможности использования дипломатических каналов.

Подраздел 3 – Общие принципы взаимопомощи

Общие принципы взаимопомощи (Статья 25)

253. Общие принципы, определяющие обязательство оказывать взаимную помощь, изложены в пункте 1. Взаимопомощь должна быть «максимально широкой». Как и в Статье 23 («Общие принципы международного сотрудничества»), взаимопомощь должна быть всесторонней, а препятствия ей – строго ограниченными. Кроме того, как и в статье 23, обязательство о сотрудничестве применяется как к правонарушениям, связанным с компьютерными системами и данными (т.е. к правонарушениям, предусмотренным пунктом 2 a-b Статьи 14), так и к сбору доказательств уголовного преступления в электронной форме. Была достигнута договоренность относительно сотрудничества в области этой широкой категории преступлений, поскольку существует общая потребность в отлаженном механизме международного сотрудничества по обеим

категориям. Однако Статьи 34 и 35 позволяют Сторонам предусматривать иную сферу применения этих мер.

254. Другие положения данной Главы разъясняют, что обязательство предоставлять взаимную помощь, как правило, действует согласно условиям применяемых договоров, законов и соглашений о юридической взаимопомощи. В соответствии с пунктом 2, каждая Сторона должна иметь юридические основания для применения особых форм сотрудничества, описанных в остальной части Главы, если ее договоры, законы и соглашения не содержат таких положений. Доступность таких механизмов, особенно описанных в Статьях 25 – 35 (Особые положения – Подразделы 1, 2, 3) очень важна для эффективного сотрудничества в уголовных делах, связанных с применением компьютера.

255. Некоторые Стороны не требуют имплементирующего законодательства для применения положений, указанных в пункте 2, поскольку положения международных договоров, предусматривающие всесторонние режимы взаимопомощи, сами по себе обладают исполнительной силой. Предполагается, что Стороны могут использовать эти положения как обладающие исполнительной силой; что они имеют достаточную гибкость, чтобы применять меры, указанные в данной Главе; либо что они могут быстро задействовать для этого любое требуемое законодательство.

256. Компьютерные данные крайне нестабильны. Несколько нажатий на клавиши или некоторые программы могут уничтожить их, сделав невозможным установление правонарушителя или уничтожив ключевые доказательства вины. Некоторые формы компьютерных данных хранятся

лишь в течение короткого периода времени, а затем удаляются. В других случаях может быть нанесен значительный ущерб людям или собственности, если доказательства не собраны оперативно. В таких срочных случаях не только запрос, но и ответ на него должны производиться оперативно. Целью пункта 3 является ускорение процесса взаимопомощи, чтобы важная информация или улики не были утеряны и удалены до того, как запрос о помощи подготовлен и передан, и до получения ответа. Пункт 3 обеспечивает это, (1) давая Сторонам полномочия подавать срочный запрос о сотрудничестве через оперативные каналы связи, а не путем традиционной, гораздо более медленной передачи письменных запечатанных документов через дипломатические пакеты или почтовые службы, и (2) требуя от запрашиваемой Стороны использования оперативных средств для ответа на запрос в таких обстоятельствах. Каждая Сторона должна иметь возможность применять эту меру, если ее договоры, законы или соглашения о взаимопомощи не предусматривают этого. Показательным является указание факса и электронной почты; согласно обстоятельствам могут использоваться любые другие оперативные средства связи. По мере развития технологии появятся другие оперативные средства связи, которые могут быть использованы для запроса о взаимопомощи. Что касается аутентичности и безопасности по данному пункту, Стороны могут сами решать, как обеспечить аутентичность обмена информацией, и существует ли необходимость особой защиты безопасности (включая шифрование), которая может потребоваться в делах государственной важности. Наконец, данный пункт позволяет Сторонам

потребовать официального подтверждения, отправленного по традиционным каналам после оперативной передачи.

257. Пункт 4 устанавливает, что взаимопомощь подчиняется применимым договорам о взаимопомощи и внутреннему законодательству. Эти режимы обеспечивают гарантии прав лиц, находящихся на территории запрашиваемой Стороны, которые могут стать субъектом просьбы о взаимопомощи. Например, такие интрузивные меры, как обыск и изъятие, не применяются в интересах запрашивающей Стороны, если удовлетворены основные требования запрашиваемой Стороны по применению такой меры во внутреннем деле. Стороны могут также обеспечить защиту прав лиц в отношении изъятых объектов, предусмотренную юридической взаимопомощью.

258. Однако пункт 4 не применяется, «если иное не предусмотрено данной Главой». Эта фраза предупреждает о том, что в Конвенции имеется несколько исключений из общего принципа. Первое исключение описано в пункте 2 данной Статьи, обязывающем каждую Сторону предусмотреть формы сотрудничества, указанные в остальной части Главы (такие как хранение, сбор в реальном времени, обыск и изъятие данных и поддержка круглосуточной работы сети), независимо от того, предусмотрены ли эти меры ее текущими соглашениями об оказании взаимной юридической помощи, или другими подобными соглашениями и законами о взаимопомощи. Второе исключение находится в Статье 27, которая всегда применяется вместо внутреннего законодательства запрашиваемой Стороны, регулирующего международное сотрудничество в отсутствие соглашения об оказании взаимной юридической помощи или другого подобного соглашения. Статья 27

предусматривает систему условий и оснований для отказа. Еще одно исключение, особо предусмотренное данным пунктом, заключается в том, что в сотрудничестве не может быть отказано, по крайней мере, в отношении правонарушений, установленных в Статьях 2–11, на основании того, что по мнению запрашиваемой Стороны запрос включает «нарушение налоговых правил». Статья 29 является исключением, поскольку предусматривает, что в сохранении данных нельзя отказать на основании правила о двойной подсудности, хотя в этом отношении и существует возможность оговорки.

259. Пункт 5 является, по сути, определением двойной подсудности для целей взаимной помощи в рамках настоящей статьи. Запрашиваемая Сторона может, в качестве условия предоставления помощи, потребовать применения двойной подсудности (например, если она сохраняет за собой право потребовать двойной подсудности в отношении сохранения данных согласно пункту 4 Статьи 29 «Оперативное обеспечение сохранности хранимых компьютерных данных»). В таком случае, двойная подсудность считается необходимой, если деяние, образующее правонарушение, является таковым согласно законам запрашиваемой Стороны, даже если эти законы помещают это правонарушение в другую категорию или используют для его определения другую терминологию. Это положение было сочтено необходимым для того, чтобы запрашиваемые Стороны не применяли слишком жесткие критерии в отношении двойной подсудности. С учетом расхождений в законодательных системах, различия в терминологии и классификации криминальных деяний неизбежны. Если действие является уголовным преступлением в обеих системах, такие технические различия не должны

помешать оказанию содействия. В случаях, когда применяется стандарт двойной подсудности, должны использоваться гибкие методы, способствующие предоставлению помощи.

Внеплановая информация (Статья 26)

260. Данная статья основана на таких положениях более ранних документов Совета Европы, как Статья 10 Конвенции об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности (ETS № 141) и Статья 28 Конвенции об уголовной ответственности за коррупцию (ETS № 173). Часто Сторона владеет ценной информацией, которая, по ее мнению, может помочь другой Стороне при проведении уголовного расследования или процессуальных действий, и о существовании которой другая Сторона не знает. В таких случаях не обязательно дожидаться просьбы о взаимопомощи. Пункт 1 дает стране, обладающей информацией, полномочия направить ее другой стране без предварительной просьбы. Это положение было сочтено полезным, поскольку по законам некоторых стран такая позитивная передача судебных доказательств нужна для обеспечения содействия в отсутствие просьбы о нем. Сторона не обязана направлять внеплановую информацию другой Стороне; она может предпринимать самостоятельные действия в свете имеющихся обстоятельств дела. Кроме того, внеплановое раскрытие информации не препятствует раскрывающей ее Стороне, имеющей на это юрисдикцию, вести следствие или разбирательство в отношении обнаруженных фактов.

261. Пункт 2 предусматривает, что в некоторых обстоятельствах Сторона направляет внеплановую информацию только в том случае, если эта закрытая информация будет

храниться в тайне, или если могут быть применены другие условия по ее использованию. В частности, конфиденциальность является важным условием в случаях, когда важные интересы предоставляющей информацию страны подвергнутся опасности при ее разглашении (например, в случае необходимости скрыть особенности методов сбора информации или преследование криминальной группировки). Если предварительный запрос показывает, что получающая Сторона не может согласиться на условие, выдвигаемое предоставляющей Стороной (например, когда невозможно согласиться на соблюдение конфиденциальности, поскольку информация требуется в качестве доказательства на открытом судебном заседании), получающая Сторона информирует об этом другую Сторону, которая после этого может не предоставлять информацию. Если принимающая Сторона соглашается на условие, она обязана его соблюдать. Условия, выставленные в рамках данной статьи, должны соответствовать тем, которые могут быть выставлены предоставляющей информацию Стороной в ответ на запрос о взаимопомощи от получающей Стороны.

Подраздел 4 – Процедуры направления запросов о взаимной помощи в отсутствие применимых международных соглашений

Процедуры направления запросов о взаимной помощи в отсутствие применимых международных соглашений (Статья 27)

262. Статья 27 обязывает Стороны применять определенные условия и процедуры взаимопомощи, если между

запрашивающей и запрашиваемой Сторонами нет договора или иного соглашения о взаимопомощи, основанного на действующем единообразном или двустороннем законодательстве. Таким образом, Статья закрепляет общий принцип оказания взаимопомощи через применение соответствующих договоров и подобных соглашений. Составители Конвенции отказались от создания отдельного общего режима взаимопомощи, который применялся бы вместо других документов и соглашений, договорившись, что в большинстве случаев более практично полагаться на существующие соглашения об оказании взаимной юридической помощи. Это даст специалистам по взаимопомощи возможность использовать те документы и соглашения, с которыми они лучше всего знакомы, и поможет избежать непонимания, которое может появиться при установлении конкурирующих режимов. Как было сказано выше, каждая Сторона обязана установить юридическую основу для сотрудничества только в отношении механизмов, необходимых для быстрого и эффективного оказания помощи по правонарушениям, совершенным с использованием компьютера (см. Статьи 29-35 (Особые положения – Подразделы 1, 2, 3)), если текущие договоры, соглашения и законы о взаимопомощи этого не предусматривают.

263. Соответственно, большинство форм взаимопомощи между Сторонами будут осуществляться согласно Европейской Конвенции о взаимной правовой помощи по уголовным делам (ETS №30) и ее Протоколу (ETS № 99). Если Стороны не желают применять положения данной статьи, и между ними есть действующие соглашения об оказании взаимной юридической помощи или иные многосторонние

соглашения, регулирующие взаимопомощь по уголовным делам (например, соглашения между странами – членами Евросоюза), они могут применять свои условия, дополненные специальными механизмами, которые действуют в отношении преступлений, связанных с использованием компьютера (см. остальную часть Главы III). Взаимопомощь может также опираться на соглашения, заключенные на основании единообразного или двустороннего законодательства – например, на систему сотрудничества, разработанную странами Северной Европы и признанную Европейской Конвенцией о взаимной правовой помощи по уголовным делам (Статья 25, пункт 4) и членами Содружества. Наконец, ссылка на договоры или соглашения о взаимопомощи на основании единообразного или двустороннего законодательства не ограничена документами, действующими на момент вступления в силу данной Конвенции, но касается также документов, которые могут быть приняты в будущем.

264. Пункты 2–10 Статьи предусматривают ряд правил по предоставлению взаимопомощи в отсутствие соглашений об оказании взаимной юридической помощи или соглашений, основанных на единообразном или двустороннем законодательстве. В них входят установление центральных органов власти, определение условий, оснований и процедур в случаях отсрочки или отказа, конфиденциальности запросов, и прямого общения. В отношении этих вопросов в отсутствие договора о взаимопомощи или соглашения, основанного на единообразном или двустороннем законодательстве, положения данной Статьи должны применяться вместо внутренних законов, регулирующих взаимопомощь. В то же время Статья 27 не предусматривает правил для

других вопросов, которые обычно освещены во внутреннем законодательстве, регулирующем международную взаимопомощь. В ней нет положений, касающихся формы и содержания запросов, снятия свидетельских показаний с запрашивающей или запрашиваемой Стороны, ведения официальных или деловых записей, перевода свидетелей под стражу, или содействия в вопросах конфискации. По таким вопросам пункт 4 Статьи 25 предусматривает, что в отсутствие соответствующего положения в данной Главе конкретные условия оказания содействия определяются законом запрашиваемой Стороны.

265. Пункт 2 требует установления одного или нескольких органов центральной власти, ответственных за направление запросов о содействии и ответы на них. Установление органов центральной власти – это типичная черта современных документов, посвященных взаимопомощи в уголовных делах. Оно особенно полезно для обеспечения быстрого реагирования, которое так важно в борьбе с преступлениями, связанными с применением компьютера. Во-первых, прямая связь между такими органами власти быстрее и эффективнее, нежели передача информации по дипломатическим каналам. Кроме того, установление активного органа центральной власти способствует внимательному рассмотрению входящих и исходящих запросов. Оно дает возможность партнерским правоохранительным органам получать советы о том, как лучше соблюсти юридические требования запрашиваемой Стороны, а также позволяет обрабатывать должным образом особо срочные или важные запросы.

266. Для повышения эффективности Сторонам рекомендуется установить единый центральный орган, отвечающий

за взаимопомощь. Как правило, наиболее эффективной является ситуация, если орган власти, назначенный с этой целью в соответствии с соглашениями о взаимопомощи или с внутренним законодательством Стороны, является также органом центральной власти по данной статье. Сторона, однако, имеет возможность назначить несколько органов центральной власти, если это соответствует ее системе взаимопомощи. В таких случаях Сторона должна убедиться, что каждый из органов власти одинаково интерпретирует положения Конвенции, и что исходящие и входящие запросы обрабатываются быстро и эффективно. Каждая Сторона должна сообщить Генеральному Секретарю Совета Европы наименования и адреса (включая адреса электронной почты и номера факсов) органов власти, созданных для получения и реагирования на просьбы о взаимопомощи согласно данной Статье; Стороны должны также удостовериться, что информация своевременно обновляется.

267. Часто главной целью страны, обращающейся с просьбой о взаимопомощи, является желание убедиться, что соблюдено ее внутреннее законодательство, регулирующее допустимость доказательства, и что в результате она может использовать это доказательство в суде. Для обеспечения таких требований в отношении доказательств, пункт 3 обязывает запрашиваемую Сторону исполнить запрос в соответствии с процедурами, указанными запрашивающей Стороной, если это согласуется с ее законами. Особое значение имеет то, что данный пункт полагается только на обязательство уважать технические процессуальные требования, но не основные процессуальные гарантии. Таким образом, запрашивающая Сторона не может требовать от

запрошенной Стороны проведения обыска и изъятия, которые не соответствуют основным юридическим требованиям запрашиваемой Стороны в отношении такой меры. Из-за ограниченного характера обязательства было решено, что сам факт того, что юридическая система запрашиваемой стороны не имеет подобной процедуры, не является достаточным основанием для отказа в применении процедуры, запрошенной запрашивающей Стороной. Для отказа процедура должна противоречить юридическим принципам запрашиваемой Стороны. Например, по закону запрашивающей Стороны процессуальным требованием является дача свидетельских показаний под присягой. Даже если запрашиваемая Сторона не имеет такого требования во внутреннем законодательстве, она должна выполнить запрос запрашивающей Стороны.

268. Пункт 4 предусматривает возможность отказа в ответ на запрос о взаимопомощи, поступившую согласно данной Статье. В содействии может быть отказано на основаниях, предусмотренных пунктом 4 Статьи 25 (т.е. на основании законодательства запрашиваемой Стороны), включая ущерб суверенности страны, ее безопасности, общественному порядку или другим ключевым интересам; либо в случаях, когда правонарушение рассматривается запрашиваемой Стороной как политическое или связанное с политическим правонарушением. В соответствии с основополагающим принципом взаимопомощи (предоставление максимально широкого содействия, см. Статьи 23, 25), основания для отказа, устанавливаемые запрашиваемой Стороной, должны быть минимальными и применяться ограниченно. Они не должны быть настолько обширными,

чтобы категорически отрицать возможность содействия, или подчинять его жестким условиям в отношении широких категорий доказательств или информации.

269. В соответствии с таким подходом было решено, что за исключением оснований, изложенных в Статье 28, отказ в содействии на основании защиты данных может применяться лишь в исключительных случаях. Такая ситуация может возникнуть, если после взвешивания ключевых интересов, относящихся к конкретному делу (интересов общества и справедливого осуществления правосудия с одной стороны и частных интересов с другой), предоставление запрашивающей стороне конкретных данных создаст настолько серьезные трудности, что они будут рассмотрены запрашиваемой Стороной как основание для отказа по причине ключевых интересов. Таким образом, предотвращается широкое, категоричное и систематическое применение принципа защиты данных для отказа в содействии. Не является основанием для отказа тот факт, что заинтересованные Стороны имеют разные системы защиты конфиденциальности данных (например, запрашивающая Сторона не имеет эквивалентного органа, контролирующего соблюдение законодательства о защите персональных данных), или используют разные средства защиты личных сведений (например, запрашивающая Сторона вместо удаления использует другие средства для защиты конфиденциальности или точности персональной информации, полученной правоохранительными органами). Перед применением «ключевых интересов» в качестве основания для отказа в сотрудничестве запрашиваемая Сторона должна попытаться изложить условия, которые позволят передать

данные другой стороне (см. пункт 6 Статьи 27 и пункт 271 данной записки).

270. Пункт 5 позволяет запрашиваемой Стороне отсрочить содействие в случаях, когда немедленные действия в ответ на запрос могут нанести ущерб расследованию или процессуальным действиям запрашиваемой Стороны. Например, если запрашивающая Сторона добивается получения доказательств или свидетельских показаний для расследования или суда, и эти же доказательства или свидетели нужны для суда, который должен начаться в запрашиваемой Стороне, эта Сторона может оправданно отсрочить оказание помощи.

271. Пункт 6 предусматривает, что в случаях, когда в сотрудничестве может быть отказано, или предоставление его отсрочено, запрашиваемая Сторона может вместо этого предоставить помощь на определенных условиях. Если условия не устраивают запрашивающую Сторону, запрашиваемая Сторона может внести в них изменения или воспользоваться своим правом на отсрочку или отказ в предоставлении помощи. Поскольку запрашиваемая Сторона обязана предоставить максимальное содействие, было решено, что оба основания для отказа и условия для него должны использоваться ограниченно.

272. Пункт 7 обязывает запрашиваемую Сторону информировать запрашивающую Сторону о результатах запроса и предоставлять причины в случае отказа или отсрочки помощи. Предоставление причин может, в числе прочего, помочь запрашивающей Стороне понять, как запрашиваемая Сторона интерпретирует требования данной Статьи, найти основание для консультации в целях повышения

эффективности взаимопомощи в будущем, и предоставить запрашивающей Стороне ранее неизвестную фактическую информацию о доступности или состоянии свидетелей или доказательств.

273. Бывает, что Сторона обращается с просьбой о взаимопомощи в особо деликатном деле, или в случае, когда преждевременное обнародование фактов, лежащих в основе дела, привело бы к катастрофическим последствиям. Пункт 8 позволяет запрашивающей Стороне просить о соблюдении конфиденциальности о факте запроса и его содержании. Однако конфиденциальности не следует добиваться в тех случаях, когда это может помешать запрашиваемой Стороне получить нужные доказательства или информацию (например, когда раскрытие информации требуется для получения судебного приказа о содействии, или когда частные лица, владеющие доказательствами, должны знать о запросе на предоставление помощи, чтобы эта помощь могла быть предоставлена). Если запрашиваемую Сторону не устраивает запрос о соблюдении конфиденциальности, она должна уведомить об этом запрашивающую Сторону, которая после этого может аннулировать или изменить такой запрос.

274. Органы центральной власти, назначенные в соответствии с пунктом 2, должны общаться друг с другом напрямую. Однако в экстренных случаях запрос о юридической взаимопомощи может быть направлена судьей и прокурором запрашивающей Стороны судье и прокурору запрашиваемой Стороны. Судья или прокурор должен также отправить копию просьбы в свой орган центральной власти для передачи органам центральной власти запрашиваемой

Стороны. Согласно подпункту b, просьбы могут быть направлены через Интерпол. Согласно подпункту c, власти запрашиваемой Стороны, получившие запрос, не входящую в сферу их компетенции, имеют двойное обязательство. Во-первых, они должны передать запрос компетентным органам запрашиваемой Стороны. Во-вторых, они должны проинформировать власти запрашивающей Стороны об этой передаче. Согласно подпункту d, просьбы также могут быть переданы напрямую без вмешательства центральных органов власти, даже если они не являются срочными, при условии что власти запрашиваемой Стороны могут выполнить запрос без применения силовых мер. Согласно подпункту e, Сторона может уведомить другие стороны через Генерального Секретаря Совета Европы о том, что в целях эффективности прямые обращения следует направлять в орган центральной власти.

Конфиденциальность и ограничения на использование информации (Статья 28)

275. Данное положение предусматривает ограничения на использование информации или материалов, чтобы в случаях, когда информация является особо значимой, запрашиваемая Сторона могла быть уверена, что ее использование ограничено сферой, в которой оказывается помощь, или что о ней будет известно только правоохранительным органам запрашивающей Стороны. Такие ограничения предоставляют гарантии, доступные, в числе прочего, для защиты данных.

276. Как и Статья 27, Статья 28 применяется только в случаях, когда между Сторонами не существует договора о

взаимопомощи или соглашения на основе единообразного или двустороннего законодательства. Если такой договор или соглашение существует, его положения о конфиденциальности и ограничениях на использование информации должны применяться вместо положений данной Статьи, если Сторонами не определено иное. Это помогает избежать конфликта существующих двусторонних и многосторонних договоров о взаимопомощи и подобных соглашений, и позволяет специалистам работать в обычном понятном им режиме, а не пытаться применять два альтернативных и возможно противоречивых документа.

277. Пункт 2 позволяет запрашиваемой Стороне при ответе на запрос о взаимопомощи выдвигать два условия. Первое из них – сохранение конфиденциальности в отношении предоставленной информации или материалов, когда запрос не может быть выполнен в отсутствие этого условия (например, когда привлекается секретный информатор). Нецелесообразно требовать абсолютной конфиденциальности, когда запрашиваемая Сторона обязана оказать помощь, ибо это часто мешает запрашивающей Стороне успешно расследовать правонарушение или осудить преступника (например, при использовании доказательств в открытом судебного заседании, подразумевающем обязательное раскрытие данных).

278. Во-вторых, запрашиваемая Сторона может сделать условием предоставления информации невозможность ее использования в расследованиях и процессуальных действиях, кроме тех, которые указаны в запросе. Это условие должно быть открыто высказано запрашиваемой Стороной, иначе ограничение не будет применяться запрашивающей

Стороной. В случае предъявления такого условия, информация и материалы будут использованы только в целях, предусмотренных в запросе, и их использование в иных целях без согласия запрашиваемой Стороны будет исключено. Стороны, участвующие в переговорах, признали два исключения из ограничений на использование информации. Они подразумеваются условиями данного пункта. Во-первых, согласно основным юридическим принципам многих стран, если предоставленный материал является доказательством, оправдывающим обвиняемого, он должен быть раскрыт защите или судебным органам. Кроме того, большинство материалов, предоставляемых согласно режиму взаимопомощи, предназначены для использования в судебном разбирательстве, которое обычно является публичным (включая обязательное раскрытие информации). Как только происходит такое раскрытие, материалы, по сути, переходят в категорию публичной информации. В таких ситуациях невозможно обеспечить конфиденциальность следствия или судопроизводства, в отношении которого запрашивалась помощь.

279. Согласно пункту 3, если Сторона, которой передана информация, не согласна с выдвинутыми условиями, она должна уведомить об этом другую Сторону, которая в свою очередь может не предоставлять информацию. Если Сторона-получатель соглашается на условия, она должна их соблюдать.

280. Согласно пункту 4 от запрашивающей Стороны может потребоваться объяснить использование информации или материалов, полученных на условиях, описанных в пункте 2, чтобы запрашиваемая Сторона могла удостовериться в

соблюдении этих условий. Было решено, что запрашиваемая Сторона не может запрашивать слишком обременительные объяснения (например, о каждом случае доступа к предоставленной информации или материалам).

Часть 2 – Особые положения

281. Данная часть предусматривает особые механизмы, необходимые для эффективных и согласованных международных действий в отношении правонарушений, связанных с использованием компьютера, и доказательств в электронной форме.

Подраздел 1 – Взаимопомощь в связи с предварительными мерами

Оперативное обеспечение сохранности хранимых компьютерных данных (Статья 29)

282. Данная статья предусматривает международный механизм, эквивалентный механизму, описанному в Статье 16 и использующемуся внутри страны. Пункт 1 уполномочивает Сторону подавать запрос, а пункт 3 требует от Сторон правоспособности на оперативное обеспечение сохранности данных, находящихся на территории запрашиваемой Стороны, при помощи компьютерной системы. Это предотвратит изменение, перемещение или удаление данных в период, требуемый для подготовки, передачи и выполнения просьбы о взаимопомощи в получении данных. Хранение данных – ограниченная и временная мера, которая должна быть гораздо более быстрой, нежели традиционная взаимопомощь. Как уже обсуждалось, компьютерные данные весьма нестабильны. Несколько нажатий на клавиши или

некоторые программы могут уничтожить их, сделав невозможным установление правонарушителя или уничтожив ключевые доказательства вины. Некоторые формы компьютерных данных хранятся лишь в течение короткого периода времени, а затем удаляются. Поэтому составители пришли к выводу о необходимости создания механизма, обеспечивающего доступность таких данных во время длительного и сложного процесса выполнения просьбы о взаимопомощи, который может занять недели и месяцы.

283. Будучи гораздо более быстрой, чем обычная практика взаимопомощи, эта мера является в то же время менее интрузивной. Должностным лицам запрашиваемой Стороны не нужно получать данные во владение от хранящего их лица. Предпочтительнее, чтобы запрашиваемая Сторона гарантировала, что хранящее лицо (часто это поставщик услуг или третья сторона) хранило (т.е. не удаляло) данные в ожидании выпуска предписания о передаче их правоохранительным органам на более поздней стадии. Преимущества такой процедуры – быстрота и защита частной жизни лица, которого касаются данные, поскольку они не будут раскрыты или изучены кем-либо из должностных лиц до выполнения критериев полного раскрытия, согласно обычному режиму взаимопомощи. В то же время запрашиваемая Сторона может использовать иные меры для обеспечения быстрого сохранения данных, включая оперативный выпуск и выполнение распоряжения о предъявлении данных или приказа об обыске. Главным требованием является быстрота действий для предотвращения безвозвратной утраты данных.

284. Пункт 2 устанавливает содержание запроса о сохранении данных. Поскольку это временная мера, и поскольку

запрос требуется подготовить и передать быстро, предоставляемая информация должна быть краткой и минимально необходимой для обеспечения сохранности данных. Помимо указания органов, которым требуется сохранение данных, и правонарушения, в отношении которого применяется эта мера, запрос должна содержать краткие факты, информацию, достаточную для определения данных и их месторасположения, признаки того, что данные имеют отношение к следствию или уголовному преследованию данного правонарушения, и что их хранение необходимо.

285. Пункт 3 устанавливает, что двойная подсудность не должна быть условием хранения данных. В целом применение принципа двойной подсудности нецелесообразно в отношении хранения данных. Во-первых, в современной практике взаимопомощи есть тенденция использовать принцип двойной подсудности только в самых интрузивных мерах процессуального характера, таких как обыск и изъятие или перехват. Хранение данных, по мнению составителей, не особенно интрузивно, так как хранящее лицо просто сохраняет данные в своем владении, и они не раскрываются и не изучаются должностными лицами запрашиваемой Стороны до подачи официальной просьбы о взаимопомощи, предполагающей раскрытие данных. Во-вторых, на практике, предоставление разъяснений, необходимых для установления двойной подсудности, часто занимает настолько много времени, что за этот период данные могут быть удалены, перемещены или изменены. Например, на ранних этапах следствия запрашивающая Сторона может знать, что произошло вмешательство в работу компьютера на ее территории, однако полное понимание характера и

степени ущерба она получает куда позже. Если запрашиваемая Сторона отсрочит сохранение данных о трафике, которые помогли бы отследить источник вторжения до момента установления двойной подсудности, важные данные будут в обычном порядке удалены провайдерами, которые хранят их лишь в течение нескольких часов или дней после того, как произошла передача. Даже если бы после этого запрашивающая Сторона установила двойную подсудность, важные данные о трафике невозможно было бы восстановить, и правонарушитель никогда не был бы установлен.

286. Согласно общему правилу Стороны должны обойтись без требований о двойной подсудности в целях сохранения данных. Однако пункт 4 подразумевает ограниченную оговорку. Если Сторона требует двойной подсудности в качестве условия для ответа на запрос о взаимопомощи, и если у нее есть причины считать, что в момент раскрытия данных принцип двойной подсудности не будет исполнен, она может сохранить за собой право требовать двойной подсудности как предварительного условия для сохранения данных. В отношении правонарушений, указанных в Статьях 2–11, считается, что условие двойной подсудности автоматически соблюдается между Сторонами, подчиняясь любым оговоркам, которые Стороны могли внести по этим правонарушениям, если это разрешено Конвенцией. Следовательно, Стороны могут предъявлять это требование только в отношении правонарушений, не определенных в Конвенции.

287. В других случаях, согласно пункту 5, запрашиваемая Сторона может отказать в запросе о сохранении данных, только если ее выполнение может нанести ущерб ее суверенности, безопасности, общественному порядку или иным

ключевым интересам; или если Сторона считает правонарушение политическим или связанным с политическим. По причине высокой значимости этой меры для эффективного расследования и преследования преступлений, связанных с использованием компьютера, было решено, что предоставление любых других оснований для отказа в запросе о сохранении данных должно пресекаться.

288. Иногда запрашиваемая Сторона понимает, что лицо, хранящее данные, может предпринять действия, угрожающие конфиденциальности или способные нанести другой ущерб расследованию (например, когда данные, подлежащие хранению, находятся у провайдера, контролируемого преступной группой, или у самого объекта расследования). В таких ситуациях, согласно Пункту 6, следует оперативно уведомить запрашивающую Сторону, чтобы она могла оценить риск выполнения просьбы о сохранении данных, либо найти более интрузивный, но вместе с тем и более надежный способ оказания взаимопомощи (например, распоряжение о предоставлении данных или обыск и изъятие).

289. Пункт 7 обязывает Стороны обеспечить хранение данных на срок не менее 60 дней, вплоть до получения официального обращения за содействием с просьбой о раскрытии данных, и продолжение их хранения после получения такой просьбы.

Оперативное раскрытие сохраненных данных о трафике (Статья 30)

290. Данная статья предусматривает международный эквивалент полномочия, установленного для внутреннего

пользования в Статье 17. Часто по просьбе Стороны, на территории которой было совершено преступление, запрашиваемая Сторона хранит данные о трафике, относящиеся к передаче, произошедшей через ее компьютеры, чтобы отследить передачу до ее источника и установить правонарушителя, либо найти важные улики. Поступая таким образом, запрашиваемая Сторона может обнаружить, что данные о трафике, найденные на ее территории, указывают на то, что передача была направлена от провайдера в третьей стране или с территории запрашивающей Стороны. В таких случаях запрашиваемая Сторона должна оперативно предоставить запрашивающей Стороне количество данных о трафике, достаточное для установления провайдера в другой стране и пути информационного обмена. Если передача данных произошла с территории третьей страны, эта информация поможет запрашивающей Стороне отправить этой стране запрос на сохранение данных и предоставление оперативной взаимопомощи, чтобы отследить передачу до первоисточника. Если передача прослеживается до территории запрашивающей Стороны, эта Сторона может добиться сохранения и раскрытия данных о трафике через внутренние процедуры.

291. Согласно пункту 2, запрашиваемая Сторона может отказать в раскрытии данных о трафике только в том случае, если раскрытие может нанести ущерб ее суверенности, безопасности, общественному порядку или другим ключевым интересам; либо если она считает правонарушение политическим или связанным с политическим. Как и в Статье 29, данный тип информации крайне важен для установления лиц, совершивших правонарушение, а также для

нахождения улик, поэтому основания для отказа должны быть строго ограничены, и было решено, что другие основания для отказа в помощи не допускаются.

Подраздел 2 – Взаимопомощь в связи со следственными полномочиями

Взаимопомощь в отношении доступа к хранимым компьютерным данным (Статья 31)

292. Каждая Сторона должна иметь возможность осуществлять от имени другой Стороны обыск или подобный доступ, изъятие или подобное обеспечение сохранности, и раскрытие данных, хранящихся в компьютерной системе, расположенной на ее территории так же как, согласно Статье 19, она должна иметь возможность совершать эти действия для внутренних целей. Пункт 1 уполномочивает Стороны запрашивать подобный вид взаимопомощи, а пункт 2 требует от запрашиваемой Стороны ее предоставления. Пункт 2 также указывает, что сроки и условия предоставления такого сотрудничества должны быть указаны в применяемых договорах, соглашениях и внутренних законодательствах, регулирующих юридическую взаимопомощь в уголовных делах. Согласно пункту 3, ответ на такой запрос должен быть оперативным в случаях, если (1) существуют основания считать, что важные данные особенно уязвимы для утери или изменения; или (2) если упомянутые договоры, соглашения и законодательства не предусматривают иного.

Трансграничный доступ к хранимым компьютерным данным с соответствующего согласия, или к общедоступным данным (статья 32)

293. Составители Конвенции долго обсуждали вопрос о том, когда Сторона может в одностороннем порядке получать доступ к компьютерным данным, хранящимся на территории другой Стороны, не обращаясь с просьбой о взаимопомощи. Были детально рассмотрены случаи, в которых странам допустимо и недопустимо действовать в одностороннем порядке. В конечном итоге составители определили, что пока невозможно создать всеобъемлющий юридически обязывающий режим регулирования этой сферы. Причина этому отчасти – недостаток опыта в подобных ситуациях, отчасти – понимание, что правильное решение нередко зависит от определенных обстоятельств каждого отдельно взятого дела. Составители решили изложить в Статье 32 только ситуации, в которых, по всеобщему согласию, возможны действия в одностороннем порядке. Было решено не регулировать другие ситуации до появления соответствующего опыта и проведения дискуссий в его свете. В этом отношении пункт 3 Статьи 39 предусматривает, что другие ситуации не санкционируются и не исключаются.

294. Статья 32 касается двух ситуаций: во-первых, случаев, когда данные, к которым осуществляется доступ, являются общедоступными; во-вторых, случаев, когда Сторона получила доступ или сами данные, находящиеся вне ее территории, через компьютерную систему на своей территории, и получила законное и добровольное согласие лица, имеющего законные полномочия на раскрытие Стороне данных через эту систему. Кто является лицом, «имеющим законные

полномочия», зависит от обстоятельств, характера лица и применяемого закона. Например, электронный адрес лица может храниться у провайдера в другой стране, или лицо может намеренно хранить данные в другой стране. Эти лица могут получить данные и, при условии, что у них есть на это законные полномочия, добровольно раскрыть данные правоохранительным органам или разрешить им доступ к данным, как это предусматривает данная Статья.

Взаимопомощь в отношении сбора данных о трафике в реальном времени (Статья 33)

295. Во многих случаях следователи не могут обеспечить отслеживание информационного обмена до его источника с помощью записей предыдущих передач, поскольку важные данные о трафике могут быть автоматически удалены провайдером до того, как их могли сохранить. Поэтому следователям каждой из Сторон важно иметь возможность получить данные о трафике в реальном времени в отношении информационного обмена, проходящего через компьютерные системы других Сторон. В соответствии со Статьей 33 каждая Сторона обязана собирать данные о трафике в реальном времени для другой Стороны. Статья требует от Сторон сотрудничества по таким вопросам, однако, как и везде, здесь существуют различия в условиях взаимопомощи. Обычно применяются те условия и сроки предоставления помощи, которые указаны в применяемых договорах, соглашениях и законах, регулирующих взаимную юридическую помощь в уголовных делах.

296. Во многих странах предоставляется широкая взаимопомощь в отношении сбора данных о трафике, так как он

считается менее интрузивной мерой, нежели перехват данных об информационном наполнении или обыск и изъятие. Однако некоторые страны используют более узкий подход. Таким же образом, как в пункте 3 Статьи 14, согласно которому Стороны могут внести оговорку в отношении внутренних мер, пункт 2 данной статьи позволяет Сторонам ограничить применение этой меры более узким рядом правонарушений, чем это предусмотрено в Статье 23. Предусмотрена одна оговорка: ни при каких обстоятельствах этот ряд не может быть более ограниченным, чем ряд правонарушений, к которым применяется данная мера в похожих внутренних делах. Поскольку сбор данных о трафике в реальном времени иногда бывает единственным способом установить личность правонарушителя, и поскольку эта мера является менее интрузивной, использование фразы «по крайней мере» в пункте 2 должно поощрять Стороны предоставлять максимальную помощь даже в случаях отсутствия двойной подсудности.

Взаимопомощь в отношении перехвата данных об информационном наполнении (Статья 34)

297. Обязательства по предоставлению взаимопомощи в осуществлении перехвата ограничены, ввиду его высокой интрузивности. Помощь должна оказываться в той степени, в которой это позволяют применяемые Сторонами договоры и законы. Поскольку оказание содействия в перехвате данных об информационном наполнении – это развивающаяся область практики взаимопомощи, было решено следовать существующим режимам оказания взаимопомощи и внутренним законодательствам, касающимся обязательств

и ограничений по ее оказанию. По этому поводу сделаны ссылки на комментарии к Статьям 14, 15 и 21, а также к оговорке № R (85)10, касающейся практического применения Европейской Конвенции о взаимной помощи по уголовным делам в отношении судебных поручений о перехвате телекоммуникаций.

Подраздел 3 – Сеть 24/7

Сеть 24/7 (Статья 35)

298. Как уже обсуждалось выше, эффективная борьба с правонарушениями, совершенными с использованием компьютерных систем, и эффективный сбор доказательств в электронной форме требуют быстрого реагирования. Кроме того, несколько нажатий на клавиши в одной части мира могут привести к мгновенным последствиям за многие тысячи километров. Поэтому существующие условия сотрудничества и взаимопомощи правоохранительных органов требуют дополнительных каналов для того, чтобы эффективно справляться с проблемами компьютерной эры. Средство, описанное в данной Статье, основано на опыте, полученном из уже функционирующей сети, созданной под эгидой стран Большой Восьмерки. Согласно этой Статье, каждая Сторона обязана создать контактный центр, работающий 24 часа в сутки 7 дней в неделю, для обеспечения немедленной помощи в расследованиях и процессуальных действиях в рамках данной Главы (в частности как это определено в Статье 35, пункт 1 a – c). Было решено, что создание такой сети является одним из важнейших средств, предусмотренных Конвенцией для того, чтобы Стороны могли эффективно реагировать на проблемы, возникающие перед

правоохранительными органами в связи с преступлениями, связанными с использованием компьютера.

299. Круглосуточный контактный центр каждой Стороны должен либо способствовать, либо напрямую предоставлять, в числе прочего, технические рекомендации, сохранение данных, сбор доказательств, юридическую информацию и установление местонахождения подозреваемых. Термин «юридическая информация» в пункте 1 означает предоставление Стороне, запрашивающей сотрудничество, любых юридических данных, требуемых для оказания официального или неофициального содействия.

300. Каждая Сторона может свободно определять место контактного центра в структуре правоохранительных органов. Некоторые Стороны могут пожелать расположить круглосуточный контактный центр на территории центрального органа власти, чтобы обеспечить их взаимопомощь; некоторые считают, что лучшим расположением является специальное подразделение полиции по борьбе с компьютерными преступлениями. Возможны также другие варианты, подходящие для конкретной Стороны и учитывающие ее государственное устройство и правовую систему. Круглосуточный центр связи должен обеспечивать как технические консультации по прекращению или отслеживанию атак, так и обязанности по международному сотрудничеству (например, установление местонахождения подозреваемых), поэтому не существует единого способа его организации, и предполагается, что структура такой сети будет со временем развиваться. При создании государственного контактного центра должное внимание следует уделить

необходимости общения с контактными центрами, использующими другие языки.

301. Пункт 2 предусматривает, что среди важных задач, выполняемых круглосуточным контактным центром, должно быть содействие быстрому исполнению тех функций, которые он не выполняет напрямую. Если такой центр является частью полицейского подразделения, он должен иметь возможность оперативно координировать свои действия с другими правительственными органами (например, с центральным органом власти по международной выдаче или взаимопомощи), чтобы соответствующие меры принимались в любое время суток. Кроме того, пункт 2 требует, чтобы контактные центры Сторон могли осуществлять оперативный обмен сообщениями с другими участниками сети.

302. Пункт 3 требует, чтобы каждый контактный центр в сети имел соответствующее оборудование. Современные телефоны, факсы и компьютеры совершенно необходимы для слаженной работы сети, а по мере развития технологий должны устанавливаться и другие виды коммуникационного и аналитического оборудования. Пункт 3 требует также, чтобы персонал контактного центра имел соответствующую подготовку в сфере компьютерных преступлений и эффективной борьбы с ними.

Глава IV – Заключительные положения

303. За отдельными исключениями, положения настоящей Главы базируются на «Типовых заключительных положениях конвенций и договоров Совета Европы», утвержденных Комитетом министров в феврале 1980 года на своем 315-м

заседании на уровне заместителей. Большинство статей с 36 по 48 используют стандартные формулировки положений или основаны на длительной практике разработки договоров Совета Европы, и поэтому не требуют особых комментариев. Однако некоторые модификации типовых положений или новые положения требуют объяснения. В данном контексте типовые положения носят необязательный характер. Как указано во Введении в типовые положения, «предполагается, что данные типовые заключительные положения облегчат задачу комитетам экспертов и помогут избежать текстовых расхождений. Типовое положение ни в коей мере не является обязательным, и в определенных случаях могут использоваться другие формулировки»

Подписание и вступление в силу (Статья 36)

304. Пункт 1 Статьи 36 составлен на основании нескольких прецедентов, установленных в других конвенциях, которые были разработаны в рамках Совета Европы. Например, Конвенция о передаче осужденных лиц (СЕД № 112) и Конвенция об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности (СЕД № 141) предусматривают подписание конвенции до ее вступления в силу не только странами – членами Совета Европы, но также странами, членами Совета не являвшимися, но участвовавшими в разработке документа. Это положение направлено на то, чтобы максимальное число заинтересованных стран (не только членов Совета Европы) как можно скорее стали Сторонами Конвенции. В данном случае положение применяется к четырем странам, не являющимся членами Совета Европы – Канаде, Японии, ЮАР и США, активно участвовавшим в разработке Конвенции. Как только Конвенция

вступает в силу, согласно пункту 3, другие страны – не члены СЕ, не охватываемые этим положением, могут быть приглашены для присоединения к Конвенции в соответствии с пунктом 1 Статьи 37.

305. Пункт 3 Статьи 36 устанавливает пороговое число ратификаций, принятий или одобрений, необходимых для вступления Конвенции в силу. Установленное значение: 5. Эта цифра выше обычного порога (3) в договорах Совета Европы и отражает убеждение, что для успешного решения проблем, связанных с международной преступностью в компьютерной среде, требуется большее число стран. В то же время указанное количество не настолько велико, чтобы чрезмерно откладывать вступление Конвенции в силу. Среди пяти первых стран по меньшей мере три должны быть членами Совета Европы, остальные могут быть одними из четырех, принимавших участие в разработке Конвенции. Конечно, данное положение допускает вступление Конвенции в силу на основании согласия на ее обязательное соблюдение, выраженного пятью странами – членами Совета Европы.

Присоединение к Конвенции (Статья 37)

306. Статья 37 также составлена на основе прецедентов, установленных в других конвенциях Совета Европы, с добавлением одного дополнительного компонента. Согласно многолетней практике, Комитет министров решает (по своей инициативе или на основании просьбы) пригласить страну, не входящую в СЕ, которая не участвовала в разработке конвенции, присоединиться к Конвенции после консультаций со всеми Сторонами, независимо от того,

являются ли они членами СЕ. Это подразумевает, что в случаях, когда любая из Сторон возражает против присоединения страны, не входящей в СЕ, Комитет министров обычно не приглашает ее присоединиться к Конвенции. Однако согласно обычной формулировке Комитет министров теоретически может пригласить такую страну присоединиться к Конвенции, даже если страна, не входящая в СЕ, возражает против этого присоединения. Это означает, что теоретически право вето обычно не предоставляется странам, не входящим в СЕ, в процессе распространения договоров Совета Европы на другие страны, не входящие в СЕ. Однако было введено прямо сформулированное требование о том, что Комитет министров консультируется со всеми Сторонами Конвенции (не только со странами – членами СЕ) и получает их единодушное согласие на приглашение страны, не входящей в СЕ присоединиться к Конвенции. Как указано выше, такое требование соответствует практике и признает, что все Стороны Конвенции должны иметь возможность определять, с какой страной, не входящей в СЕ, они вступают в договорные отношения. Тем не менее, согласно принятой практике, официальное решение о приглашении страны, не входящей в ЕС, присоединиться к Конвенции должно быть принято представителями договаривающихся Сторон, обладающих правом заседать в Комитете министров. Это решение требует двух третей голосов, что предусмотрено в Статье 20 d Устава Совета Европы, и единодушного голосования представителей договаривающихся Сторон, обладающих правом заседать в Комитете министров.

307. Федеративные государства, желающие присоединиться к Конвенции, и намеревающиеся сделать заявление согласно Статье 41, должны заранее подать предварительный текст заявления, указанный в пункте 3 Статьи 41, чтобы Стороны могли оценить, как применение федеративных положений повлияет на будущее применение Конвенции Сторонами (см. п.320).

Действие Конвенции (Статья 39)

308. Пункты 1 и 2 Статьи 39 касаются взаимоотношений Конвенции с другими международными соглашениями и договоренностями. Указанные выше типовые положения не касаются того, как конвенции Совета Европы должны соотноситься между собой или с другими двусторонними или односторонними договорами, заключенными вне Совета Европы. Традиционный подход, используемый в конвенциях Совета Европы в сфере уголовного права (например, Соглашение о незаконных перевозках по морю наркотиков и психотропных веществ (СЕД №156)) предусматривает, что: (1) новые конвенции не влияют на права и обязательства, происходящие из существующих многосторонних международных конвенций по особым вопросам; (2) Стороны новой конвенции могут заключать между собой двусторонние или многосторонние соглашения по вопросам, указанным в конвенции, для дополнения и закрепления ее положений или для содействия применению заключенных в ней принципов; (3) если две и более Стороны новой конвенции уже заключили договор или соглашение в отношении вопроса, рассматриваемого в конвенции, или иным образом установили взаимоотношения по этому вопросу, они должны применять

этот договор или соглашение для урегулирования таких взаимоотношений вместо новой конвенции, при условии что это способствует международному сотрудничеству.

309. Ввиду того что Конвенция дополняет, а не замещает двусторонние и многосторонние соглашения и договоренности между Сторонами, составители сочли, что ограничивающая ссылка на «особые вопросы» не является информативной и что она может привести к ненужной путанице. Вместо этого пункт 1 Статьи 39 просто указывает, что данная Конвенция дополняет другие применяемые договоры и соглашения между Сторонами и упоминает в частности три договора Совета Европы в качестве не исчерпывающих примеров: Европейскую Конвенцию о выдаче 1957 г. (СЕД № 24), Европейскую Конвенцию о взаимопомощи по уголовным делам 1959 г. (СЕД № 30) и ее Дополнительный Протокол 1978 г. (СЕД № 99). Следовательно, в отношении общих вопросов эти соглашения и договоренности должны в принципе применяться Сторонами Конвенции о компьютерных преступлениях. В отношении особых вопросов, изложенных только в данной Конвенции, правило интерпретации lex specialis derogat legi generali (специальный закон отменяет общий закон) предусматривает, что Стороны должны отдавать приоритет правилам, содержащимся в Конвенции. Примером является Статья 30, которая предусматривает оперативное раскрытие сохраненных данных о трафике, когда это необходимо для установления пути конкретного информационного обмена. В этой специфической области Конвенция, как lex specialis (специальный закон), должна предоставлять правило первой очереди над положениями более общих соглашений о взаимопомощи.

310. Таким же образом составители сочли возможной проблемой язык, который делает применение существующих или будущих соглашений зависимым от того, «закрепляют» они или «способствуют» сотрудничеству, поскольку согласно подходу, установленному в Главе о международном сотрудничестве, предполагается, что Стороны применяют соответствующие международные соглашения и договоренности.

311. Когда основой для сотрудничества является действующий договор или соглашение о взаимопомощи, данная Конвенция при необходимости лишь дополняет существующие правила. Например, Конвенция предусматривает передачу просьбы о взаимопомощи через оперативные средства связи (см. пункт 3 Статьи 25), если такая возможность не существует в изначальном договоре или соглашении.

312. Согласно дополняющему характеру Конвенции, и в частности, ее подходу к международному сотрудничеству, пункт 2 устанавливает, что Стороны могут свободно применять соглашения, которые уже вступили в силу или могут вступить в силу в будущем. Прецедент такой формулировки можно найти в Конвенции о передаче осужденных лиц (СЕД № 112). Разумеется, в контексте международного сотрудничества ожидается, что применение других международных соглашений (многие из которых предлагают проверенные многолетние формулы международного сотрудничества) будет ему способствовать. Согласно условиям данной Конвенции, Стороны могут также согласиться применять ее положения о международном сотрудничестве вместо других соглашений (см. Статью 27(1)). В таких случаях положения о сотрудничестве, изложенные в Статье 27, заменяют собой соответствующие правила в иных соглашениях. Поскольку данная

Конвенция в целом предусматривает минимум обязательств, пункт 2 Статьи 39 признает, что Стороны свободны принимать на себя более специфические обязательства в дополнение к указанным в Конвенции, когда они устанавливают отношения по описанным в ней вопросам. Однако это не абсолютно верно: поступая так, Стороны должны уважать цели и принципы Конвенции, и, следовательно, не могут брать на себя обязательства, которые ей противоречат.

313. Определяя отношение Конвенции к иным международным соглашениям, составители также сошлись во мнении, что Стороны могут искать дополнительное руководство по соответствующим положениям в Венской конвенции о праве международных договоров.

314. При том, что Конвенция обеспечивает столь необходимый уровень гармонизации, она не претендует на решение всех спорных вопросов, касающихся преступлений, связанных с использованием компьютера. Поэтому был введен пункт 3, разъясняющий, что Конвенция оказывает влияние только на те вопросы, которые она призвана решить. Незатронутыми остаются иные права, ограничения, обязательства и ответственность, которые существуют, но не рассматриваются в Конвенции. Прецедент такой «исключающей оговорки» можно найти в других международных соглашениях (например, в Конвенции ООН о борьбе с финансированием терроризма).

Заявления (Статья 40)

315. Статья 40 ссылается на определенные статьи, в основном касающиеся правонарушений, установленных

Конвенцией в разделе материального права, где Сторонам разрешено включать определенные дополнительные элементы, изменяющие сферу применения положений. Такие дополнительные элементы направлены на согласование понятийных и юридических различий, которые более оправданы в договоре с глобальными амбициями, чем исключительно в контексте Совета Европы. Заявления считаются допустимой интерпретацией положений Конвенции; их следует отличать от оговорок, которые позволяют Стороне исключать или изменять правовое значение некоторых обязательств, изложенных в Конвенции. Поскольку Сторонам Конвенции важно знать, какие дополнительные элементы были внесены другими Сторонами, страна обязана сообщить об их внесении Генеральному секретарю Совета Европы в момент подписания или сдачи на хранение грамот о ратификации, принятии, одобрении или присоединении. Такое уведомление особенно важно в отношении определения правонарушений, так как условие двойной подсудности должно быть соблюдено Сторонами при применении определенных процессуальных полномочий. В отношении количества заявлений ограничения не предусмотрены.

Положение о федеративных государствах (Статья 41)

316. Чтобы дать возможность как можно большему количеству стран стать Сторонами Конвенции, Статья 41 допускает оговорку, помогающую устранить трудности, с которыми могут столкнуться федеративные государства в результате характерного распределения власти между центральными и региональными органами. Вне сферы уголовного законодательства существуют прецеденты для

федеральных заявлений или оговорок в отношении международных соглашений[11]. Статья 41 признает, что в результате устоявшегося внутреннего законодательства и процессуальных норм Стороны, являющейся федеративным государством, могут возникнуть небольшие изменения в области применения. Эти изменения должны основываться на Конституции или иных основных принципах разделения полномочий в вопросах уголовного правосудия между центральной властью и территориальными единицами федеративного государства. Составители Конвенции пришли к согласию в том, что действие положения о федеративных государствах приведет лишь к небольшим изменениям в применении Конвенции.

317. Например, в США, согласно Конституции и основным принципам федерализма, федеральное уголовное законодательство обычно регулирует действия на основании их влияния на межштатную или внешнюю торговлю, в то время как вопросы минимальной или исключительно местной важности, как правило, регулируются штатами. Такой подход к федерализму, тем не менее, обеспечивает широкий охват незаконных деяний, включенных в данную Конвенцию согласно федеральному уголовному законодательству США, однако признает, что входящие в состав страны штаты должны регулировать деяния, имеющие небольшое

11. Например, Конвенция о статусе беженцев от 28 июля 1951, статья 34; Конвенция о статусе апатридов от 28 сентября 1954 г., статья 37; Конвенция о признании и приведении в исполнение иностранных арбитражных решений от 10 июня 1958 г., статья 11; Конвенция об охране всемирного культурного и природного наследия от 16 ноября 1972 г., статья 34.

воздействие или исключительно местный характер. В некоторых случаях в пределах небольшой категории деяний, регулируемых штатом, а не федеральным законом, штат может не обеспечить мер, которые в ином случае подпадали бы под действие Конвенции. Например, атака на отдельный персональный компьютер или сеть компьютеров, связанных друг с другом в одном здании, может быть преступной, если это предусмотрено законом штата, в котором она произошла. Однако такая атака становится федеральным правонарушением, если доступ к компьютеру произошел через Интернет, поскольку использование Интернета предусматривает достаточное для привлечения федерального законодательства воздействие на межштатную или внешнюю торговлю. Исполнение Конвенции через федеральный закон США или через закон другого федеративного государства в похожих обстоятельствах согласуется с требованиями Статьи 41.

318. Сфера применения положения о федеративных государствах ограничена положениями Главы II (материальное уголовное право, процессуальное право и юрисдикция). Федеративные государства, использующие это положение, тем не менее обязаны сотрудничать с другими Сторонами согласно Главе III, даже если штат или иная территориальная единица, в которых находится скрывающееся от правосудия лицо или доказательства, не рассматривает деяние как уголовное, или не имеет требуемых Конвенцией процедур.

319. Кроме того, пункт 2 Статьи 41 устанавливает, что федеративное государство, использующее оговорку согласно пункту 1 данной Статьи, не может применять условия такой оговорки для того, чтобы исключить или существенно

уменьшить свои обязательства по обеспечению мер, указанных в Главе II. В целом оно должно обеспечить широкие и эффективные действия правоохранительных органов. Что касается положений, применение которых подпадает под законодательную юрисдикцию штатов или иных территориальных единиц, федеральное правительство должно направить эти положения властям таких единиц, чтобы поощрить их к принятию соответствующих мер по их применению.

Оговорки (Статья 42)

320. Статья 42 предусматривает несколько возможностей для оговорок. Такой подход вызван тем, что Конвенция охватывает сферу уголовного и уголовно-процессуального законодательства, которая относительно нова для многих стран. Кроме того, глобальный характер Конвенции, которая будет открыта для стран – членов Совета Европы и не только, делает необходимой возможность таких оговорок. Их цель – способствовать тому, чтобы Сторонами Конвенции стали как можно больше стран, и в то же время позволить этим странам сохранить определенные подходы и понятия, согласующиеся с их внутренним законодательством. Также составители попытались ограничить возможность делать оговорки, чтобы в максимально возможной степени обеспечить соблюдение Конвенции Сторонами. Таким образом, могут быть сделаны только перечисленные оговорки. Кроме того, оговорки могут быть сделаны Стороной лишь в момент подписания или сдачи на хранение документа о ратификации, принятии, одобрении или присоединении.

321. Признавая, что для некоторых Сторон оговорки необходимы для избежания конфликта с их конституционными или основными юридическими принципами, Статья 43 не указывает конкретный период времени для снятия оговорок. Они должны быть сняты так скоро, как это позволяют обстоятельства.

322. Чтобы оказать некоторое давление на Стороны и заставить их хотя бы рассмотреть возможность снятия оговорок, Конвенция дает Генеральному Секретарю Совета Европы полномочия делать регулярные запросы в отношении перспективы снятия. Возможность таких запросов является существующей практикой согласно нескольким документам Совета Европы. Таким образом, Стороны получают возможность указать, требуется ли им сохранение оговорок в отношении некоторых положений, и снять впоследствии те, которые им больше не нужны. Можно надеяться, что с течением времени Стороны смогут снять как можно больше своих оговорок, чтобы обеспечить единообразное соблюдение Конвенции.

Поправки (Статья 44)

323. Прецедент для Статьи 44 имеется в Конвенции об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности (СЕД № 141), где он стал новшеством в отношении конвенций об уголовном праве, разработанных в рамках Совета Европы. Процедура внесения поправок предназначена в основном для относительно небольших изменений процессуального и технического характера. Составители сочли, что значительные изменения в Конвенции могут быть сделаны в виде дополнительных протоколов.

324. Стороны могут самостоятельно изучить необходимость внесения поправок или протоколов согласно процедуре консультации, описанной в Статье 46. Стороны должны периодически информировать об этом Европейский Комитет по проблемам преступности (ЕКПП), чтобы он при необходимости содействовал Сторонам в их усилиях по изменению и дополнению Конвенции.

325. В соответствии с пунктом 5, любая принятая поправка вступает в силу только с момента уведомления Сторонами Генерального Секретаря о ее принятии. Это требование обеспечит единообразное развитие Конвенции.

Урегулирование споров (Статья 45)

326. Пункт 1 Статьи 45 предусматривает, что Европейский комитет по проблемам преступности (ЕКПП) должен получать информацию об интерпретации и применении положений Конвенции. Пункт 2 обязывает Стороны добиваться мирного разрешения любого спора, касающегося интерпретации или применения Конвенции. Любая процедура по разрешению споров должна быть согласована заинтересованными Сторонами. Данное положение предлагает три возможных механизма для разрешения споров: Европейский комитет по проблемам преступности (ЕКПП), арбитражный суд или Международный Суд.

Консультации Сторон (Статья 46)

327. Статья 46 создает рамки для консультаций Сторон в отношении применения Конвенции, эффекта значительных правовых, стратегических или технологических нововведений,

относящихся к преступлениям, совершенным с использованием компьютера, и к сбору доказательств в электронной форме, а также возможности вносить дополнения и поправки в Конвенцию. Консультации должны особо изучать вопросы, возникающие в процессе использования и применения Конвенции, включая результаты заявлений и оговорок, сделанных согласно Статьям 40 и 42.

328. Данная процедура является достаточно гибкой и предоставляет Сторонам решать, как и когда собираться для консультаций. Составители Конвенции сочли такую процедуру необходимой для того, чтобы все Стороны Конвенции (включая страны – не члены СЕ) были на равных основаниях задействованы в любых последующих механизмах, сохраняя в то же время полномочия Европейского Комитета по проблемам преступности (ЕКПП). Комитет должен не только регулярно получать информацию о консультациях между Сторонами, но и оказывать им содействие и необходимую помощь в их усилиях по внесению дополнений или поправок в Конвенцию. С учетом необходимости эффективного предотвращения и наказания преступлений, связанных с применением компьютера, а также связанных с ним вопросов конфиденциальности, потенциального воздействия на предпринимательскую деятельность и других важных факторов, полезными для таких консультаций могут оказаться суждения заинтересованных сторон, включая правоохранительные органы, неправительственные организации и частный бизнес (см. также пункт 14).

329. Пункт 3 предусматривает пересмотр действия Конвенции через три года после ее вступления в силу, с внесением при необходимости соответствующих поправок.

Европейский Комитет по проблемам преступности должен провести такой пересмотр в сотрудничестве со Сторонами.

330. Пункт 4 указывает, что финансирование консультаций производится Сторонами согласно пункту 1 Статьи 46, за исключением случаев, когда расходы берет на себя Совет Европы. Однако помимо Европейского комитета по проблемам преступности (ЕКПП), помощь Сторонам по вопросам, связанным с Конвенцией, оказывает также Секретариат Совета Европы.

Дополнительный протокол к Конвенции о преступлениях в сфере компьютерной информации, об инкриминировании расистских актов и совершенного ксенофоба при помощи информационных систем. Страсбург, 28 января 2003 года

Государства-члены Совета Европы и другие государства–стороны Конвенции о преступлениях в сфере компьютерной информации, открытой к подписанию в Будапеште 23 ноября 2001 года, подписавшие настоящий Протокол,

Считая, что целью Совета Европы является достижение большего единства между его членами;

Напоминая, что все люди рождены свободными и равными в правах и достоинстве;

Подчеркивая необходимость обеспечения полной и эффективной реализации всех прав человека без дискриминации или различий, как закреплено в Европейских и других документах;

Будучи убеждены, что действия, связанные с проявлением расизма и ксенофобии, нарушают права человека и угрожают нормам закона и демократической стабильности;

Считая, что внутреннему и международному законодательству необходимо обеспечить адекватные законные ответные

меры в борьбе против пропаганды расизма и ксенофобии, проводимой посредством компьютерных систем;

Зная о том, что пропаганда таких действий часто является причиной введения уголовной ответственности в национальном законодательстве;

Принимая во внимание Конвенцию о преступлениях в сфере компьютерной информации, которая предусматривает современные и гибкие средства международного сотрудничества, и будучи убежденными в необходимости гармонизации действующих положений законодательства, касающихся борьбы против пропаганды расизма и ксенофобии;

Зная, что компьютерные системы предлагают беспрецедентные средства упрощения свободы высказываний и общения на земном шаре;

Признавая, что свобода высказываний образует одну из необходимых основ демократического общества и является одним из основных условий для его прогресса и для развития каждого человека;

Обеспокоенные, тем не менее, риском ненадлежащего использования и злоупотребления имеющимися компьютерными системами для пропаганды расизма и ксенофобии;

Заботясь о необходимости обеспечить должное равновесие между свободой выражения и эффективной борьбой против действий, связанных с проявлением расизма и ксенофобии;

Признавая, что настоящий Протокол не затрагивает установленные принципы, касающиеся свободы высказываний в национальных юридических системах;

Принимая во внимание соответствующие международные юридические документы в этой области и в частности Конвенцию о защите прав человека и основных свобод и Протокол № 12 к ней относительно общего запрещения дискриминации, существующие конвенции Совета Европы о сотрудничестве в правовой области и в частности Конвенцию о преступлениях в сфере компьютерной информации, Международную Конвенцию Организации Объединенных Наций об уничтожении всех форм расовой дискриминации от 21 декабря 1965 года, Совместную Акцию Европейского Союза от 15 июля 1996 года, принятую Советом на основании статьи К.3 Договора о Европейском Союзе, относительно действий по борьбе с расизмом и ксенофобией;

Приветствуя недавние события, которые способствуют дальнейшему международному взаимопониманию, и сотрудничество в борьбе с преступлениями в сфере компьютерной информации, расизмом и ксенофобией;

Принимая во внимание План Действий, принятый Главами государств и Правительств Совета Европы по случаю их второй встречи на высшем уровне (Страсбург, 10-11 октября 1997 года) по поиску общих ответных мер на развитие новых технологий, базирующихся на стандартах и ценностях Совета Европы;

Согласились о нижеследующем:

Глава I – Общие положения

Статья 1 – Цель

Целью настоящего Протокола является дополнение Сторонами Протокола положений Конвенции о

преступлениях в сфере компьютерной информации, открытой для подписания в Будапеште 23 ноября 2001 года (далее именуемой «Конвенция»), в отношении введения уголовной ответственности за правонарушения, связанные с проявлением расизма и ксенофобии, совершенные посредством компьютерных систем.

Статья 2 – Определение

1. Для целей настоящего Протокола:

«расистские и ксенофобские материалы» означают любые письменные материалы, любое изображение или любое другое представление идей или теорий, которые пропагандируют, способствуют или подстрекают к ненависти, дискриминации или насилию против любой личности или группы лиц, если в качестве предлога к этому используются факторы, основанные на расе, цвете кожи, национальном или этническом происхождении, а также религии.

2. Термины и выражения, используемые в настоящем Протоколе, толкуются так же, как они толкуются согласно Конвенции.

Глава II – Меры принимаемые на национальном уровне

Статья 3 – Распространение расистских и ксенофобских материалов посредством компьютерных систем

1. Каждая Сторона принимает такие законодательные и иные меры, которые могут потребоваться для того, чтобы

квалифицировать в качестве уголовных преступлений в соответствии с ее внутренним правом, когда это сделано умышленно и противоправно, следующее поведение:

распространение расистского и ксенофобского материала или обеспечение доступа к нему для общественности через компьютерные системы.

2. Сторона может сохранить за собой право не вводить уголовную ответственность за поведение, указанное в пункте 1 настоящей статьи, если материал, как определено в пункте 1 статьи 2, пропагандирует, способствует или подстрекает к дискриминации, не связанной с ненавистью или насилием, при условии доступности других эффективных средств защиты.

3. Несмотря на пункт 2 настоящей статьи, Сторона может сохранить за собой право не применять пункт 1 к случаям дискриминации, для которых ввиду принципов, установленных в ее внутренней судебной системе относительно свободы высказываний, она не может обеспечить эффективные средства защиты, как упомянуто в пункте 2 настоящей статьи.

Статья 4 – Мотивированная угроза расизма и ксенофобии

Каждая Сторона принимает такие законодательные и иные меры, которые могут потребоваться для того, чтобы квалифицировать в качестве уголовных преступлений в соответствии с ее внутренним правом, когда это сделано умышленно и противоправно, следующее поведение:

угроза через компьютерную систему совершения серьезного уголовного преступления, как определено ее внутренним правом, в отношении (i) лиц по причине того, что они принадлежат к группе, отличной по расе, цвету кожи, национальному или этническому происхождению, а также религии, или (ii) группы лиц с учетом этих факторов.

Статья 5 – Расистское и ксенофобское мотивированное оскорбление

1. Каждая Сторона принимает такие законодательные и иные меры, которые могут потребоваться для того, чтобы квалифицировать в качестве уголовных преступлений в соответствии с ее внутренним правом, когда это сделано умышленно и противоправно, следующее поведение:

публичное оскорбление через компьютерную систему (i) лиц по причине того, что они принадлежат к группе, отличной по расе, цвету кожи, национальному или этническому происхождению, а также религии, или (ii) группы лиц с учетом этих факторов.

2. Сторона может:

a. либо требовать того, чтобы преступление, упомянутое в пункте 1 настоящей статьи, имело результат того, что лицо или группа лиц, упомянутых в пункте 1, подвергнуты ненависти, презрению или осмеянию;

b. либо сохранить за собой право не применять, полностью или частично, пункт 1 настоящей статьи.

Статья 6 – Отрицание, чрезвычайная минимизация, одобрение или оправдание геноцида или преступлений против человечества

1. Каждая Сторона принимает такие законодательные меры, которые могут потребоваться для того, чтобы квалифицировать в качестве уголовных преступлений в соответствии с ее внутренним правом, когда это сделано умышленно и противоправно следующее поведение:

распространение или обеспечение доступа для общественности через компьютерную систему материала, который полностью отрицает или чрезвычайно умаляет отрицательные последствия, одобряет или оправдывает действия, являющиеся геноцидом или преступлениями против человечества, как определено международным правом и как это признано окончательными и обязательными решениями Международного Военного Трибунала, образованного в соответствии с Лондонским Соглашением от 8 августа 1945 года, или любого другого международного суда, образованного согласно соответствующим международным документам и юрисдикция которых признана Стороной.

2. Сторона может :

a. или требовать того, чтобы отрицание или чрезвычайное умаление отрицательных последствий, упомянутые в пункте 1 настоящей статьи, совершены с намерением подстрекать к ненависти, дискриминации или насилию против любого лица или группы лиц, если в качестве предлога к этому используются факторы, основанные на расе, цвете кожи, национальном или этническом происхождении, а также религии;

b. или сохранить за собой право не применять полностью или частично пункт 1 настоящей статьи.

Статья 7 – Пособничество и подстрекательство

Каждая Сторона принимает такие законодательные и иные меры, которые могут потребоваться для того, чтобы квалифицировать в качестве уголовных преступлений в соответствии с ее внутренним правом, когда это сделано умышленно и противоправно, пособничество или подстрекательство к совершению преступлений, квалифицированных в соответствии с настоящим Протоколом, с намерением совершения такого преступления.

Глава III – Связь между настоящим Протоколом и Конвенцией

Статья 8 – Связь между настоящим Протоколом и Конвенцией

1. Статьи 1, 12, 13, 22, 41, 44, 45 и 46 Конвенции применяются, *mutatis mutandis*, к настоящему Протоколу.

2. 2. Стороны увеличивают сферу применения мер, определенных в статьях 14 - 21 и статьях 23 - 35 Конвенции статьями 2 - 7 настоящего Протокола.

Глава IV – Заключительные положения

Статья 9 – Выражение согласия принять на себя обязательства

1. Настоящий Протокол открыт для подписания Государствами, подписавшими Конвенцию, которые могут выразить согласие принять на себя обязательства путем:

a. либо подписания без оговорки относительно ратификации, принятия или одобрения; или

b. либо подписания с оговоркой относительно ратификации, принятия или одобрения с последующей ратификацией, принятием или одобрением.

2. Государство не может подписать настоящий Протокол без оговорки относительно ратификации, принятия или одобрения либо сдать на хранение грамоту о ратификации, документ о принятии или одобрении, если оно предварительно или одновременно не сдало на хранение грамоту о ратификации, документ о принятии или одобрении Конвенции.

3. Грамоты о ратификации, документы о принятии или одобрении сдаются на хранение Генеральному секретарю Совета Европы.

Статья 10 – Вступление в силу

1. Настоящий Протокол вступает в силу в первый день месяца, следующего за истекшим трехмесячным периодом считая с даты, когда пять Государств выразят согласие принять на себя обязательства, вытекающие из настоящего Протокола, в соответствии с положениями статьи 9.

2. Для тех Государств, которые в последующем выразят свое согласие принять на себя обязательства по настоящему Протоколу, он вступает в силу в первый день месяца, следующего за истекшим трехмесячным периодом, считая с даты его подписания без оговорки относительно ратификации, принятия или одобрения либо сдачи на хранение грамоты о ратификации, документа о принятии или одобрении.

Статья 11 – Присоединение

1. После вступления в силу настоящего Протокола любое Государство, присоединившееся к Конвенции, может также присоединиться к настоящему Протоколу.

2. Присоединение осуществляется посредством сдачи на хранение Генеральному секретарю Совета Европы документа о присоединении, который вступает в силу в первый день месяца, следующего за истекшим трехмесячным периодом, считая с даты его сдачи на хранение.

Статья 12 – Оговорки и заявления

1. Оговорки и заявления, сделанные Сторонами в отношении положения Конвенции, также применяются к Протоколу, если Сторона не заявит об ином при подписании или сдаче на хранение ратификационной грамоты, документа о принятии, одобрении или присоединении.

2. Путем направления письменного уведомления на имя Генерального секретаря Совета Европы любая Сторона может при подписании или сдаче на хранение ратификационной грамоты, документа о принятии, одобрении или присоединении, заявить, что она воспользуется оговоркой (оговорками), предусмотренной статьями 3, 5 и 6 настоящего Протокола. В то же время Сторона может воспользоваться в отношении положений настоящего Протокола, оговоркой (оговорками), предусмотренной пунктом 2 статьи 22 и пунктом 1 статьи 41 Конвенции, независимо от выполнения, сделанного Стороной согласно Конвенции. Никаких других оговорок не может быть сделано.

3. Путем направления письменного уведомления на имя Генерального секретаря Совета Европы любая Сторона может при подписании или сдаче на хранение ратификационной грамоты, документа о принятии, одобрении или присоединении заявить, что она воспользуется возможностью требования дополнительных признаков, как предусмотрено пунктом 2.a статьи 5 и пунктом 2.a статьи 6 настоящего Протокола.

Статья 13 – Статус и отзыв оговорки

1. Сторона, сделавшая оговорку в соответствии со статьей 12 настоящего Протокола, отзывает такую оговорку, полностью или частично, так скоро, как того позволят обстоятельства. Такой отзыв вступает в силу с даты получения письменного уведомления, направленного на имя Генерального секретаря Совета Европы. Если в таком уведомлении указано, что отзыв оговорки должен вступить в силу с даты, указанной в нем, и такая дата наступит позже получения такого уведомления Генеральным секретарем Совета Европы, отзыв вступает в силу с этой более поздней даты.

2. Генеральный секретарь Совета Европы может периодически осведомляться у Сторон, которые сделали одну или несколько оговорок в соответствии со статьей 12 настоящего Протокола, о перспективах отзыва таких оговорок.

Статья 14 – Территориальное применение

1. Любое Государство может во время подписания или при сдаче на хранение своей ратификационной грамоты или документа о принятии, одобрении или присоединении

указать территорию или территории, на которые распространяется действие настоящего Протокола.

2. Любое Государство может в любое время впоследствии путем направления заявления на имя Генерального секретаря Совета Европы распространить действие настоящего Протокола на любую другую указанную в заявлении территорию. Для такой территории настоящий Протокол вступает в силу в первый день месяца, следующего за истекшим трехмесячным периодом, считая с даты получения такого заявления Генеральным секретарем Совета Европы.

3. Любое заявление, сделанное в соответствии с двумя предыдущими пунктами, в отношении любой территории, указанной в таком заявлении, может быть отозвано путем направления уведомления на имя Генерального секретаря Совета Европы. Такой отзыв вступает в силу в первый день месяца, следующего за истекшим трехмесячным периодом, считая с даты получения такого уведомления Генеральным секретарем Совета Европы.

Статья 15 – Денонсация

1. Любая Сторона может в любое время денонсировать настоящий Протокол посредством направления уведомления на имя Генерального секретаря Совета Европы.

2. Такая денонсация вступает в силу в первый день месяца, следующего за истекшим трехмесячным периодом считая с даты получения уведомления Генеральным секретарем Совета Европы.

Статья 16 – Уведомления

Генеральный секретарь Совета Европы уведомляет Государства-члены Совета Европы, Государства, не являющиеся членами Совета Европы, которые участвовали в разработке настоящего Протокола, а также любое Государство, присоединившееся к настоящему Протоколу, или которому было предложено присоединиться к нему:

a. о любом подписании;

b. о сдаче на хранение любой ратификационной грамоты или любого документа о принятии, одобрении или присоединении;

c. о любой дате вступления в силу настоящего Протокола в соответствии со статьями 9, 10 и 11;

d. о любом ином акте, уведомлении или сообщении, относящихся к настоящему Протоколу.

В удостоверение чего нижеподписавшиеся, должным образом на то уполномоченные, подписали настоящий Протокол.

Совершено в Страсбурге 28 января 2003 года на английском и французском языках, причем оба текста имеют одинаковую силу, в единственном экземпляре, который хранится в архиве Совета Европы. Генеральный Секретарь Совета Европы направляет заверенную копию каждому Государству-члену Совета Европы, Государствам, не являющимся членами Совета Европы, участвовавшим в разработке настоящего Протокола, и любому Государству, которому было предложено присоединиться к Конвенции.

Пояснительный доклад

Текст данного пояснительного доклада не является документом, обеспечивающим авторитетное толкование Протокола, хотя при этом данный документ и может способствовать соблюдению содержащихся в Протоколе положений. Данный Протокол был открыт для подписания в Страсбурге 28 января 2003 года по случаю первой части сессии Парламентской Ассамблеи 2003 года.

Введение

1. После принятия в 1948 году Всеобщей декларации прав человека международное сообщество проделало значительный прогресс в борьбе с расизмом, расовой дискриминацией, ксенофобией и связанной с ними нетерпимостью. Были приняты национальные и международные законы, а также ряд международных документов в области прав человека, в частности, при этом необходимо упомянуть Нью-йоркскую международную Конвенцию 1966 года о ликвидации всех форм расовой дискриминации, заключенную в рамках ООН (КЛРД). И хотя был достигнут прогресс, стремление к миру, свободному от расовой ненависти и предвзятости, по-прежнему реализовано лишь частично.

2. Притом что технологическое, коммерческое и экономическое развитие сближает народы мира, тем не менее, расовая дискриминация, ксенофобия и другие формы нетерпимости по прежнему существуют в наших обществах. Глобализация создает риски, которые могут привести к

изоляции и ко все большему неравенству, весьма часто по расовым и этническим признакам.

3. В частности, появление международных сетей коммуникаций, таких как Интернет, дает некоторым лицам современные и мощные средства оказания поддержки расизму и ксенофобии и позволяет им легко и широко распространять заявления, содержащие подобные идеи. Для того чтобы проводить расследования и преследовать этих лиц, жизненно необходимо международное сотрудничество. Для обеспечения взаимной помощи в отношении преступлений, связанных с компьютерами, в широком смысле этого слова, причем гибко и на современной основе, и была подготовлена Конвенция о киберпреступности (СЕД 185), нижеименуемая "Конвенция". У данного Протокола двойная задача: во-первых, гармонизировать субстантивное уголовное право в борьбе против расизма и ксенофобии в Интернете, а во-вторых, совершенствовать международное сотрудничество в этой области. Подобный тип гармонизации способствует борьбе против таких преступлений на национальном и международном уровне. Соответствующие правонарушения в национальном законодательстве могут предупреждать злоупотребления компьютерными системами в расистских целях в Государствах-Сторонах, чьи законы в этой области имеют менее определенный характер. С учетом этого могут быть усилены и полезные обмены взаимным опытом по практическому регулированию подобных дел. Оказывается содействие международному сотрудничеству (прежде всего экстрадиции и взаимной правовой помощи), в том числе и в связи с требованиями «двойной криминализации».

4. Комитет, разрабатывавший Конвенцию, обсуждал возможность включения других правонарушений, связанных с контентом, таких как распространение расистской пропаганды через компьютерные системы. При этом Комитет не смог достичь консенсуса по вопросу об уголовной ответственности за такие действия. Притом что имелась значительная поддержка включению подобных деяний в качестве уголовного правонарушения, некоторые делегации выразили серьезную обеспокоенность в связи с включением такого положения с учетом свободы выражения мнения. Притом что отмечалась сложность этого вопроса, было решено, что Комитет передаст вопрос о подготовке Дополнительного протокола к Конвенции на рассмотрение Европейского комитета по уголовным проблемам (CDPC).

5. Парламентская Ассамблея в своем заключении 226(2001) в отношении Конвенции рекомендовала незамедлительно подготовить Протокол к Конвенции под заголовком "Расширение сферы действия Конвенции для включения новых форм правонарушений" с целью определения и установления уголовной ответственности, в том числе за распространение расисткой пропаганды.

6. Исходя из этого, Комитет министров поручил Европейскому комитету по уголовным проблемам (CDPC) и, в частности, ее Комитету экспертов по установлению уголовной ответственности за акты расизма и ксенофобного характера, совершаемые через компьютерные системы (PC-RX), подготовить проект Дополнительного протокола как обязывающий юридический документ, открытый для подписания и ратификации

Договаривающимися Сторонами в Конвенции, в котором, в частности, будет содержаться следующее:

i. определение и сфера действия аспектов по установлению уголовной ответственности за акты расизма и ксенофобского характера, совершаемые через компьютерные сети, в том числе производство, предложение, распространение или иные формы распространения материалов или посланий с подобным содержанием через компьютерные сети;

ii. степень применения субстантивных, процессуальных положений, а также положений в области международного сотрудничества в рамках Конвенции о киберпреступности к расследованию и преследованию правонарушений, определенных в соответствии с Дополнительным протоколом.

7. Данный Протокол предусматривает расширение сферы действия Конвенции, в том числе применение субстантивных, процессуальных положений, а также положений в области международного сотрудничества, таким образом, чтобы охватить также правонарушения расистской и ксенофобской пропаганды. Таким образом, помимо гармонизации аспектов субстантивного права в отношении подобного поведения, цель Протокола состоит в том, чтобы расширить возможности Сторон использовать средства и формы международного сотрудничества, предусмотренные в Конвенции в данной сфере.

Комментарии по статьям Протокола

Глава I – Общие положения

Статья 1 – Цель

8. Цель настоящего Протокола состоит в том, чтобы дополнить между Сторонами в Протоколе положения Конвенции, в том что касается уголовной ответственности за акты расистского и ксенофобного характера, совершенные через компьютерные системы.

9. Положения Протокола имеют обязывающий характер. Для соблюдения этих обязательств Государства-Стороны должны не только принять соответствующее законодательство, но и обеспечивать его эффективное исполнение.

Статья 2 – Определение

Пункт 1 – «Расистские и ксенофобские материалы»

10. На международном и национальном уровне для борьбы с расизмом или ксенофобией был разработан ряд правовых документов. Составители данного Протокола учитывали, в частности i) Международную конвенцию о ликвидации всех форм расовой дискриминации (КЛРД), ii) Протокол № 12 (СЕД 177) к Конвенции о защите прав человека и основных свобод (ЕКПЧ), iii) Совместную деятельность от 15 июля 1996 года Европейского Союза, принятую Советом на основе статьи К.3 к Договору о Европейском Союзе в отношении деятельности по борьбе с расизмом и ксенофобией, iv) Всемирную конференцию против расизма, расовой дискриминации, ксенофобии и связанной с этим

нетерпимостью (Дурбан, 31 августа – 8 сентября 2001 года), v) выводы Европейской конференции против расизма (Страсбург, 13 октября 2000 года), vi) комплексное исследование, опубликованное Комиссией Совета Европы против расизма и ксенофобии (ЕКРИ), опубликованное в августе 2000 года (CRI(2000)27), и vii) Предложение от ноября 2001 года со стороны Европейской комиссии о Рамочном решении Совета о борьбе с расизмом и ксенофобией (в рамках Европейского Союза).

11. В статье 10 ЕКПЧ признается право на свободу выражения мнения, что включает свободу на то, чтобы придерживаться мнений и получать и распространять информацию и идеи. "Статья 10 ЕКПЧ применима к той информации и идеям, которые благоприятно воспринимаются или рассматриваются как безвредные или которые воспринимаются с безразличием, но также и те, которые оскорбляют, шокируют или вызывают возмущение у государства или какой-то группы населения»[1]. При этом Европейский суд по правам человека полагает, что действия государства, направленные на ограничение права на свободу выражения мнения, должны быть должным образом обоснованы с учетом ограничений пункта 2 статьи 10 ЕКПЧ, в частности, когда такие идеи или выражения мнений нарушают права других. Данный Протокол на основе национальных и международных документов устанавливает, в какой мере распространение расистских и ксенофобских идей нарушает права других лиц.

1. См. в этом контексте, например, постановление по делу Хендисайд (Handyside) от 7 декабря 1976 года, Серия A, № 24, стр. 23, пункт 49

12. Определение, содержащееся в статье 2, относится к печатным материалам (например, документам, книгам, журналам, заявлениям, посланиям и т.д.), изображениям (например, картинам, фотографиям, рисункам или т.д.) или иному выражению мыслей или теорий расистского и ксенофобского характера в таком формате, который может быть сохранен, обработан и передан средствами компьютерной системы.

13. Определение, содержащееся в статье 2 данного Протокола, относится к определенному поведению, к которому может привести содержание определенного материала, а не к выражению чувств/верований/отвращения, как это содержится в соответствующем материале. Определение строится в максимально возможной степени на существующих национальных и международных определениях (ООН, ЕС), а также на соответствующих документах.

14. Определение требует, чтобы такой материал пропагандировал, способствовал или подстрекал к ненависти, дискриминации или насилию. "Пропагандировал" относится к призывам к ненависти, дискриминации или насилию, "способствовал" – относится к содействию или продвижению ненависти, дискриминации или насилия, а "подстрекал" – относится к призыву других лиц к ненависти, дискриминации или насилию.

15. Термин "насилие" относится к незаконному использованию силы, а термин "ненависть" относится к сильной неприязни или враждебности.

16. При толковании термина "дискриминация" необходимо учитывать ЕКПЧ (статью 14 и Протокол 12), а также

соответствующую прецедентную практику и статью 1 КЛРД. Запрет дискриминации, содержащийся в ЕКПЧ, гарантирует каждому, находящемуся под юрисдикцией государства-стороны, равенство в соблюдении прав и свобод, защищаемых на основании самой ЕКПЧ. Статья 14 ЕКПЧ предусматривает общее обязательство для государств, дополняющее права и свободы, предусмотренные в ЕКПЧ. В этом контексте термин "дискриминация", используемый в Протоколе, относится к дифференцированному необоснованному обращению с лицами или группой лиц на основе определенных характеристик. В ряде постановлений (таких как по бельгийскому лингвистическому делу, делу Абдалазиз, Кабалес и Балкандали[2]), Европейский суд по правам человека заявлял, что «различие в обращении является дискриминационным, если оно «не имеет под собой объективных или разумных обоснований», то есть не преследует «законной цели» или же не существует «разумного взаимоотношения соразмерности между применявшимися мерами и поставленной целью». Является ли обращение дискриминационным или же нет – это рассматривается с учетом конкретных обстоятельств дела. Рекомендации о толковании термина «дискриминация» можно найти также в статье 1 КЛРД, в которой термин «расовая дискриминация» определяется как "любое различие, исключение, ограничение или предпочтение, основанное на признаках расы, цвета кожи, родового, национального или этнического происхождения, имеющие

2. Постановление по делу "Абулазиз, Кабалес и Балкандали" (Abulaziz, Cabales and Balkandali) от 28 мая 1985 года, Серия А № 94, стр. 32, пункт 62; Бельгийское лингвистическое дело, постановление от 23 июля 1968 года, Серия А № 6, стр. 34, пункт 10.

целью или следствием уничтожение или умаление признания, использования или осуществления на равных началах прав человека и основных свобод в политической, экономической, социальной, культурной или любых других областях общественной жизни".

17. Ненависть, дискриминация или насилие должны быть направлены на какое-либо лицо или группу лиц на основании того, что они принадлежат к группе, отличающейся по признаку "расы, цвета кожи, родового, национального или этнического происхождения, а также религии, если это используется как предлог в отношении любого из этих факторов».

18. Следует отметить, что эти признаки не совсем такие, как основания, содержащиеся, например, в статье 1 Протокола № 12 ЕКПЧ, поскольку некоторые из тех признаков, которые содержатся там, не относятся к расизму или ксенофобии. Основания, содержащиеся в статье 2 Протокола, также не идентичны тем, которые содержатся в КЛРД, поскольку в ней рассматривается "расовая дискриминация" в целом, а не "расизм" как таковой. В целом эти основания должны толковаться в таком их значении, как это установлено в национальном и международном праве и практике. Однако некоторые из них требуют дополнительного разъяснения, в том что касается их конкретного значения в контексте данного Протокола.

19. "Родовое происхождение" относится в основном к лицам или группам лиц, которые происходят от лиц, которые могут быть идентифицированы на основании определенных характеристик (таких как раса или цвет кожи),

но необязательно все эти характеристики по прежнему существуют. Несмотря на это, в силу своего родового происхождения, такие лица или группы лиц могут подвергаться ненависти, дискриминации или насилию. "Родовое происхождение" не относится к социальному происхождению.

20. Понятие "национальное происхождение" необходимо понимать в широком фактическом контексте. Это может относиться к истории отдельных лиц, не только в отношении их национальности или происхождения их предков, но и к их собственной национальной принадлежности, независимо от того, обладают ли они ей по-прежнему с юридической точки зрения. Когда лица имеют более чем одно гражданство или являются лицами без гражданства, то широкое толкование этого понятия призвано защищать их, если они подвергаются дискриминации по любому из этих оснований. Более того, понятие "национальное происхождение" может относиться не только к принадлежности к одной из стран, что признано в международном плане как таковое, но и к меньшинствам или к другим группам лиц с аналогичными характеристиками.

21. Понятие "религия" часто упоминается в международных документах и национальном законодательстве. Данный термин относится к убеждениям и верованиям. Включение данного термина как такового в определение подразумевало бы риск выхода за сферу действия данного Протокола. При этом религия может использоваться как предлог, алиби или замена других факторов, перечисленных в данном определении. "Религия", исходя из этого, должна толковаться именно в этом узком смысле слова.

Пункт 2

22. Предусматривая, что термины и выражения, используемые в данном Протоколе, должны толковаться аналогичным образом по сравнению с тем, как они толкуются на основании Конвенции, данная статья обеспечивает единое толкование обоих этих документов. Это означает, что термины и выражения, используемые в данном пояснительном докладе, должны толковаться таким же образом, как и термины и выражения толкуются в пояснительном докладе к Конвенции.

Глава II – Меры, которые необходимо принять на национальном уровне

Общие соображения

23. Правонарушения, установленные в данном Протоколе, содержат ряд общих аспектов, которые взяты из Конвенции. В целях ясности далее включены соответствующие положения пояснительного доклада к Конвенции.

24. Особенность предусмотренных правонарушений состоит в том, что имеются конкретные требования для определения того, что данное поведение осуществляется "неправомерно". Это отражает тот взгляд, что описываемое поведение не всегда наказывается как таковое, но может быть правовым или обоснованным только в тех случаях, когда применимы классические формы правовой защиты, такие как согласие, самооборона или необходимость, но где другие принципы или интересы приводят к исключению уголовной ответственности (например, в целях охраны

порядка, проведения научных работ или исследований). Выражение "неправомерное" исходит из того значения, в котором оно используется. Таким образом, не ограничивая то, как Стороны могут реализовывать эту концепцию в своем внутреннем праве, это может относиться к поведению, осуществляемому без полномочий (законодательных, административных, судебных, договорных или на основании согласия), или к поведению, которое в ином случае не охватывается установленными формами юридической защиты, оправданий, обоснований или соответствующих принципов на основании национального права. Исходя из этого, Протокол не затрагивает поведение, осуществляемое в соответствии с законными правительственными полномочиями (например, когда правительство Стороны действует для поддержания общественного порядка, защиты национальной безопасности или расследования уголовных преступлений). Кроме того, уголовная ответственность не может устанавливаться в отношении законных и общих действий, присущих характеру сетей или законной и общей деятельности или коммерческой практике. Сами Стороны должны определять, как реализовывать эти изъятия в своих национальных правовых системах (в рамках уголовного права или иным образом).

25. Для того чтобы наступала уголовная ответственность, все правонарушения, предусмотренные в Протоколе, должны совершаться "намеренно". В некоторых случаях частью правонарушения является дополнительный конкретный аспект намеренности. Составители Протокола, так же как и Конвенции, согласились в том, что точное понятие "намеренность" должно быть предметом национального толкования. Лица не могут подвергаться уголовной

ответственности в отношении какого-либо из правонарушений, предусмотренных данным Протоколом, если они не имели требуемого намерения. Например, недостаточно, чтобы провайдер услуг подвергался уголовной ответственности на основании этого положения, если такой провайдер услуг служил для доступа к веб-сайту или ньюз-рум или размещал их, притом что там содержался соответствующий материал, если у такого провайдера не было определенного намерения на основании национального права в данном конкретном случае. Более того, от провайдера услуг не требуется осуществлять мониторинг для того, чтобы избегать уголовной ответственности.

26. Что касается понятия "компьютерная система", то это такое же понятие, как и то, которое содержится в Конвенции и разъясняется в пунктах 23 и 24 пояснительного доклада к ней. Это составляет соблюдение статьи 2 данного Протокола (см. также выше пояснение к статье 2).

Статья 3 – Распространение расистских и ксенофобских материалов в компьютерной системе

27. Данная статья требует от Государств-Сторон устанавливать уголовную ответственность в связи с распространением или иным способом предоставления доступа к расистским и ксенофобским материалам публике через компьютерную систему. Сам акт распространения или предоставления доступа является уголовным только в том случае, если содержание также имеет расистский или ксенофобский характер.

28. "Распространение" относится к активному распространению расистских и ксенофобских материалов, как это определено в статье 2 Протокола, среди других лиц, в то время как "предоставление доступа" относится к размещению в Интернете расистских и ксенофобских материалов для использования другими лицами. Этот термин также призван охватить создание и подборку гиперссылок для того, чтобы облегчить доступ к таким материалам.

29. Термин "среди населения", используемый в статье 3, четко показывает, что частное общение или выражение мнений, сообщаемых или передаваемых через компьютерную систему, не подпадает под сферу действия данного положения. Действительно, такие средства коммуникации или выражения мнений, как традиционной формы корреспонденции, защищены на основании статьи 8 ЕКПЧ.

30. Сам факт того, рассматривается ли передача расистских и ксенофобских материалов как частная коммуникация или как распространение среди населения, определяется на основании обстоятельств конкретного случая. Прежде всего, что важно – это намерения посылающего сообщение в отношение того, чтобы оно было получено лишь определенным получателем. Наличие данного субъективного намерения может быть установлено на основе ряда объективных факторов, таких как содержание сообщения, используемая технология, применяемые меры безопасности и тот контекст, в котором было послано данное сообщение. Когда такие сообщения направляются одновременно более чем одному получателю, то количество получателей и характер отношений между отправителем и получателем/получателями являются тем

фактором, который определяет, следует ли рассматривать данное общение как частное.

31. Обмен расистскими и ксенофобскими материалами в чатах, размещение аналогичных посланий в новостных группах или на форумах для обсуждений является примером того, как подобные материалы становятся доступными населению. В этих случаях материалы доступны любому человеку. Даже тогда, когда материал потребует авторизации путем пароля, то материал доступен населению, когда такое разрешение дается каждому или любому человеку, который отвечает определенным критериям. Для того чтобы определить, являлся ли доступ или распространение публичным или нет, следует учитывать характер отношений между соответствующими лицами.

32. Пункты 2 и 3 включены для обеспечения возможности оговорок при весьма ограниченных обстоятельствах. Это необходимо рассматривать в сочетании и последовательно. Поэтому, Сторона, во-первых, имеет возможность не предусматривать уголовную ответственность в связи с поведением, описанным в данной статье, в тех случаях, когда материалы пропагандируют, содействуют или подстрекают к дискриминации, но не связаны с ненавистью или насилием, при условии, что имеются другие эффективные средства правовой защиты. Например, такие средства могут быть гражданскими или административными. В тех случаях, когда Сторона не может, в связи с установленными принципами своей правовой системы в области свободы выражения мнения, обеспечивать такие средства, она может оставить за собой право не осуществлять обязательство на основании пункта 1

данной статьи, при условии, что это касается только пропаганды, содействия или подстрекательства к дискриминации, которая не связана с ненавистью или насилием. Сторона может также ограничить сферу действия оговорки требованием о том, что дискриминация, например, должна быть оскорбительной, вызывать унижение или создавать угрозу для группы лиц.

Статья 4 – Угроза, мотивированная расизмом и ксенофобией

33. В законодательстве большинства стран предусматривается уголовная ответственность за угрозу в целом. Составители согласились подчеркнуть в Протоколе то, что, вне всякого сомнения, в отношении угроз расистского и ксенофобского характера должна предусматриваться уголовная ответственность.

34. Понятие "угроза" может относиться к угрозе, которая создает страх у лиц, в отношении которых направлена угроза, которые пострадают от совершения серьезного уголовного преступления (например, затрагивающего жизнь, личную безопасность или целостность, серьезный ущерб собственности и т.д. самой жертвы или его родственников). На усмотрение Государств-Сторон оставляется право определять, что является серьезным уголовным преступлением.

35. В соответствии с этой статьей угроза должна быть направлена либо i) лицу на основании того, что он или она принадлежат к группе, отличающейся расовым происхождением, цветом кожи, родовым, национальным или

этническим происхождением, а также религией, если это используется как предлог в связи с любым из этих признаков, или же ii) группе лиц, которые отличаются в силу одной из этих характеристик. Нет ограничения в том, что угроза должна иметь публичный характер. Данная статья охватывает также угрозы через личные коммуникации.

Статья 5 – Оскорбления на почве расизма и ксенофобии

36. В статье 5 рассматривается вопрос публичного оскорбления лица или группы лиц в силу того, что они принадлежат или воспринимаются как принадлежащие к группе, отличающейся особыми характеристиками. Понятие "оскорбление" относится к оскорбительному, презрительному или бранному выражению, которое наносит ущерб чести или достоинству лица. Из самого выражения должно быть ясно, что это оскорбление направлено напрямую на оскорбляемое лицо, принадлежащее к этой группе. В отличие от угрозы, оскорбление, выраженное в частных коммуникациях, не охватывается данным положением.

37. Пункт 2(i) позволяет Сторонам требовать, чтобы такое поведение сказывалось в том, чтобы лицо или группа лиц не только потенциально, но и действительно подвергались ненависти, презрению или высмеиванию.

38. Пункт 2(ii) позволяет Сторонам принимать оговорки, которые идут дальше, даже приводя к тому, что пункт 1 к ним не применяется.

Статья 6 – Отрицание, грубое преуменьшение, одобрение или оправдание геноцида или преступлений против человечности

39. В последние годы национальные суды рассматривали разные дела, в которых лица (публично, в СМИ и т.д.) выражали идеи или теории, направленные на отрицание, грубое преуменьшение, одобрение или оправдание серьезных преступлений, которые имели место, в частности во время Второй мировой войны (особенно Холокоста). Такие формы поведения часто оправдываются предлогом проведения научных исследований, при том что в действительности это направлено на поддержание и продвижение политических оснований, которые привели к Холокосту. Более того, такие формы поведения вдохновляли или даже стимулировали и поощряли расистские и ксенофобские группы в их действиях, в том числе совершаемых через компьютерные системы. Выражение таких идей оскорбляет (память) тех лиц, которые стали жертвой этого зла, а также их родственников. Наконец, это угрожает достоинству человеческого сообщества.

40. Эта проблема рассматривается в статье 6, которая имеет такую же структуру, как и статья 3. Составители Протокола согласились в том, что важно предусматривать уголовную ответственность за выражение мнений, которые отрицают, грубо преуменьшают, одобряют или оправдывают акты, представляющие собой геноцид или преступления против человечности, как это определено в международном праве и признано таковым на основании окончательных и обязывающих решений Международного военного трибунала, созданного на основании Лондонского соглашения от 8 апреля 1945 года. Это связано с тем, что наиболее серьезные и

установленные действия, которые привели к геноциду и к преступлениям против человечности, имели место в период 1940-1945 годов. При этом составители Протокола признали, что с тех пор имели место другие случаи геноцида и преступлений против человечности, которые были во многом мотивированы теориями и идеями расистского и ксенофобского характера. Исходя из этого, составители Протокола сочли необходимым не ограничивать сферу действия этого положения лишь преступлениями, совершенными нацистским режимом во время Второй мировой войны и установленными как таковыми Нюрнбергским судом, но также рассмотрели и формы геноцида и преступлений против человечности, установленные другими международными судами, созданными после 1945 года на основании соответствующих международных правовых документов (таких как резолюции Совета Безопасности ООН, двусторонние договоры и т.д.). Такими судами могут, например, быть Международные уголовные трибуналы по бывшей Югославии, Руанде, Постоянный Международный уголовный суд. Данная статья позволяет также ссылаться на окончательные и обязывающие решения будущих международных судов в той мере, в какой юрисдикция такого суда признается Стороной, подписавшей данный Протокол.

41. Это положение призвано уточнить, что факты, в отношении которых была установлена историческая правда, не могут отрицаться, грубо преуменьшаться, одобряться или оправдываться для того, чтобы поддерживать эти отвратительные теории и идеи.

42. Европейский суд по правам человека четко разъяснил, что отрицание или пересмотр "четко установленных

исторических фактов – таких как Холокост – […] не подпадает под защиту статьи 10 в связи со статьей 17 ЕКПЧ" (см. в этой связи постановление по делу "Леидё и Исорни (Lehideux and Isorni) " от 23 сентября 1998 года)[3].

43. Пункт 2 статьи 6 позволяет Стороне либо i) требовать, на основании заявлений, что отрицание или серьезное преуменьшение, о которых говорится в пункте 1 статьи 6, совершены с намерением возбудить ненависть, дискриминацию или насилие в отношении лица или группы лиц, основываясь на расе, цвете кожи, родовом, национальном или этническом происхождении, а также религии, если это используется в качестве предлога в связи с любым из этих факторов, либо ii) использовать оговорку, позволяющую Стороне не применять – полностью или частично – данное положение.

Статья 7 – Пособничество и подстрекательство

44. Задача этой статьи – установить в качестве уголовного правонарушения содействие или подстрекательство при совершении любых из правонарушений, совершенных на основании статей 3-6. В отличие от Конвенции Протокол не содержит уголовной ответственности в связи с попыткой совершить предусмотренные в нем правонарушения, поскольку многие из видов поведения, в отношении которых предусмотрена уголовная ответственность, являются подготовительными по своей природе.

3. Постановление по делу Леидё и Исорни (Lehideux and Isorni) от 23 сентября 1998 года, Доклады 1998-VII, пункт 47

45. Ответственность возникает в связи с содействием или подстрекательством тогда, когда лицо, совершающее преступление, установленное на основании Протокола, получает помощь со стороны другого лица, которое также намеренно совершает преступление. Например, хотя передача расистских и ксенофобных материалов через Интернет требует помощи провайдера услуг в качестве канала информации, провайдер услуг, который не имеет преступных намерений, не может нести ответственность на основании данного раздела. Таким образом, для провайдера услуг не предусматривается обязанность активно осуществлять мониторинг контента для избежания уголовной ответственности на основании данного положения.

46. Так же как и все правонарушения, устанавливаемые в соответствии с данным Протоколом, содействие или подстрекательство должны совершаться намеренно.

Глава III – Отношения между Конвенцией и данным Протоколом

Статья 8 – Отношения между Конвенцией и данным Протоколом

47. В статье 8 рассматриваются взаимоотношения между Конвенцией и данным Протоколом. Это положение избегает включения ряда положений Конвенции в данный Протокол. Оно указывает, что некоторые из положений Конвенции применяются, mutatis mutandis, к данному Протоколу (например, в отношении дополнительной ответственности и санкций, юрисдикций и части заключительных положений). Пункт 2 напоминает Сторонам, что значение,

установленное в Конвенции, должно применяться к правонарушениям, предусмотренным в Протоколе. В целях ясности уточняются соответствующие статьи.

Глава IV – Заключительные положения

48. Положения, содержащиеся в данной Главе, в основном основаны на "Модели итоговых положений конвенций и соглашений, заключаемых в Совете Европы", которые были утверждены Комитетом министров на 314-ом заседании постоянных представителей в феврале 1980 года. Поскольку в статьях 9-16 либо используется стандартная формулировка модельных положений или же они основываются на долгосрочной договорной практике Совета Европы, они не вызывают необходимости в отдельных комментариях. Однако некоторые изменения стандартных положений или же некоторые новые положения требуют дополнительного разъяснения. В этом контексте отмечается, что модельные положения были приняты как необязывающий набор положений. Как указывается во введении к модельным положениям, "данные модельные заключительные положения призваны лишь облегчить задачу комитетов экспертов и избежать текстуальных расхождений, которые не были бы реально обоснованы. Данная модель ни в коем образе не является обязывающей и в отношении конкретных случаев могут применяться разные положения" (см. также в этом контексте пункты 304-330 пояснительного доклада к Конвенции).

49. В пункте 2 статьи 12 уточняется, что Стороны могут использовать оговорку, как это предусмотрено в статьях 3,5 и 6 данного Протокола. Никаких других оговорок сделано быть не может.

50. Данный Протокол открыт для подписания лишь для Сторон, подписавших Конвенцию. Протокол вступит в силу три месяца спустя после того, как пять Сторон в Конвенции выразят свое согласие на то, чтобы быть им связанными (статьи 9-10).

51. Конвенция позволяет сделать оговорки в отношении некоторых положений, которые, на основании соответствующего положения статьи 8 Протокола, могут влиять на обязательства Стороны также и на основании Протокола. Тем не менее, Сторона может уведомить Генерального секретаря, что она не будет применять эту оговорку в отношении содержания Протокола. Это изложено в пункте 2 статьи 12 Протокола.

52. При этом когда Сторона не использовала такую возможность оговорки на основании Конвенции, то ей может понадобиться ограничить свои обязательства в отношении правонарушений, предусмотренных Конвенцией. Пункт 2 статьи 12 позволяет Сторонам сделать это в отношении пункта 2 статьи 22 и пункта 1 статьи 41 Конвенции.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ КОМИТЕТА «T-CY»

(приняты на 8-м, 9-м и 12-м пленарных заседаниях комитета «T-CY»)

Введение

На проходившем в декабре 2012 года 8-м пленарном заседании комитета Конвенции о киберпреступности (сокращённо – комитет «T-CY») было принято решение об издании методических рекомендаций, направленных на содействие реализации положений будапештской Конвенции о компьютерных преступлениях (Конвенции о киберпреступности) и на повышение эффективности их применения на практике в свете изменений, происходящих в области права, политики и технического прогресса.[1]

Настоящие методические рекомендации отражают общее понимание сторонами конвенции того, как следует её применять.

В «Будапештской конвенции» используется «технически нейтральная терминология таким образом, чтобы определяющие правонарушения нормы материального уголовного права могли быть применимы к ныне существующим и будущим техническим средствам».[2] В результате новые виды вредоносных программ или же преступлений будут и в дальнейшем подпадать под действие этого международного юридического документа.

1. См. полномочия комитета «T-CY» (статья 46 «Будапештской конвенции»).
2. Пункт 36 пояснительного доклада, прилагаемого к «Будапештской конвенции».

Методическая рекомендация, касающаяся понятия «компьютерной системы» (принята на 8-м пленарном заседании комитета «T-CY»)

1. Введение

На своей первой встрече, состоявшейся в г. Страсбурге 20-21 марта 2006 года, члены комитета «T-CY» рассмотрели вопрос о сфере применения определения «компьютерной системы» (статья 1.a «Будапештской конвенции») в свете появления и развития новых видов технических средств, выходящих за рамки традиционных компьютерных систем на базе центральной или же настольной ЭВМ.

Со времён составления «Будапештской конвенции» был разработан целый ряд современных технических устройств, представленных новым поколением мобильных «умных» телефонов (так называемых «смартфонов»), карманных и планшетных компьютеров, а также других разновидностей оборудования, генерирующего, обрабатывающего и передающего данные. Соответственно, возникла необходимость обсудить вопрос о том, охватываются ли эти новые средства понятием «компьютерной системы» в том виде, в котором оно сформулировано в «Будапештской конвенции».

В 2006 г. комитет «T-CY» пришел к выводу о том, что определение «компьютерной системы», содержащееся в статье 1.a «Будапештской конвенции», распространяется на вышеперечисленные устройства.

В настоящей методической рекомендации излагается эта общая позиция сторон конвенции, нашедшая своё

отражение в докладе первой встречи комитета Конвенции о киберпреступности (документ T-CY(2006)11).

2. Статья 1.a Будапештской Конвенции о компьютерных преступлениях (ETS 185)

Текст конвенции

Статья 1 – Определения

Во исполнение конвенции:

a. термин «компьютерная система» означает любое устройство или группу взаимосвязанных или смежных устройств, одно или более из которых, работая в соответствии с заданной программой, осуществляет автоматизированную обработку данных;

Выдержка из пояснительного доклада к конвенции:

23. В соответствии с положениями конвенции, компьютерная система представляет собой устройство, состоящее из компьютерного оборудования (т. н. аппаратных средств) и программного обеспечения (т. н. программных средств) и разработанного для обработки цифровых данных в автоматическом режиме. Она может также выполнять операции по вводу данных, их выводу и хранению. Компьютерная система может работать автономно или же в составе компьютерной сети, состоящей из других подобных устройств. Термин «в автоматическом режиме» обозначает работу без прямого вмешательства человека. Под термином «обработка данных» имеется в виду обработка данных компьютерной системой в соответствии с заранее заданной программой.

«Компьютерная программа» представляет собой набор команд, выполняемых компьютером с целью достижения поставленной перед ним задачи. Компьютер может исполнять разные программы. Обычно компьютерная система состоит из различных устройств, которые можно разбить на процессор (или центральный процессор) и на периферийное (внешнее) оборудование. Таковое состоит из устройств, выполняющих ряд специализированных функций под управлением центрального процессора (это принтер, экран компьютера, устройства по считыванию/записи лазерных дисков и другие виды накопителей).

24. Компьютерная сеть состоит из двух и более связанных между собою компьютерных систем. Связь между ними может быть проводной/кабельной, беспроводной (например, осуществляться посредством радиоволн, инфракрасных лучей или по спутнику) или же обеспечиваться одновременно как проводными, так и беспроводными средствами. Географически компьютерная сеть может быть ограничена небольшой территорией (в таком случае, она называется «локальной компьютерной сетью», английское сокращение - LAN) или же охватывать значительный район (тогда она будет называться «компьютерной сетью широкого охвата», английское сокращение - WAN). Оба вида сетей могут быть связаны друг с другом. Интернет представляет собой глобальную компьютерную сеть, состоящую из множества взаимосвязанных сетей, использующих одинаковые протоколы обмена информацией. Существуют и другие разновидности компьютерных сетей, способных обеспечивать передачу цифровых данных между различными составляющими их компьютерными системами вне зависимости от того, подключены они к

интернету или нет. Компьютерные системы могут быть подключены к сети в качестве терминалов или же промежуточных звеньев, способствующих дальнейшей передаче информации по ним с целью обеспечения беспрепятственного обмена данными, что и является основной функцией сетей.

3. Позиция комитета «T-CY» по вопросу о сфере применения понятия «компьютерная система» (статья 1.a «Будапештской конвенции»)

В статье 1.a «Будапештской конвенции» «компьютерная система» определяется как любое «устройство или группа взаимосвязанных или смежных устройств, одно или более из которых, работая в соответствии с заданной программой, осуществляет автоматизированную обработку данных».

Члены комитета «T-CY» сходятся на том, что данное определение распространяется, например, на современные мобильные телефоны, являющиеся многофункциональными устройствами, способными, в частности, генерировать, обрабатывать и передавать данные. Среди выполняемых ими функций присутствуют такие как обеспечение доступа к интернету, рассылка электронных писем с приложениями, загрузка разного рода материалов и документов.

Равно, комитет «T-CY» признаёт, что устройства типа «электронных секретарей» (карманных персональных компьютеров) также генерируют, обрабатывают и передают данные вне зависимости от того, наделены ли они или нет возможностями беспроводной связи.

Комитет «T-CY» подчёркивает, что при выполнении вышеперечисленных функций таковые устройства производят

обработку «компьютерных данных» в соответствии с определением, данным в статье 1.b «Будапештской конвенции». Более того, комитет «T-CY» полагает, что одновременно ими генерируются «параметры передачи цифровых данных» в том смысле, в котором они определяются статьей 1.d конвенции.

Таким образом, производя обработку цифровых данных, они функционируют как «компьютерные системы» в смысле статьи 1.a «Будапештской конвенции».

Члены комитета «T-CY» сходятся на том, что всё это соответствует толкованию понятия «компьютерной системы», данному в пояснительном докладе «Будапештской конвенции», регламентирующей их использование в таком качестве.

4. Заключение комитета « T-CY »

Комитет «T-CY» согласен с тем, что определение «компьютерной системы», фигурирующее в статье 1.a «Будапештской конвенции», распространяется на появляющиеся современные виды технических средств, выходящие за рамки традиционных компьютерных систем на базе центральной или же настольной ЭВМ и представленные новым поколением мобильных «умных» телефонов (так называемых «смартфонов»), карманных и планшетных компьютеров и другими техническими средствами.

Методическая рекомендация о положениях «Будапештской конвенции», относящихся к «бот-сетями» (принята на 9-м пленарном заседании комитета «T-CY»)

1. Введение

На проходившем в декабре 2012 года 8-м пленарном заседании комитета Конвенции о киберпреступности (сокращённо – комитет «T-CY») было принято решение об издании методических рекомендаций, направленных на содействие реализации положений будапештской Конвенции о компьютерных преступлениях и на повышение эффективности их применения на практике в свете изменений, происходящих в области права, политики и технического прогресса.[1]

Настоящие методические рекомендации отражают общее понимание сторонами конвенции того, как следует её применять.

Данная рекомендация касается вопроса так называемых «бот-сетей».

В «Будапештской конвенции» используется «технически нейтральная терминология таким образом, чтобы определяющие правонарушения нормы материального уголовного права могли быть применимы к ныне существующим и будущим техническим средствам».[2] В результате новые виды

1. См. полномочия комитета «T-CY» (статья 46 «Будапештской конвенции»).
2. Пункт 36 пояснительного доклада, прилагаемого к «Будапештской конвенции».

вредоносных программ или же преступлений будут и в дальнейшем подпадать под действие данного международного юридического документа.

В этой методической рекомендации показывается, как различные статьи Конвенции о компьютерных преступлениях применяются в борьбе с «бот-сетями».

2. Положения будапештской Конвенции о компьютерных преступлениях, относящиеся к рассматриваемому вопросу (ETS 185)

Под термином «бот-сеть» понимается:

> «сеть компьютеров, заражённых вредоносными программами (компьютерными вирусами). Такая сеть инфицированных («зомбированных») компьютеров может быть задействована для проведения целенаправленных действий против компьютерных систем («кибератак»). «Зомбированные» компьютеры - часто без ведома их пользователей - могут управляться с другого компьютера. Такой «управляющий» компьютер известен также под названием «центра управления и контроля».[3]

Организаторы такой сети взаимосвязанных компьютеров могут преследовать как преступные, так и созидательные цели.[4] Таким образом, факт построения «бот-сети» из ряда взаимосвязанных ЭВМ сам по себе второстепенен. Наиболее

---

3. Проект Директивы Европейского парламента и Совета Евросоюза об атаках на информационные системы, отменившей одноимённое рамочное соглашение Совета министров ЕС 2005/222/JHA (com (2010) 517 final).

4. Компьютерные сети могут умышленно создаваться в преступных целях. Преступные деяния, совершаемые с помощью таких сетей,

значимым же здесь является то, что компьютеры «бот-сети» эксплуатируются без согласия их пользователей в преступных целях для получения кумулятивного эффекта.

«Бот-сети» подпадают под действие того или иного раздела «Будапештской конвенции» в зависимости от их конкретных функций. В каждом из соответствующих положений конвенции содержится критерий преднамеренности («противоправно», «с целью обмана» и так далее), который должен быть легко доказуем при рассмотрении работы «бот-сети».

Статьи, имеющие отношение к рассматриваемому вопросу	**Примеры**
Статья 2 – Несанкционированный доступ	Создание и эксплуатация «бот-сети» предполагают наличие несанкционированного доступа к компьютерным системам.[7] «Бот-сети» могут использоваться для получения противоправного (несанкционированного) доступа к другим компьютерным системам.
Статья 3 – Неправомерный перехват	В «бот-сетях» могут использоваться технические средства, позволяющие перехватывать передачу входящих/исходящих и внутрисистемных компьютерных данных, не предназначенных для общего пользования.

подпадают под действие положений «Будапештской конвенции», но в этой методической рекомендации не рассматриваются.
5. См. также методическую рекомендацию № 1, касающуюся понятия «компьютерной системы».

Статьи, имеющие отношение к рассматриваемому вопросу	Примеры
Статья 4 – Воздействие на данные (вмешательство в базу данных)	Создание «бот-сети» всегда приводит к изменению компьютерных данных и может спровоцировать их повреждение, удаление, порчу или же стирание. Работа «бот-сетей» сама по себе вызывает повреждение, удаление, порчу, изменение или же стирание компьютерных данных.
Статья 5 – Вмешательство в работу компьютерных систем	«Бот-сети» могут затруднять работу компьютерных систем, в частности, при проведении распределенных атак типа «отказ в обслуживании».[6]
Статья 6 – Противозаконное использование устройств	Все «бот-сети» состоят из технических устройств, подпадающих под действие определения статьи 6 «Будапештской конвенции», так как они изначально разрабатывались или же были приспособлены для совершения противоправных деяний, предусмотренных статьями 2-5 конвенции.[7]

6. См. отдельную методическую рекомендацию, посвящённую этому вопросу.

7. Стороны, сдержанно относящиеся к статье 6 «Будапештской конвенции», тем не менее, должны ввести уголовную ответственность за продажу, распространение или же предоставление в пользование технических устройств, подпадающих под действие настоящей статьи.

Статьи, имеющие отношение к рассматриваемому вопросу	Примеры
	Что же касается самих программ, используемых при создании и эксплуатации «бот-сетей», то они подпадают под действие статьи 6 конвенции. Соответственно, статьей 6 «Будапештской конвенции» вводится уголовная ответственность за производство, продажу, приобретение в целях дальнейшего использования, ввоз, распространение или же использование любых иных способов обеспечения доступности технических устройств «бот-сетей», а также программ, используемых для их создания и эксплуатации.
Статья 7 – Подлог с использованием компьютерных технологий	В зависимости от поставленных перед ней задач «бот-сеть» может вводить, изменять, удалять или стирать компьютерные данные, в результате чего поддельные данные рассматриваются и используются в юридических целях так, как если бы они были подлинными.
Статья 8 – Мошенничество с использованием компьютерных технологий	С помощью «бот-сетей» можно лишить человека принадлежащей ему собственности; другой человек, используя эти сети, может извлечь экономическую выгоду путём ввода, изменения, удаления или стирания компьютерных данных и/или вмешательства в работу компьютерных систем.
Статья 9 – Правонарушения, связанные с детской порнографией	С помощью «бот-сетей» можно распространять материалы с детской порнографией.

Статьи, имеющие отношение к рассматриваемому вопросу	**Примеры**
Статья 10 – Правонарушения, связанные с нарушением авторского права и смежных прав	Используя «бот-сети», возможно противозаконно распространять данные, защищённые законами об интеллектуальной собственности.
Статья 11 – Попытка совершения преступления, подстрекательство к таковому или же соучастие в нём	«Бот сети» могут использоваться при попытке совершения ряда преступлений, предусмотренных в «Будапештской конвенции», в подстрекательстве к их совершению или же при соучастии в них.
Статья 13 – Меры наказания	«Бот-сети» используются для достижения многих преступных целей, в некоторых случаях последствия их применения оказываются весьма тяжкими для частных лиц, организаций государственного и частного сектора или же для стратегически важных объектов инфраструктуры. Тем не менее, внутригосударственное законодательство той или иной стороны конвенции может предусматривать неподобающе мягкие наказания за преступления, совершенные с использованием «Бот-сетей», наказания, выносимые без учёта отягчающих обстоятельств, попыток совершения преступлений, перечисленных в «Будапештской конвенции», подстрекательства к их совершению или же соучастия в них. В таких случаях этим сторонам необходимо рассмотреть возможность внесения поправок в своё внутригосударственное законодательство.

Статьи, имеющие отношение к рассматриваемому вопросу	Примеры
	Соответственно, сторонам «Будапештской конвенции» надлежит, во исполнение статьи 13, обеспечить вынесение за совершение уголовных правонарушений, связанных с использованием «бот-сетей», «эффективных, соразмерных и устрашающих мер наказания, вплоть до лишения свободы». К юридическим лицам могут применяться как уголовные, так и не уголовные наказания, в том числе денежные взыскания. Сторонам конвенции следует также принять во внимание и отягчающие обстоятельства в тех случаях, когда, например, «бот-сети» охватывают значительное количество компьютерных систем или же когда проводимые с их помощью кибератаки становятся причиной смерти/телесных повреждений, вызывают значительный материальный ущерб или же наносят урон стратегически важным объектам инфраструктуры.

3. Заключение комитета «T-CY»

Вышеуказанный список статей, относящихся к вопросу о борьбе с «бот-сетями», свидетельствует о многообразии возможностей их использования в преступных целях и, соответственно, о многообразии применимых к ним норм уголовного права.

Таким образом, комитет «T-CY» согласен с тем, что различные аспекты использования “бот-сетей» подпадают под действие положений «Будапештской конвенции».

Методическая рекомендация по вопросу о проведении DDOS-атак (принята на 9-м пленарном заседании комитета «T-CY»)

1. Введение

На проходившем в декабре 2012 года 8-м пленарном заседании комитета Конвенции о киберпреступности (сокращённо – комитет «T-CY») было принято решение об издании методических рекомендаций, направленных на содействие реализации положений будапештской Конвенции о компьютерных преступлениях и на повышение эффективности их применения на практике в свете изменений, происходящих в области права, политики и технического прогресса.[1]

Настоящие методические рекомендации отражают общее понимание сторонами конвенции того, как следует её применять.

Данная методическая рекомендация касается вопроса о компьютерных атаках с целью нарушения нормального обслуживания пользователей (английское сокращение – DOS-атаки) и о распределенных атаках типа «отказ в обслуживании» (английское сокращение – DDOS-атаки).

В «Будапештской конвенции» используется «технически нейтральная терминология таким образом, чтобы определяющие правонарушения нормы материального уголовного права могли быть применимы к ныне существующим и буду-

1. См. полномочия комитета «T-CY» (статья 46 «Будапештской конвенции»).

щим техническим средствам».[2] В результате новые виды вредоносных программ или же преступлений будут и в дальнейшем подпадать под действие данного международного юридического документа.

В этой методической рекомендации показывается, как различные статьи Конвенции о компьютерных преступлениях применяются в борьбе с DOS/DDOS – атаками.

2. Положения будапештской Конвенции о компьютерных преступлениях, относящиеся к рассматриваемому вопросу (ETS 185)

Компьютерные атаки с целью нарушения нормального обслуживания пользователей (DOS-атаки) представляют собой попытку привести компьютерную систему в непригодное для эксплуатации состояние с помощью целого ряда способов. К ним может относиться перегрузка компьютеров или же сетей, ставших мишенью DOS-атаки, внешними коммуникационными запросами, в результате чего данная услуга становится недоступной для законного пользователя. Распределенная атака типа «отказ в обслуживании» (DDOS-атака) состоит из множества DOS-атак, проводимых одновременно с большого количества компьютеров. В настоящее время существует целый ряд широко распространённых способов проведения DOS/DDOS – атак, включая, например, направление множества бесформенных запросов компьютерной системе; превышение пределов пропускной способности сетей

2. Пункт 36 пояснительного доклада, прилагаемого к «Будапештской конвенции».

компьютеров; направление на сервер электронной почты большего числа мейлов, нежели чем он может принять и обработать.

DOS/DDOS – атаки подпадают под действие того или иного раздела «Будапештской конвенции» в зависимости от их конкретных функций. В каждом из соответствующих положений конвенции содержится критерий преднамеренности («противоправно», «с целью обмана» и так далее), который должен быть легко доказуем при рассмотрении дел по факту проведения DOS/DDOS – атак.

3. Толкование комитетом «T-CY» введения уголовной ответственности за проведение DDOS-атак

Статьи, имеющие отношение к рассматриваемому вопросу	**Примеры**
Статья 2 – Несанкционированный доступ	В результате проведения DOS/DDOS-атак может быть получен доступ к компьютерным системам.
Статья 4 – Воздействие на данные (вмешательство в базу данных)	DOS/DDOS-атаки могут вызвать повреждение, удаление, порчу, изменение или же стирание компьютерных данных.
Статья 5 – Вмешательство в работу компьютерных систем	Цель проведения DOS/DDOS-атак как раз и заключается в том, чтобы серьёзно затруднить работу компьютерной системы.

Статьи, имеющие отношение к рассматриваемому вопросу	**Примеры**
Статья 11 – Попытка совершения преступления, подстрекательство к таковому или же соучастие в нём	DOS/DDOS-атаки могут использоваться при попытке совершения ряда преступлений, предусмотренных «Будапештской конвенцией», в подстрекательстве к их совершению или же при соучастии в них. Речь идёт о таких преступных деяниях как подлог с использованием компьютерных технологий (ст. 7), мошенничество с использованием компьютерных технологий (ст. 8), правонарушения, связанные с детской порнографией (ст. 9), правонарушения, связанные с нарушением авторского и смежных прав (ст. 10).
Статья 13 – Меры наказания	DOS/DDOS-атаки опасны со многих точек зрения. В особенности, в тех случаях, когда они направлены против компьютерных систем, бесперебойная работа которых важна для повседневного жизнеобеспечения человека: в качестве примера можно привести выведение из строя компьютерных сетей, обслуживающих банковские или же госпитальные структуры. Тем не менее, внутригосударственное законодательство той или иной стороны конвенции может предусматривать неподобающе мягкие наказания за преступления, совершенные с использованием DOS/DDOS-атак, наказания, выносимые без учёта отягчающих обстоятельств, попыток совершения преступлений, предусмотренных «Будапештской конвенцией»,

Статьи, имеющие отношение к рассматриваемому вопросу	Примеры
	подстрекательства к их совершению или же соучастия в них. В таких случаях этим сторонам необходимо рассмотреть возможность внесения соответствующих поправок в своё внутригосударственное законодательство. Следовательно, сторонам «Будапештской конвенции» надлежит, во исполнение статьи 13, обеспечить вынесение за совершение уголовных правонарушений, связанных с использованием DOS/DDOS-атак, «эффективных, соразмерных и устрашающих мер наказания, вплоть до лишения свободы». К юридическим лицам могут применяться как уголовные, так и не уголовные наказания, в том числе денежные взыскания. Сторонам конвенции следует также принять во внимание и отягчающие обстоятельства в тех случаях, когда, например, DOS/DDOS-атаки охватывают значительное количество компьютерных систем или же когда они становятся причиной смерти/телесных повреждений, значительного материального ущерба или же наносят урон стратегически важным объектам инфраструктуры.

4. Заключение комитета «T-CY»

Вышеуказанный список статей, относящихся к DOS/DDOS-атакам, свидетельствует о многообразии возможностей их использования в преступных целях.

Таким образом, комитет «T-CY» согласен с тем, что различные аспекты применения DOS/DDOS-атак подпадают под действие положений «Будапештской конвенции».

Методическая рекомендация по вопросу о «выуживании» («фишинге») и краже личных данных (принята на 9-м пленарном заседании комитета «T-CY»)

1. Введение

На проходившем в декабре 2012 года 8-м пленарном заседании комитета Конвенции о киберпреступности (сокращённо – комитет «T-CY») было принято решение об издании методических рекомендаций, направленных на содействие реализации положений будапештской Конвенции о компьютерных преступлениях и на повышение эффективности их применения на практике в свете изменений, происходящих в области права, политики и технического прогресса.[1]

Настоящие методические рекомендации отражают общее понимание сторонами того, как следует её применять.

Данная методическая рекомендация касается вопроса кражи личных данных с помощью их «выуживания» («фишинга») и иных подобных методов,[2] аа также вопроса связанного с ними мошенничества.

В «Будапештской конвенции» используется «технически нейтральная терминология таким образом, чтобы определяющие правонарушения нормы материального уголовного

1. См. полномочия комитета «T-CY» (статья 46 «Будапештской конвенции»)

2. Деяния подобные «фишингу» известны под разными названиями типа целенаправленный «фишинг», «СМишинг», «фарминг», «вишинг» и т. д.

права могли быть применимы к ныне существующим и будущим техническим средствам».[3] В результате новые виды вредоносных программ или же преступлений будут и в дальнейшем подпадать под действие данного международного юридического документа.

В этой методической рекомендации показывается, как различные статьи Конвенции о компьютерных преступлениях применяются к краже личных данных и к связанному с ней мошенничеству с использованием компьютерных систем.

2. «Выуживание» («фишиинг») и кража личных данных

За отсутствием общепринятого определения или же устоявшегося применения термина кражи личных данных (буквально – «кражи личности») можно сказать, что под ним обычно понимаются преступные деяния мошеннического характера, состоящие в получении путём обмана (то есть, без ведома и согласия пострадавшего лица) его личных данных с целью их дальнейшего использования. В качестве синонима иногда употребляется термин «мошенническое использование личных данных» (буквально – «мошенничество с личностью»), хотя под ним может также пониматься и использование вымышленных (не обязательно реальных) личных данных.

Конечно же, персональные данные вымышленного или же реально существующего лица могут стать объектом

3. Пункт 36 пояснительного доклада, прилагаемого к «Будапештской конвенции».

разнообразных незаконных махинаций в рамках целого ряда противоправных деяний. Но в настоящей методической рекомендации рассматривается вопрос кражи личных данных с целью их исключительно мошеннического использования.

Присвоение чужой личности предполагает узурпацию таких её характеристик как фамилия и имя, дата рождения, ныне действующие/предыдущие адреса и т. д. Всё это - без ведома и согласия пострадавшего. В дальнейшем вышеуказанные личные данные используются для приобретения товаров и услуг от его имени.

Кража личных данных осуществляется с помощью использования технологий их «выуживания» (т. н. «фишинга»), целенаправленного «фишинга», скрытного перенаправления пользователей на ложный IP-адрес (т. н. «фарминга»), выманивания у пользователей их конфиденциальных банковских данных путем перенаправления их на ложный банковский сайт, искусно имитирующий реально существующий (т. н. «спуфинг») или же с помощью любых иных действий такого рода, направленных на получение, например, паролей доступа к банковским счетам, зачастую, по электронной почте или же через поддельные интернет-сайты.

Кража личных данных затрагивает правительства, представителей деловых кругов, простых граждан и наносит им большой ущерб. Она подрывает доверие людей к компьютерным технологиям.

В законодательствах многих стран кража личных данных не выделена в особый вид преступления. Лицам, совершившим

кражу личных данных, обычно выносятся более серьёзные обвинения (например, мошенничество с финансовыми ресурсами). Присвоение вымышленной личности обычно предполагает совершение таких преступных деяний как подлог документов и внесение изменений в компьютерные данные. Наличие вымышленной личности облегчает совершение многих преступлений, включая незаконную эмиграцию, торговлю людьми, отмывание незаконно добытых денежных средств, незаконную торговлю наркотиками, финансовое мошенничество, наносящее ущерб государствам и частному сектору, и так далее. Но, по большей части, присвоение вымышленной личности сопряжено с мошенничеством.

Теоретически, совершение кражи личных данных можно разбить на три отдельных этапа:

– этап 1 – получение личных данных путём, например, прямой кражи таковых, а также с помощью поисковых моторов, проведения внутренних и внешних компьютерных атак (с применением неправомерного доступа к компьютерным системам, «Троянов», клавиатурных шпионов «кейлоггеров», программ-шпионов и другого вредоносного программного обеспечения) или же благодаря использованию «фишинга» и иных методов прикладной социологии;

– этап 2 – обладание и распоряжение личными данными; сюда входит продажа такого рода сведений третьим лицам;

– этап 3 – использование личных данных для совершения мошеннических и иных преступных деяний, напри-

мер, для присвоения чужой личности с целью пользования её банковскими счетами и кредитными картами, открытия новых счетов, взятия займов и кредитов, покупки товаров и услуг или же для распространения вредоносных программ.

В заключении можно сказать, что кража личных данных с помощью их «выуживания» («фишинга») и иных подобных методов совершается, по большей части, с целью подготовки ведения такой преступной деятельности, как мошенничество с использованием компьютерных технологий. Даже если кража личных данных и не карается как самостоятельный вид уголовного преступления, правоохранительные органы всегда могут преследовать в судебном порядке её авторов за последующие совершенные ими правонарушения.

3. Толкование комитетом «T-CY» введения «Будапештской конвенцией» уголовной ответственности за совершение кражи личных данных и сопутствующего мошенничества

В «Будапештской конвенции» основное внимание уделяется определению самих преступных деяний, а не рассмотрению используемых при их совершении технических средств и методов. Соответственно, в ней нет отдельных положений, касающихся «выуживания» («фишинга») личных данных и их кражи. Тем не менее, полное применение норм материального права, содержащ0ихся в конвенции, позволит государствам ввести уголовную ответственность за совершение преступных деяний, связанных с кражей личных данных.

«Будапештская конвенция» обязует государства ввести уголовную ответственность за совершение таких правонарушений как несанкционированный доступ к компьютерным системам, неправомерный перехват данных, воздействие на данные (вмешательство в базу данных), вмешательство в работу компьютерных систем, противозаконное использование устройств и мошенничество с использованием компьютерных технологий:

Этап	**Статья конвенции**	**Примеры**
Этап 1 – получение личных данных	Статья2–Несанкционированный доступ	В ходе усилий, предпринимаемых компьютерными пиратами для того, чтобы обойти защиту с помощью паролей путём установки программ их взлома или использования программных недоделок, к компьютеру может быть получен доступ с целью «выуживания»/кражи личных данных пользователя. Неправомерный (несанкционированный) доступ к компьютерным системам является одним из наиболее распространённых видов преступлений, совершаемых с целью завладения такой конфиденциальной информацией как, например, личные данные.

Этап	Статья конвенции	Примеры
	Статья 3 – Неправомерный перехват	Кражa личных данных зачастую предполагает использование «клавиатурных шпионов» («кейлоггеров») или других разновидностей вредоносных вирусов с целью совершения неправомерного перехвата входящих/исходящих/внутрисистемных компьютерных данных, не предназначенных для общего пользования и содержащих такую конфиденциальную информацию как сведения личного характера.
	Статья 4 – Воздействие на данные (вмешательство в базу данных)	«Выуживание» («фишинг») сведений личного характера и их кражa могут привести к повреждению, удалению, порче, изменению или же стиранию компьютерных данных. Зачастую это происходит в процессе получения неправомерного (несанкционированного) доступа к компьютерной системе в ходе установки на неё «клавиатурных шпионов» («кейлоггеров») с целью получения конфиденциальной информации.
	Статья 5 – Вмешательство в работу компьютерных систем	«Выуживание» («фишинг») личных данных и их кражa могут затруднить работу компьютерной системы. При этом облегчается выполнение задачи по завладению сведениями личного характера.

Этап	Статья конвенции	Примеры
	Статья 7 – Подлог с использованием компьютерных технологий	«Выуживание» («фишинг») личных данных и их кража могут быть сопряжены с вводом, изменением, удалением или стиранием компьютерных данных, в результате чего поддельные данные рассматриваются и используются так, как если бы они были подлинными. Возможно, «выуживание» («фишинг») личных данных наиболее часто применяется в целях дальнейшего совершения подлога с использованием компьютерных технологий (в качестве примера здесь можно привести «фишинг» через поддельные сайты реально существующих финансовых учреждений). Соответственно, этот вид противоправной деятельности является наиболее распространённым способом сбора такой конфиденциальной информации как личные данные.
Этап 2 – обладание и распоряжение личными данными	Статья 6 – Противозаконное использование устройств	Выкраденная информация личного характера – включая пароли, параметры доступа, реквизиты кредитных карт и т. д. – может быть приравнена к обладанию «устройствами и компьютерными программами, изначально разработанными или же приспособленными для совершения правонарушений, предусмотренных статьями 2-5 конвенции» или же рассматриваться как «компьютерные пароли, коды доступа или иные подобные данные, с помощью которых можно получить доступ ко всей компьютерной системе или же к её части».

Этап	Статья конвенции	Примеры
Этап 3 – использование личных данных для совершения мошеннических и иных преступных деяний	Статья 8 – Мошенничество с использованием компьютерных технологий	Присвоение чужой личности путём ввода, изменения, удаления или стирания компьютерных данных и/или вмешательства в работу компьютерных систем может позволить преступнику пользоваться банковскими счетами и кредитными картами пострадавшего лица, брать займы и кредиты или же заказывать товары и услуги. В результате этого один человек лишается принадлежащей ему собственности, а другой извлекает для себя экономическую выгоду.
Ко всем трём этапам применимы следующие статьи:	Статья 11 – Попытка совершения преступления, подстрекательство к таковому или же соучастие в нём	Получение, обладание и распоряжение информацией личного характера могут входить в состав правонарушения, квалифицируемого как попытке совершения ряда преступлений, предусмотренных «Будапештской конвенцией», в подстрекательстве к их совершению или же при соучастии в них.

Этап	Статья конвенции	Примеры
	Статья 13 – Меры наказания	Кража личных данных может преследовать множество преступных целей. При этом в некоторых случаях причиняется серьёзный ущерб физическим лицам, а также организациям государственного и частного сектора. Тем не менее, внутригосударственное законодательство той или иной стороны конвенции может предусматривать неподобающе мягкие наказания за совершение кражи личных данных, наказания, выносимые без учёта отягчающих обстоятельств, попыток совершения преступлений, предусмотренных в «Будапештской конвенции», подстрекательства к их совершению или же соучастия в них. В таких случаях этим сторонам необходимо рассмотреть возможность внесения поправок в своё внутригосударственное законодательство.

Этап	Статья конвенции	Примеры
		Соответственно, сторонам «Будапештской конвенции» надлежит, во исполнение статьи 13, обеспечить вынесение за совершение уголовных правонарушений, связанных с кражей личных данных, «эффективных, соразмерных и устрашающих мер наказания, вплоть до лишения свободы». К юридическим лицам могут применяться как уголовные, так и не уголовные наказания, в том числе денежные взыскания. Сторонам конвенции следует также принять во внимание и отягчающие обстоятельства в тех случаях, когда, например, кража личных данных затрагивает интересы значительного числа лиц, причиняет им тяжкие душевные и физические страдания или же подвергает их опасности.

4. Заключение комитета «T-CY»

Комитет «T-CY» полагает, что выше были наглядно показаны различные сферы применения и составляющие преступления, квалифицируемого как «выуживание» («фишинг»)/кража личных данных, и относящиеся к ним нормы уголовного права.

Таким образом, комитет «T-CY» согласен с тем, что различные аспекты вышеуказанных преступлений подпадают под действие положений «Будапештской конвенции».

Методическая рекомендация по вопросу о компьютерных атаках на стратегически важные объекты информационной инфраструктуры (принята на 9-м пленарном заседании комитета «T-CY2)

1. Введение

На проходившем в декабре 2012 года 8-м пленарном заседании комитета Конвенции о киберпреступности (сокращённо – комитет «T-CY») было принято решение об издании методических рекомендаций, направленных на содействие реализации положений будапештской Конвенции о компьютерных преступлениях и на повышение эффективности их применения на практике в свете изменений, происходящих в области права, политики и технического прогресса.[1]

Настоящие методические рекомендации отражают общее понимание сторонами конвенции того, как следует её применять.

В данной методической рекомендации рассматривается вопрос о компьютерных атаках на стратегически важные объекты информационной инфраструктуры (т. н. «критическую информационную инфраструктуру»).

В «Будапештской конвенции» используется «технически нейтральная терминология таким образом, чтобы определяющие правонарушения нормы материального уголовного права могли быть применимы к ныне существующим и

1. См. полномочия комитета «T-CY» (статья 46 «Будапештской конвенции»)

будущим техническим средствам».[2] В результате новые виды вредоносных программ или же преступлений будут и в дальнейшем подпадать под действие данного международного юридического документа.

В этой методической рекомендации показывается, как различные статьи Конвенции о компьютерных преступлениях применяются к компьютерным атакам на стратегически важные объекты информационной инфраструктуры.

2. Положения будапештской Конвенции о компьютерных преступлениях, относящиеся к рассматриваемому вопросу (ETS 185)

Стратегически важные объекты инфраструктуры могут быть определены как составляющие комплекс физических и виртуальных систем и объектов, значение которых столь жизненно велико для страны, что любой сбой в их работе, приведение в нерабочее состояние или же уничтожение могут привести к ослаблению национальной безопасности и обороноспособности, экономической безопасности, системы здравоохранения и государственной безопасности, взятых по отдельности или же вместе. У каждой страны есть своё определение стратегически важных объектов инфраструктуры. Тем не менее, во многих государствах считается, что к ним относятся объекты энергетики, продовольственной безопасности, водоснабжения, снабжения горюче-смазочными материалами, транспорта, связи,

2. Пункт 36 пояснительного доклада, прилагаемого к «Будапештской конвенции».

финансового сектора, промышленности, обороны, государственного управления и коммунальных услуг.

Стратегически важные объекты инфраструктуры управляются с помощью компьютерных систем, в число которых входят, в частности, системы управления производственными процессами или системы оперативно-диспетчерского управления. Как правило, они обозначаются термином «стратегически важные объекты информационной инфраструктуры» (также, т. н. «критическая информационная инфраструктура»).

Если верить частным и государственными источникам, каждый год по всему миру происходит большое, хотя точно и неизвестное количество компьютерных атак на стратегически важные объекты информационной инфраструктуры. При их проведении используются те же методы, что и при совершении других компьютерных преступлений. Различие состоит в последствиях таких атак для общества: они могут привести к хищению денежных средств со счетов государственного казначейства, к прекращению водоснабжения, к перебоям в работе авиатранспорта и так далее.

Тем не менее, ныне существующие и будущие формы компьютерных атак на стратегически важные объекты информационной инфраструктуры подпадают под действие следующих разделов «Будапештской конвенции» в зависимости от характера таковых атак. В каждом из соответствующих положений конвенции содержится критерий преднамеренности («противоправно», «с целью обмана» и так далее), который следует учитывать при квалификации преступления.

3. Толкование комитатом «T-CY» введения уголовной ответственности за проведение компьютерных атак на стратегически важные объекты информационной инфраструктуры

Статьи, имеющие отношение к рассматриваемому вопросу	**Примеры**
Статья 2 – Несанкционированный доступ	В ходе проведения атак на стратегически важные объекты информационной инфраструктуры может быть получен доступ к компьютерной системе.
Статья 3 – Неправомерный перехват	При проведении атак на стратегически важные объекты информационной инфраструктуры могут использоваться технические средства, позволяющие осуществлять перехват входящих/исходящих и внутрисистемных компьютерных данных, не предназначенных для общего пользования.
Статья 4 – Воздействие на данные	Атаки на стратегически важные объекты информационной инфраструктуры могут вызвать повреждение, удаление, порчу, изменение или же стирание компьютерных данных.
Статья 5 – Вмешательство в работу компьютерных систем	Атаки на стратегически важные объекты информационной инфраструктуры могут затруднить работу компьютерной системы, в чём, собственно говоря, и заключается их основная задача.

Статьи, имеющие отношение к рассматриваемому вопросу	**Примеры**
Статья 7 – Подлог с использованием компьютерных технологий	Атаки на стратегически важные объекты информационной инфраструктуры могут привести к вводу, изменению, удалению или же стиранию компьютерных данных, в результате чего поддельные данные будут рассматриваться и использоваться в юридических целях так, как если бы они были подлинными.
Статья 8 – Мошенничество с использованием компьютерных технологий	С помощью атаки на стратегически важные объекты информационной инфраструктуры можно лишить человека принадлежащей ему собственности; в результате другой человек может извлечь для себя экономическую выгоду путём ввода, изменения, удаления или стирания компьютерных данных и/или вмешательства в работу компьютерных систем.
Статья 11 – Попытка совершения преступления, подстрекательство к таковому или же соучастие в нём	Атаки на стратегически важные объекты информационной инфраструктуры могут использоваться при попытке совершения ряда преступлений, предусмотренных в «Будапештской конвенции», в подстрекательстве к их совершению или же при соучастии в них.

Статьи, имеющие отношение к рассматриваемому вопросу	**Примеры**
Статья 13 – Меры наказания	В различных странах по причинам технического, культурного и иного порядка последствия атак на стратегически важные объекты информационной инфраструктуры могут быть разными. Но, как правило, правительства выражают в этой связи озабоченность в том случае, если таковые причиняют серьёзный и обширный ущерб. Тем не менее, внутригосударственное законодательство той или иной стороны конвенции может предусматривать неподобающе мягкие наказания за проведение атак на стратегически важные объекты информационной инфраструктуры, наказания, выносимые без учёта отягчающих обстоятельств, попыток совершения преступлений, перечисленных в «Будапештской конвенции», подстрекательства к их совершению или же соучастия в них. В таких случаях этим сторонам необходимо рассмотреть возможность внесения поправок в своё внутригосударственное законодательство. Соответственно, сторонам «Будапештской конвенции» надлежит, во исполнение статьи 13, обеспечить вынесение за совершение уголовных правонарушений, связанных с проведением таковых атак, «эффективных, соразмерных и устрашающих мер наказания, вплоть до лишения свободы». К юридическим лицам могут применяться как уголовные, так и не уголовные наказания, в том числе денежные взыскания.

Статьи, имеющие отношение к рассматриваемому вопросу	Примеры
	Сторонам конвенции следует также принять во внимание и отягчающие обстоятельства в тех случаях, когда, например, атаки на стратегически важные объекты информационной инфраструктуры охватывают значительное количество компьютерных систем, когда они становятся причиной смерти/телесных повреждений или же приводят к значительному материальному ущербу.

4. Заключение комитета «T-CY»

Вышеуказанный список статей, относящихся к атакам на стратегически важные объекты информационной инфраструктуры, свидетельствует о многообразии возможностей их использования в преступных целях.

Таким образом, комитет «T-CY» согласен с тем, что различные аспекты подобных атак подпадают под действие положений «Будапештской конвенции».

Методическая рекомендация о новых видах вредоносных программ (принята на 9-м пленарном заседании комитета «T-CY2»)

1. Введение

На проходившем в декабре 2012 года 8-м пленарном заседании комитета Конвенции о киберпреступности (сокращённо – комитет «T-CY») было принято решение об издании методических рекомендаций, направленных на содействие реализации положений будапештской Конвенции о компьютерных преступлениях и на повышение эффективности их применения на практике в свете изменений, происходящих в области права, политики и технического прогресса.[1]

Настоящие методические рекомендации отражают общее понимание сторонами конвенции того, как следует её применять.

В данной рекомендации рассматривается вопрос, касающийся новых видов вредоносных программ.

В «Будапештской конвенции» используется «технически нейтральная терминология таким образом, чтобы определяющие правонарушения нормы материального уголовного права могли быть применимы к ныне существующим и будущим техническим средствам».[2] В результате новые виды вредоносных программ или же преступлений будут и в

1. См. полномочия комитета «T-CY» (статья 46 «Будапештской конвенции»).
2. Пункт 36 пояснительного доклада, прилагаемого к «Будапештской конвенции»

дальнейшем подпадать под действие данного международного юридического документа.

В этой методической рекомендации показывается, как различные статьи Конвенции о компьютерных преступлениях применяются к новым видам вредоносных программ.

2. Положения будапештской Конвенции о компьютерных преступлениях, относящиеся к рассматриваемому вопросу (ETS 185)

В настоящее время существует множество разновидностей вредоносных программ. Они определяются Организацией европейского сотрудничества и развития как «общий термин, употребляющийся для обозначения программного обеспечения, внедрённого в информационную систему для причинения вреда этой или другим системам, или же для их использования в иных целях, нежели чем те, для которых они предназначались их владельцами».[3] Общеизвестные виды вредоносного программного обеспечения включают компьютерных «червей», вирусов и «Троянов». Нынешние их разновидности способны воровать данные путём копирования таковых и их отсылки по различным адресам; с их помощью возможно манипулировать данными; они могут затруднять работу компьютерных систем, управляющих, в частности, стратегически важными объектами инфраструктуры; «Трояны»-вымогатели способны удалять, стирать данные или же блокировать доступ к ним; а специально разработанное вредоносные программы могут целенаправленно воздействовать на отдельные компьютерные системы.

3. http://www.oecd.org/internet/ieconomy/40724457.pdf

Согласно частным и правительственным источникам, каждый год создаётся и раскрывается большое количество всё новых видов вредоносных программ. Цели, преследуемые их разработчиками, самые разнообразные. Как и их предшественники, они используются для кражи денежных средств, выведения из строя систем водоснабжения, шантажа пользователей и так далее.

Число и разнообразие вредоносных программ столь велико, что было бы невозможно перечислить в уголовном законе даже их ныне существующие виды. Разработчики Конвенции о компьютерных преступлениях сознательно избегают употребления таких терминов как компьютерные «черви», вирусы и «Трояны», так как в результате быстрых изменений в этой области конвенция рисковала бы скоро устареть и потерять свою действенность.

Естественно, в законе невозможно предусмотреть и будущие виды такого программного обеспечения.

По всем вышеперечисленным причинным важно сосредоточиться на целях, преследуемых создателями вредоносных программ, и на последствиях их применения.

Соответственно, как ныне существующие, так и будущие виды вредоносных программ подпадают под действие следующих положений «Будапештской конвенции» в зависимости от выполняемых ими в настоящее время функций. В каждом из соответствующих положений конвенции содержатся критерии преднамеренности («противоправно», «с целью обмана» и так далее), которые следует учитывать при квалификации преступления.

3. Толкование комитетом «T-CY» введения уголовной ответственности заиспользование новых видов вредоносных программ

Статьи, имеющие отношение к рассматриваемому вопросу	**Примеры**
Статья 2 – Несанкционированный доступ	Вредоносные программы могут использоваться для получения доступа к компьютерным системам.
Статья 3 – Неправомерный перехват	Вредоносные программы могут использоваться для осуществления перехвата компьютерных данных.
Статья 4 – Воздействие на данные (вмешательство в базу данных)	Вредоносные программы вызывают повреждение, удаление, порчу, изменение или же стирание компьютерных данных.
Статья 5 – Вмешательство в работу компьютерных систем	Вредоносные программы могут затруднять работу компьютерных систем.

Статьи, имеющие отношение к рассматриваемому вопросу	**Примеры**
Статья 6 – Противозаконное использование устройств .	В соответствии с определением, содержащимся в статье 6 «Будапештской конвенции», вредоносные программы приравниваются к техническим устройствам (стороны конвенции, сдержанно относящиеся к её 6-й статье, должны тем не менее ввести уголовную ответственность за продажу, распространение или же использование любых иных способов обеспечения доступности технических устройств, подпадающих под действие вышеуказанной статьи). Дело в том, что вредоносные программы, как правило, были изначально разработаны или же приспособлены для совершения правонарушений, предусмотренных статьями 2-5 конвенции. Кроме того, 6-й статьей этого международного юридического документа вводится уголовная ответственность за продажу, приобретение с целью использования, импорт, распространение или же употребление любых иных способов обеспечения доступности компьютерных паролей, кодов доступа или иных подобных данных, с помощью которых можно получить доступ к компьютерной системе. Вышеперечисленные признаки часто характеризуют вредоносные программы.

Статьи, имеющие отношение к рассматриваемому вопросу	**Примеры**
Статья 7 – Подлог с использованием компьютерных технологий.	Вредоносные программы могут использоваться для ввода, изменения, удаления или же стирания компьютерных данных, в результате чего поддельные данные рассматриваются и используются в юридических целях так, как если бы они были подлинными.
Статья 8 – Мошенничество с использованием компьютерных технологий.	С помощью вредоносных программ можно лишить человека принадлежащей ему собственности; другой человек, используя эти программы, может извлечь для себя экономическую выгоду путём ввода, изменения, удаления или стирания компьютерных данных и/или вмешательства в работу компьютерных систем.
Статья 11 – Попытка совершения преступления, подстрекательство к таковому или же соучастие в нём	Вредоносные программы могут использоваться при попытке совершения ряда преступлений, перечисленных в «Будапештской конвенции», в подстрекательстве к их совершению или же при соучастии в них.

Статьи, имеющие отношение к рассматриваемому вопросу	**Примеры**
Статья 13 – Меры наказания	Последствия применения новых видов вредоносных программ могут быть самыми разнообразными. Некоторые из них относительно незначительны; другие вредоносные программы могут представлять опасность для людей, стратегически важных объектов инфраструктуры и так далее. В любом случае, в различных странах по причинам технического, культурного и иного порядка таковые последствия могут быть разными. Тем не менее, внутригосударственное законодательство той или иной стороны конвенции может предусматривать неподобающе мягкие наказания за разработку и использование вредоносных программ, наказания, выносимые без учёта отягчающих обстоятельств, попыток совершения преступлений, перечисленных в «Будапештской конвенции», подстрекательства к их совершению или же соучастия в них. В таких случаях этим сторонам необходимо рассмотреть возможность внесения поправок в своё внутригосударственное законодательство. Соответственно, сторонам «Будапештской конвенции» надлежит, во исполнение статьи 13, обеспечить

Статьи, имеющие отношение к рассматриваемому вопросу	Примеры
	вынесение за совершение уголовных правонарушений, связанных с разработкой и использованием вредоносных программ, «эффективных, соразмерных и устрашающих мер наказания, вплоть до лишения свободы». К юридическим лицам могут применяться как уголовные, так и не уголовные наказания, в том числе денежные взыскания. Сторонам конвенции следует также принять во внимание и отягчающие обстоятельства в тех случаях, когда, например, проводимые с помощью вредоносных программ атаки охватывают значительное количество компьютерных систем, когда они становятся причиной смерти/телесных повреждений, наносят значительный материальный ущерб или же причиняют урон стратегически важным объектам инфраструктуры.

4. Заключение комитета «T-CY»

Вышеуказанный список статей, относящихся ко всем видам вредоносных программ, свидетельствует о многообразии возможностей их использования в преступных целях.

Таким образом, комитет «T-CY» согласен с тем, что все виды вредоносных программ подпадают под действие положений «Будапештской конвенции».

Методическая рекомендация по вопросу о трансграничном доступе к данным – ст. 32 (принята на 12-м пленарном заседании комитета «T-CY»)

1. Введение

На проходившем в декабре 2012 года 8-м пленарном заседании комитета Конвенции о киберпреступности (сокращённо – комитет «T-CY») было принято решение об издании методических рекомендаций, направленных на содействие реализации положений будапештской Конвенции о компьютерных преступлениях и на повышение эффективности их применения на практике в свете изменений, происходящих в области права, политики и технического прогресса.[4]

Настоящие методические рекомендации отражают общее понимание сторонами конвенции того, как следует её применять.

В данной методической рекомендации рассматривается вопрос о трансграничном доступе к данным, предусмотренном статьей 32 «Будапештской конвенции».[5]

В пункте «b» статьи 32 «Будапештской конвенции» содержится исключение из принципа территориальности: при

4. См. полномочия комитета «T-CY» (статья 46 «Будапештской конвенции»)

5. Настоящая методическая рекомендация составлена на основании доклада под названием «Трансграничный доступ к данным и юрисдикция» (документ T-CY(2012)3), принятого на пленарном заседании комитета «T-CY», проходившем в декабре 2012 г.

определённых ограничительно установленных обстоятельствах им разрешается осуществление одностороннего трансграничного доступа к данным без обращения к структурам судебной взаимопомощи. Поощряется более эффективное использование сторонами «Будапештской конвенции» всех её положений, касающихся вопросов международного сотрудничества, включая структуры судебной взаимопомощи.

В общем и целом, методы и порядок применения вышеуказанной статьи, а также условия и предоставляемые при этом гарантии могут быть самыми разными в каждом конкретно взятом государстве - стороне конвенции. Но при этом в каждом случае сохраняется и требует особого внимания забота о соблюдении процессуальных прав подозреваемых лиц, о защите конфиденциальности личных данных, об обеспечении правовых оснований доступа к данным, хранящимся на территории под иностранной юрисдикцией или же на удалённых серверах («в облаках»), а также о соблюдении национального суверенитета.

Настоящая методическая рекомендация направлена на то, чтобы способствовать реализации положений «Будапештской конвенции», развеять недопонимание в отношении её положений, касающихся вопроса трансграничного доступа к данным, и успокоить третьи стороны.

---

http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/TCY2013/TCYreports/TCY_2012_3_transborder_rep_V31public_7Dec12.pdf
http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/TCY2013/TCYreports/TCY_2012_3_transborder_rep_V31public_7Dec12.pdf

Таким образом, эта методическая рекомендация поможет сторонам конвенции полностью использовать возможности, предоставляемые ею в области трансграничного доступа к данным.

2. Статья 32 «Будапештской конвенции»

Текст статьи:

Статья 32 – «Трансграничный доступ к хранящимся компьютерным данным с соответствующего согласия или к общедоступным данным.

Сторона может без согласия другой Стороны:

a. получать доступ к общедоступным компьютерным данным (из открытых источников) независимо от их географического местоположения;

b. получать через компьютерную систему на своей территории доступ к хранящимся на территории другой Стороны компьютерным данным или получать их, если эта Сторона имеет законное и добровольное согласие лица, которое имеет законные полномочия раскрывать эти данные этой Стороне через такую компьютерную систему».

Выдержка из объяснительного доклада к «Будапештской конвенции»:

293. Разработчиками «Будапештской конвенции» весьма обстоятельно обсуждался вопрос о том, когда той или иной стороне конвенции разрешается в одностороннем порядке и без обращения к структурам судебной взаимопомощи осуществлять доступ к компьютерным данным, хранящимся на территории другой стороны. Они детально рассмотрели случаи, в которых для государств может быть приемлемо или же неприемлемо

действовать в одностороннем порядке. В конечном итоге, авторы проекта конвенции пришли к тому выводу, что пока невозможно выстроить цельную, юридически обязательную правовую систему, регламентирующую данную область. Частично это было вызвано недостатком на то время конкретного опыта работы в подобных ситуациях; отчасти - пониманием того, что должное решение вопроса зачастую зависит от конкретных обстоятельств в каждом конкретно взятом случае. В свою очередь, это делало затруднительным выведение общих норм. В конце концов, разработчики решили закрепить в статье 32 конвенции лишь те ситуации, в которых, по общему мнению, односторонние действия допустимы. Они согласились не вводить норм, регламентирующих остальные случаи до тех пор, пока не наберётся достаточный опыт в этой области и пока он не будет должным образом осмыслен. По этому поводу в 3-м пункте статьи 39 конвенции предусматривается, что в остальных ситуациях односторонний порядок действий не разрешается и не исключается.

294. В статье 32 (трансграничный доступ к хранящимся компьютерным данным с соответствующего согласия или к общедоступным данным) рассматриваются две ситуации: первая, при которой подлежащие доступу данные являются общедоступными; и вторая, когда сторона конвенции имеет доступ или же получает данные, находящиеся за пределами её границ, с помощью компьютерной системы на своей территории от лица, уполномоченного законом раскрыть таковые данные другой стороне через вышеуказанную компьютерную систему, при условии, что оно даёт на это своё законное и добровольное согласие. Кто считается лицом, «уполномоченным законом» раскрывать данные? Это зависит от конкретных обстоятельств дела, от личности «уполномоченного» и применяемых норм закона. Например, электронный адрес такого лица может находиться в памяти компьютерной системы зарубежного поставщика

интернет-услуг или же оно может сознательно хранить свои данные в другой стране. Такие лица вправе извлекать искомые данные и, будучи уполномочены на то законом, добровольно раскрывать их содержание сотрудникам правоохранительных органов или же предоставлять им доступ к вышеуказанным данным, как это и предусматривается статьей 32 «Будапештской конвенции».

3. Толкование комитетом «T-CY» статьи 32 «Будапештской конвенции»

Касательно пункта «a» статьи 32 конвенции (получение доступа к общедоступным компьютерным данным из открытых источников независимо от их географического местоположения) никаких особых вопросов не возникло и никаких отдельных методических рекомендаций от комитета «T-CY» не потребовалось.

Само собой разумеется, что сотрудники правоохранительных органов могут получать доступ ко всем общедоступным данным и с этой целью подписываться или абонироваться на получение услуг, доступных широкой общественности.[6]

С том случае, если часть общедоступного сайта или сервиса становится недоступной для широкой общественности, то они перестают считаться общедоступными в том смысле, в котором это понятие толкуется в статье 32 «Будапештской конвенции».

---

6. Тем не менее, внутригосударственным законодательством может быть ограничен доступ правоохранительных органов к общедоступным данным или же их использование.

Что касается пункта «b» статьи 32, то он может распространяться на две следующие типичные ситуации:

– Электронный адрес того или иного лица находится в памяти компьютерной системы зарубежного поставщика интернет-услуг или же оно может сознательно хранить свои данные в другой стране. Таковое лицо вправе извлекать искомые данные и, будучи уполномочено на то законом, добровольно раскрывать их содержание сотрудникам правоохранительных органов или же предоставлять им доступ к вышеуказанным данным, как это и предусматривается статьей 32 «Будапештской конвенции».[7]

– Задержано с соблюдением всех требований закона лицо, подозреваемое в торговле наркотиками. Электронный почтовый ящик его/её планшета, смартфона или иного компьютерного устройства открыт. Возможно, в нём есть доказательства совершения преступления. Если подозреваемый добровольно соглашается на доступ полиции к его учётной записи и если сотрудники полиции уверены в том, что данные, содержащиеся в электронном почтовом ящике, физически хранятся на территории другого государства – стороны конвенции, то тогда – во исполнение пункта «b» статьи 32 - полиция вправе осуществить доступ к вышеуказанным данным.

Остальные ситуации ни разрешены, ни исключены.[8]

---

7. Пункт 294 объяснительного доклада.

8. Пункт 293 объяснительного доклада. См. также статью 39.3 «Будапештской конвенции».

В отношении пункта «b» статьи 32 (трансграничный доступ к данным, обусловленный получением разрешения) комитет «T-CY» разделяет следующее общее видение по нижеизложенным вопросам:

3.1. Общие положения и гарантии

Как указывалось выше, предполагается, что стороны конвенции составляют общность доверяющих друг другу государств, в которых утвердились принципы верховенства права и соблюдения прав человека в соответствии со статьей 15 «Будапештской конвенции».[9]

---

9. Статья 14 – Сфера применения процессуальных норм
1. Каждая Сторона принимает законодательные и иные меры, необходимые для установления полномочий и процедур, предусмотренных положениями настоящего раздела в целях проведения конкретных уголовных расследований или судебного разбирательства.
2. За исключением случаев, когда положениями Статьи 21 конкретно предусматривается иное, каждая Сторона применяет полномочия и процедуры, упомянутые в параграфе 1 настоящей Статьи, в отношении::
   a. уголовных преступлений, предусмотренных в соответствии со Статьями 2 - 11 настоящей Конвенции;
   b. других уголовных преступлений, совершенных при помощи компьютерной системы;
   c. сбора доказательств в электронной форме уголовного преступления.
3. a. Каждая Сторона может сделать оговорку о сохранении за собой права применять меры, упомянутые в Статье 20, только в отношении правонарушений или категорий правонарушений, указанных в этой оговорке, при условии, что круг таких правонарушений или категорий правонарушений не более ограничен, чем круг правонарушений, к которым

Как указывалось выше, предполагается, что стороны конвенции составляют общность доверяющих друг другу государств, в которых утвердились принципы верховенства права и соблюдения прав человека в соответствии со статьей 15 «Будапештской конвенции».[10]

она применяет меры, предусмотренные в Статье 21. Каждая Сторона рассматривает пути ограничения сферы действия такой оговорки, чтобы сделать возможным максимально широкое применение мер, упомянутых в Статье 20.

b. В том случае, когда Сторона ввиду ограничений в своем законодательстве, действующем на момент принятия настоящей Конвенции, не имеет возможности применить меры, предусмотренные Статьями 20 и 21, к информации, передаваемой по компьютерной системе поставщика услуг, которая:
   i. используется для обслуживания замкнутой группы пользователей,
   ii. не использует общественных сетей связи, а также не соединена ни с какими другими компьютерными системами, будь то общественными или частными, эта Сторона может сохранить за собой право не применять указанных мер к такой передаче информации. Каждая Сторона рассматривает пути ограничения этого права с тем, чтобы сделать возможным максимально широкое применение мер, упомянутых в Статьях 20 и 21.

10. Статья 15 – Условия и гарантии

1. Каждая Сторона обеспечивает, чтобы установление, исполнение и применение полномочий и процедур, предусмотренных настоящим Разделом, осуществлялись в соответствии с условиями и гарантиями, предусмотренными нормами ее внутригосударственного права, обеспечивающими надлежащую защиту прав человека и свобод, включая права, вытекающие из обязательств, которые Сторона взяла на себя по Европейской

При применении вышеуказанных мер следует учитывать права частных лиц и интересы третьих сторон.

Таким образом, сторона конвенции, проводящая дистанционно розыскные мероприятия на территории другого государства – стороны, может рассмотреть возможность оповестить об этом соответствующие органы власти последнего.

3.2. О понятиях «трансграничный» и «местонахождение»

Под трансграничным доступом следует понимать «осуществление в одностороннем порядке доступа к компьютерным данным, хранящимся на территории другой стороны без обращения к структурам судебной взаимопомощи».[11]

Конвенции о Защите Прав Человека и Основных Свобод, принятой Советом Европы в 1950 году Международным пактом о Гражданских и Политических Правах, принятым Организацией Объединенных Наций в 1966 году, а также другими применимыми международными договорами по правам человека и предусматривающими принцип соразмерности.

2. Такие условия и гарантии с учетом характера полномочий и процедур включают, среди прочего, судебный или иной независимый надзор, основания правомочности применения, ограничение сферы и сроков действия таких полномочий или процедур.
3. В той мере, в какой это соответствует общественным интересам, в частности обоснованному отправлению правосудия, Сторона рассматривает влияние предусмотренных данным разделом полномочий и процедур на права, ответственность и законные интересы третьих сторон.

11. Пункт 293 объяснительного доклада к «Будапештской конвенции».

Эта следственная мера может применяться взаимообразно между сторонами «Будапештской конвенции».

В пункте «b» статьи 32 упоминаются «компьютерные данные, хранящиеся на территории другой стороны». Соответственно, предполагается, что вышеуказанный пункт может применяться в том случае, если известно местонахождение искомых данных.

Пункт «b» статьи 32 не распространяется на те случаи, когда данные не хранятся на территории другой стороны или же когда их местонахождение точно не установлено. Сторона конвенции не может на основании статьи 32.b добиваться раскрытия компьютерных данных, хранящихся на её собственной территории.

Применительно к другим ситуациям, статья 32.b не должна рассматриваться «ни как разрешающая, ни как исключающая» таковые. Соответственно, в тех случаях, когда достоверно не известно, хранятся ли искомые данные на территории другой стороны, сторонам конвенции надлежит самостоятельно оценить законность проводимых оперативно-розыскных мероприятий или же применения иных способов доступа к таковым данным в свете своего внутригосударственного законодательства, применимых к данным случаям принципов международного права или же состояния международных отношений.

3.3. О понятии «доступ, получаемый без согласия другой стороны»

В соответствии со статьёй 32.b, обращение к структурам судебной взаимопомощи не обязательно, в то время как

сама «Будапештская конвенция» не требует, но и не исключает оповещения другой стороны. Одна сторона конвенции может информировать другую сторону, если считает это уместным.

3.4. О понятии «согласия»

В статье 32.b указывается, что согласие на доступ к данным должно быть законным и добровольным. Это значит, что лица, предоставляющие доступ к данным или же дающие своё согласие на их раскрытие, не должны делать это под принуждением или в результате их обмана.[12]

В зависимости от положений внутригосударственного законодательства, согласие даваемое несовершеннолетним, или же лицом, страдающим психическими или иными расстройствами, может не считаться законным/юридически значимым.

В большинстве государств – сторон «Будапештской конвенции» условия сотрудничества в рамках расследования уголовного дела требуют явно выраженного согласия. Например, принятие лицом всего комплекса положений и условий пользования той или иной услугой в сети может не рассматриваться в качестве явно выраженного согласия, даже если в них и сказано, что таковые предполагают предоставление требуемых данных органам уголовного правосудия в случае обнаружения злоупотреблений.

---

12. В некоторых странах согласие, даваемое во избежание уголовного преследования или же с целью смягчения выдвигаемых статей обвинения или же мер наказания, также считается законным и добровольным.

3.5. О применяемом праве

Действуя во исполнение статьи 32.b, правоохранительные органы должны во всех случаях применять те же правовые нормы, что и в своём государстве. Если доступ к данным и их раскрытие не разрешены у себя в стране, то не разрешаются они и по статье 32.b.

Предполагается, что стороны конвенции составляют общность доверяющих друг другу государств, в которых утвердились принципы верховенства права и соблюдения прав человека в соответствии со статьей 15 «Будапештской конвенции».

3.6. О лице, уполномоченном предоставлять доступ к данным или же раскрывать их

Касательно определения лица, «уполномоченного законом» раскрывать данные, следует указать, что оно зависит от конкретных обстоятельств дела, а также от применяемых норм и положений закона.

Например, им может быть физическое лицо, предоставляющее доступ к учётной записи своей электронной почты или же другим данным, которые оно хранит на удалённых серверах за рубежом.[13] Им также может быть и юридическое лицо.

Поставщики интернет-услуг вряд ли способны дать юридически значимое и добровольное согласие на раскрытие данных своих пользователей во исполнение статьи 32. Обычно, они лишь предоставляют место для хранения

13. См. пример, данный в пункте 294 объяснительного доклада.

таковых данных, не будучи ни их владельцами, ни контролёрами. Следовательно, юридически провайдеры не уполномочены давать своё согласие на раскрытие данных. Конечно, правоохранительные органы могут получить их из-за рубежа другими способами, например, в рамках взаимной юридической помощи или же задействовав механизмы, применяемые в чрезвычайных ситуациях.

3.7. Внутригосударственные юридически значимые запросы и статья 32.b

Статья 32.b не распространяется на внутренние запросы о раскрытии данных или же на подобные юридически значимые ходатайства в самом государстве – стороне конвенции

3.8. О местонахождении лица, дающего своё согласие на предоставление доступа к данным или же на их раскрытие

Обычно предполагается, что лицо, дающее своё согласие на доступ к данным или же на их раскрытие, физически находится на территории запрашиваемой стороны.

Тем не менее, здесь существуют различные варианты. Можно представить себе, что физическое или юридическое лицо находится на территории запрашивающих правоохранительных органов на тот момент, когда оно даёт своё согласие на предоставление доступа к данным или же на их раскрытие, или когда оно соглашается раскрыть их, не предоставляя при этом доступа к данным. Возможен такой вариант, при котором лицо находится в стране хранения данных на момент получения его согласия на их раскрытие

и/или предоставление доступа. Это лицо может также физически находиться в третьей стране во время дачи согласия на сотрудничество или предоставления доступа к данным. Если речь идёт о юридическом лице (например, о частном юридическом лице), то таковое лицо может быть представлено одновременно на территории запрашивающих правоохранительных органов, не территории хранения запрашиваемых данных или даже в третьей стране.

Следует учитывать тот факт, что многие стороны конвенции протестуют против того, чтобы на находящихся на их территории лиц напрямую выходили иностранные правоохранительные органы, склоняющие таковых к сотрудничеству (некоторые государства даже рассматривают эти действия как уголовно наказуемое правонарушение).

4. Заключение комитета «T-CY»

Комитет «T-CY» согласен с тем, что настоящая методическая рекомендация отражает общее видение сторонами вопросов, касающихся сферы применения и положений статьи 32 «Будапештской конвенции».

Методическая рекомендация о «СПАМЕ» (принята на 12-м пленарном заседании комитета «T-CY»)

1. Введение

На проходившем в декабре 2012 года 8-м пленарном заседании комитета Конвенции о киберпреступности

(сокращённо – комитет «T-CY») было принято решение об издании методических рекомендаций, направленных на содействие реализации положений будапештской Конвенции о компьютерных преступлениях и на повышение эффективности их применения на практике в свете изменений, происходящих в области права, политики и технического прогресса[1]

Настоящие методические рекомендации отражают общее понимание сторонами конвенции того, как следует её применять.

В данной методической рекомендации рассматривается вопрос «СПАМА». В «Будапештской конвенции» используется «технически нейтральная терминология таким образом, чтобы определяющие правонарушения нормы материального уголовного права могли быть применимы к ныне существующим и будущим техническим средствам».[2] В результате новые виды вредоносных программ или же преступлений будут и в дальнейшем подпадать под действие данного международного юридического документа.

В этой методической рекомендации показывается, как различные статьи Конвенции о компьютерных преступлениях применяются к статьям «Будапештской конвенции», касающимся «СПАМА».

---

1. См. полномочия комитета «T-CY» (статья 46 «Будапештской конвенции»).
2. Пункт 36 пояснительного доклада, прилагаемого к «Будапештской конвенции»

2. Положения будапештской Конвенции о компьютерных преступлениях, относящиеся к рассматриваемому вопросу (ETS 185)

«СПАМ» часто определяется как массовая рассылка электронных писем, направляемых по значительному количеству адресов без различия личности получателей, так как их содержание рассчитано на как можно более широкий охват целевой аудитории.

Рассматриваемая тема имеет три различных аспекта, касающихся:

– содержания «СПАМА»,

– действий по рассылке «СПАМА» и

– способов, используемых для его передачи.

Содержание «СПАМА» может быть законным и незаконным. Если содержание «СПАМА» носит противозаконный характер (как, например, в случае предложения купить поддельные лекарства или же принять участие в мошеннических финансовых офертах), то такое правонарушение может подпадать под действие соответствующих положений национального законодательства. Сами действия по передаче «СПАМА» (включая массовую рассылку электронных писем уголовно ненаказуемого содержания) могут квалифицироваться как гражданские или уголовные правонарушения в соответствии с нормами ряда национальных законодательств.

Положения «Будапештской конвенции» не распространяются на случаи распространения «СПАМА», содержание

которого не является противозаконным и не воздействует на работу компьютерной системы, но может создавать неудобства для его конечных потребителей.

Способы, используемые при рассылке «СПАМА», могут квалифицироваться как противозаконные в соответствии с положениями «Будапештской конвенции», а «СПАМ» приравниваться к ряду других правонарушений, не перечисленных в ниже прилагаемой таблице (см. например, статью 7).

Как и в предыдущих методических рекомендациях, в каждом из соответствующих положений конвенции, перечисляемых в левой колонке данной таблицы, содержится критерий преднамеренности («противоправно», «с целью обмана» и так далее). Но, применительно к некоторым случаям рассылки «СПАМА», преднамеренный характер действий может оказаться трудно доказуемым.

3. Толкование комитетом «T-CY» положений конвенции о «СПАМЕ»

Статьи, имеющие отношение к рассматриваемому вопросу	**Примеры**
Статья 2 – Несанкционированный доступ	«СПАМ» может содержать вредоносные программы, имеющие доступ к компьютерной системе или позволяющие получить таковой.

Статьи, имеющие отношение к рассматриваемому вопросу	**Примеры**
Статья 3 – Неправомерный перехват	«СПАМ» может содержать вредоносные программы, способные вести неправомерный перехват компьютерных данных или же делать возможным их перехват и передачу.
Статья 4 – Воздействие на данные (вмешательство в базу данных)	СПАМ» может содержать вредоносные программы, способные вызвать повреждение, удаление, порчу, изменение или же стирание компьютерных данных.
Статья 5 – Вмешательство в работу компьютерных систем	Передача «СПАМА» может серьёзно затруднить работу компьютерных систем. «СПАМ» может содержать вредоносные программы, способные серьёзно затруднить функционирование компьютерных систем.
Статья 6 – Противозаконное использование устройств	Для передачи «СПАМА» могут использоваться устройства, подпадающие под действие статьи 6 «Будапештской конвенции». С другой стороны, сам «СПАМ» может содержать программы, приравниваемые к устройствам, предусмотренным вышеуказанной статьей.
Статья 8 – Мошенничество с использованием компьютерных технологий	«СПАМ» может использоваться для введения, изменения, устранения или стирания компьютерных данных или же для вмешательства в работу компьютерных систем с целью извлечения незаконной экономической выгоды.

Статьи, имеющие отношение к рассматриваемому вопросу	**Примеры**
Статья 10 – Правонарушения, связанные с нарушением авторского права и смежных прав	«СПАМ» может использоваться для рекламы и продажи поддельных товаров, включая программное обеспечение и другие объекты, защищённые авторским правом.
Статья 11 – Попытка совершения преступления, подстрекательство к таковому или же соучастие в нём	«СПАМ» и его рассылка могут использоваться при попытке совершения ряда преступлений, перечисленных в «Будапештской конвенции», в подстрекательстве к их совершению или же при соучастии в них: таких как подлог с использованием компьютерных технологий (ст. 7) или же мошенничество с использованием компьютерных технологий (ст. 8).

Статьи, имеющие отношение к рассматриваемому вопросу	**Примеры**
Статья 13 – Меры наказания	«СПАМ» может использоваться для достижения множества преступных целей, в некоторых случаях, с тяжкими последствиями для физических лиц, а также для организаций государственного и частного сектора. Даже если та или иная сторона «Будапештской конвенции» и не предусматривает уголовной ответственности за рассылку «СПАМА» как такового, ей следует ввести подобную ответственность за совершение сопряжённых со «СПАМОМ» правонарушений, перечисленных выше, с учётом отягчающих обстоятельств. Сторонам «Будапештской конвенции» надлежит, во исполнение статьи 13, обеспечить вынесение за совершение уголовных правонарушений, связанных со «СПАМОМ», «эффективных, соразмерных и устрашающих мер наказания, вплоть до лишения свободы». К юридическим лицам могут применяться как уголовные, так и не уголовные наказания, в том числе денежные взыскания.

4. Заключение комитета «T-CY»

Приведённый выше список статей свидетельствует о многообразии возможностей использования в преступных целях «СПАМА» и его рассылки.

Таким образом, комитет «T-CY» согласен с тем, что различные аспекты использования «СПАМА» подпадают под действие положений «Будапештской конвенции».

Prems 123015

RUS

Совет Европы является ведущей организацией на континенте в области прав человека. Он включает в себя 47 стран, 28 из которых являются членами Европейского Союза. Все страны-члены Совета Европы подписали Европейскую конвенцию о правах человека – международный договор, призванный защищать права человека, демократию и верховенство права. За применением Конвенции в государствах-членах следит Европейский суд по правам человека.

www.coe.int

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE