Н. Ж. Апахаев, И. Т. Мусабекова,
И. С. Амреева

КИБЕРПРЕСТУПНОСТЬ

УЧЕБНОЕ ПОСОБИЕ

Н.Ж. Апахаев, И.Т. Мусабекова, И.С. Амреева.

КИБЕРПРЕСТУПНОСТЬ

Учебное пособие

Алматы, 2022

УДК 343(075.8)
ББК 67.408я73
А 76

Рассмотрено и одобрено на заседании методического совета Академии Кайнар. Протокол № 5/76 от 27 декабря 2021 г.

Рецензенты:
Алмагамбетов П.А.;
Тлеуов Г.Б.

Апахаев Н.Ж., Мусабекова И.Т., Амреева И.С.
А 76 Киберпреступность: Учебное пособие (конспект лекции). – Алматы, 2022. – 155 с.

ISBN 978-601-08-1404-2

Данная работа представляет собой учебное пособие, в которой с раскрываются теоретические аспекты киберпреступности в общем порядке.

Пособие рассчитано на студентов, преподавателей высших учебных заведений, сотрудников правоохранительных органов.

ӘОЖ 343(075.8)
КБЖ 67.411я73

ISBN 978-601-80854-1-3

ОГЛАВЛЕНИЕ

Введение

Информационно-коммуникационные технологии (ИКТ) изменили способы, при помощи которых люди ведут свои дела, покупают товары и услуги, отправляют и получают деньги, общаются, обмениваются информацией, взаимодействуют друг с другом, формируют и развивают отношения с другими людьми. Такие изменения, а также постоянно растущие масштабы использования ИКТ и зависимость от них создают уязвимости, которыми могут воспользоваться преступники и другие злоумышленники, нацеленные на ИКТ и/или использующие ИКТ для совершения преступлений. В данном учебном пособии дается представление об основных понятиях, относящихся к киберпреступности, рассказывается о том, что такое киберпреступность, рассматриваются тенденции в области развития Интернета, технологий и киберпреступности, а также проблемы технического, правового, этического и оперативного характера, связанные с расследованием киберпреступлений и предупреждением киберпреступности. В литературе для чтения, выбранной для данного предмета, содержится обзор ключевых понятий, основных терминов и определений, а также общие сведения о киберпреступности, связанных с ней проблемах и мерах по ее предупреждению.

Тема 1. Введение в киберпреступность.

1. Основы компьютерных технологий.

Компьютерная система может быть представлена настольными или портативными компьютерами. Однако мобильные телефоны, планшетные компьютеры и устройства Интернета вещей (IoT), являющиеся устройствами, подключенными к Интернету (например, бытовые приборы и умные часы), которые взаимосвязаны и взаимодействуют друг с другом и позволяют отслеживать объекты, людей, животных и/или растения, а также обмениваться информацией о них с целью предоставления пользователям этих устройств определенной услуги, а также многие другие устройства также могут рассматриваться в качестве компьютерных систем. Существуют разные определения компьютерной системы. Например, статья 1(a) Конвенции Совета Европы о киберпреступности 2001 года определяет «компьютерную систему» как «любое устройство или группу взаимосвязанных или смежных устройств, одно или более из которых, действуя в соответствии с программой, осуществляет автоматизированную обработку данных» (для ознакомления с руководящими указаниями в отношении толкования понятия «компьютерная система», включенного в Конвенцию, см. публикацию Комитета участников Конвенции о киберпреступности 2012 года (Cybercrime Convention Committee, 2012). В то же время в статье 1 Конвенции Африканского союза о кибербезопасности и защите персональных данных 2014 года компьютерная система определяется как «электронное, магнитное, оптическое, электрохимическое или иное высокоскоростное устройство обработки данных или группа взаимосвязанных или сопряженных устройств, выполняющих логические, арифметические функции или функции хранения, включая средство хранения данных или средство связи, непосредственно связанное с таким устройством или такими устройствами или работающее в сочетании с таким устройством или такими устройствами». Компьютерные системы имеют свойство обрабатывать данные. Статья 2(3) Конвенции Лиги арабских государств о борьбе с преступлениями в области информационных технологий 2010 года определяет данные как «все, что может храниться, обрабатываться, генерироваться и передаваться с помощью информационных технологий, например, цифры, буквы, символы и т.д.». Для обозначения данных используются и другие термины: в статье 1 (b) Конвенции Совета Европы о киберпреступности используется термин «компьютерные данные» («любое представление фактов, информации или понятий в форме, подходящей для обработки в компьютерной системе, включая программу, подходящую для того, чтобы компьютерная система выполняла функцию»; в статье Конвенции Африканского союза о кибербезопасности и защите персональных данных 2014 года используется термин «компьютеризированные данные», который имеет практически такое же определение данных, что и термин, используемый в Конвенции Совета Европы о киберпреступности 2001 года («любое представление фактов, информации или понятий в форме, подходящей для обработки в компьютерной системе»); а в статье 1(b) Соглашения о сотрудничестве государств-участников Содружества Независимых

Государств в борьбе с преступлениями в сфере компьютерной информации 2001 года используется термин «компьютерная информация» («информация, находящаяся в памяти компьютера, на машинных или иных носителях в форме, доступной восприятию ЭВМ, или передающаяся по каналам связи»). Большинство компьютерных систем, с которыми мы знакомы, хранят данные. Например, смартфон может создать фотографию при помощи встроенной камеры (обработка данных), и он также может сохранить эту фотографию для последующего доступа (хранение данных). Данные обычно хранятся во внутренней постоянной памяти, именуемой жестким диском. Лица, которые предоставляют услуги, связанные с компьютерной системой, именуются поставщиками услуг. Статья 2(2) Конвенции Лиги арабских государств о борьбе с пятью преступлениями в области информационных технологий 2010 года определяет поставщика услуг как «любое физическое либо юридическое лицо, будь то публичное или частное, которое предоставляет абонентам услуги, необходимые для осуществления коммуникации с использование информационных технологий, или которое обрабатывает или хранит информацию от имени службы связи или ее пользователей». Интернет-услуги для домашних компьютеров и мобильных телефонов предоставляются поставщиками услуг Интернета. Поставщик Интернет-услуг использует компьютерные системы, которые могут отправлять данные на компьютеры или телефоны и получать данные, отправляемые с компьютеров или телефонов. Когда два или более компьютера могут обмениваться данными, отправляя их друг другу, создается компьютерная сеть. Представьте себе свою электронную почту. Когда вы используете электронную почту, вы, вероятно, открываете браузер и подключаетесь к веб-сайту. После входа в систему вы можете отправлять и получать электронные письма. По всей вероятности, этот веб-сайт принадлежит не вам, а другой организации. Эта организация предоставляет услуги электронной почты и может считаться поставщиком услуг. Обратите внимание, что услуги доступа к Интернету и услуги доступа к вашей электронной почте – это две совершенно разные услуги. Это приводит нас к данным о трафике, которые определяются в статье 1(d) Конвенции Совета Европы о компьютерных преступлениях 2001 года как «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». Ранее мы говорили о компьютерных данных как о данных, которые хранятся или обрабатываются компьютерной системой. Данные о трафике – это данные, которые передаются по компьютерной сети. Теперь еще раз представьте себе свою электронную почту. Вы пишете свое электронное письмо, а затем «отправляете» это сообщение получателю. Данные в электронном письме направляются через сеть, пока не достигнут адресата. Данные о трафике – это любые данные, необходимые для того, чтобы электронное письмо достигло своего адресата. Хорошим примером является телефон. Представьте себе, что

вы захотели позвонить своему приятелю. И вам, и вашему приятелю нужны телефоны, и вам обоим нужны номера телефонов. Ваш поставщик услуг предоставит вам номер телефона и доступ к сети, если вы оплатите счет за телефон. Затем вам нужно будет узнать номер телефона вашего приятеля, чтобы сделать звонок. После того, как вы и ваш приятель получите услугу и узнаете номера друг друга, вы сможете общаться. То же самое, в принципе, можно сказать и о компьютерных сетях. Когда вы хотите получить доступ к веб-сайту, вы вводите доменное имя (например, yahoo.com) в Интернет-браузер (или веб-браузер) (например, Google, Bing). Это доменное имя может быть связано (т.е. сопоставлено) с одним или несколькими адресами Интернет-протокола (или IP-адресами), «уникальными идентификаторами, присваиваемыми компьютерам или другим подключаемым к Интернету цифровым устройствам поставщиком услуг Интернета, когда они подключаются к Интернету» (Maras, 2014, p. 385). Система доменных имен (DNS) обеспечивает доступ к Интернету путем преобразования доменных имен в IP-адрес.

2. Глобальные тенденции в области использования технологий и подключения к Интернету.

На Земле существует очень мало мест, где вы не сможете получить доступ к Интернету. В большинстве стран есть, как минимум, один поставщик Интернет-услуг, который предоставляет сетевую инфраструктуру (аппаратное обеспечение, такое как оборудование, кабели и беспроводной доступ) для крупных городов. Даже в районах, где нет местных поставщиков Интернет-услуг, глобальные спутниковые сети могут обеспечить доступ к Интернету для отдаленных районов. Широкополосная технология в развивающихся странах внедряется медленными темпами, в результате чего население этих стран для доступа в Интернет использует мобильные технологии. Благодаря доступности Интернет-услуг через 7 мобильные устройства, использование Интернета неуклонно растет. Смартфоны становятся все менее дорогостоящими и включают в себя все больше функций, а поставщики услуг мобильной связи обеспечивают более надежный доступ в Интернет через менее дорогие сети сотовой связи. Это способствует увеличению уровня проникновения Интернета во многих странах. 2016 год стал первым годом, когда большинство пользователей Интернета во всем мире для выхода в Интернет стали использовать мобильные устройства (Statcounter, 2016). Уровень проникновения Интернета означает «процент от общей численности населения данной страны или региона, который использует Интернет» (IGI Global, n.d.). По состоянию на сентябрь 2017 года уровень проникновения Интернета в мире оценивается в 51%. Таким образом, примерно половина населения мира имеет доступ к Интернету и возможность пользоваться Интернетом (см. рисунок 1 с указанием уровня проникновения Интернета с разбивкой по регионам).

По мере повышения надежности доступа в Интернет и увеличения количества людей, подключающихся к Интернету, растет количество важных услуг, предоставляемых в режиме онлайн. Например, подключение к

Интернету является очень быстрым и очень надежным в Южной Корее. По оценкам Организации экономического сотрудничества и развития (ОЭСР), в 2018 году уровень проникновения Интернета в домохозяйствах в Южной Корее составил 99,5%. При таком большом количестве людей, подключенных к Интернету, корейское правительство и коммерческие структуры предлагают все больше онлайновых услуг. Например, если вы получаете квитанцию на оплату штрафа за превышение скорости (автоматически с подключенной к Интернету камеры фиксации нарушений скоростного режима), вы можете посетить правительственный веб-сайт, чтобы просмотреть информацию о своей штрафной квитанции. Затем вы можете немедленно оплатить штраф через систему банковских электронных платежей. Этот процесс расчета может быть полностью безбумажным. В некоторых случаях количество государственных услуг, предоставляемых офлайн, меньше количества онлайновых услуг. В настоящее время в Китае сложилась схожая ситуация, только в еще больших масштабах. Согласно 41-му Статистическому отчету о развитии Интернета в Китае, опубликованному в январе 2018 года, по состоянию на «конец декабря 2017 года число пользователей Интернета в Китае достигло 772 миллионов человек, увеличившись на 40,74 миллионов по сравнению с концом 2016 года... Уровень Интернет проникновения достиг 55,8%, что на 2,6 процентных пункта больше, чем в конце 2016 года… Число пользователей мобильного Интернета в Китае достигло 753 миллионов человек, что на 57,34 миллионов больше по сравнению с концом 2016 года». К таким Интернет-услугам, как мгновенный обмен сообщениями, онлайн-платежи, онлайн-покупки, онлайн-доставка еды или онлайн-бронирование поездок, обращаются сотни миллионов пользователей. Такие приложения, как WeChat (инструмент для мгновенного обмена сообщениями) и Alipay (система платежей в пользу третьих лиц), стали важными приложениями практически для каждого смартфона. Мобильные устройства, мобильный Интернет и эти приложения настолько популярны, что государственные услуги, платежи, инвестиции, общественный и частный транспорт и многие другие услуги полностью интегрированы с ними (Kessel and Mozur, n.d., p. 7). В условиях, когда критически важные услуги все чаще предлагаются в режиме онлайн, причем иногда это сопровождается сокращением количества офлайновых услуг, также появляется все больше возможностей для злоупотребления технологиями и совершения преступлений.

3. Понятие киберпреступности. Не существует общепринятого определения киберпреступности. Тем не менее, следующее определение включает в себя элементы, общие для всех существующих определений киберпреступности. Киберпреступление – это действие, нарушающее закон, которое совершается с использованием информационно-коммуникационных технологий (ИКТ) и либо нацелено на сети, системы, данные, веб-сайты и/или технологии, либо способствует совершению преступления (ITU, 2012; Maras, 2014; Maras, 2016). Киберпреступление отличается от традиционного преступления тем, что оно «не признает физические или географические границы» и может совершаться с меньшими усилиями, большей легкостью и

с большей скоростью, чем традиционное преступление (хотя это зависит от вида киберпреступления и вида традиционного преступления, с которым оно сравнивается) (Maras, 2014;). Европол разделяет киберпреступления на киберзависимые преступления (т.е. «любое преступление, которое может быть совершено только с использованием компьютеров, компьютерных сетей или других форм информационно-коммуникационных технологий»; McGuire and Dowling, 2013, p. 4; Europol, 2018, p. 15) и преступления, совершаемые посредством кибертехнологий (т.е. традиционные преступления, совершаемые с помощью Интернета и цифровых технологий). Ключевое различие между этими категориями киберпреступности заключается в роли информационно-коммуникационных технологий в совершении правонарушения – являются ли ИКТ целью преступления или неотъемлемой частью способа совершения преступления (modus operandi или M.O.; т.е. метода действия), использованного преступником (УНП ООН, 2013, стр. 16). Когда ИКТ являются целью преступления, такое киберпреступление негативно влияет на конфиденциальность, целостность и/или доступность компьютерных данных или систем (УНП ООН, 2013). Конфиденциальность, целостность и доступность составляют так называемую «Триаду КЦД» (Rouse, 2014): проще говоря, конфиденциальная информация должна оставаться конфиденциальной, ее не следует изменять без разрешения владельца, а данные, услуги и системы должны быть доступным для владельца в любое время. Когда ИКТ являются частью способа совершения преступления, киберпреступность включает в себя традиционное преступление (например, мошенничество и кражу), совершению которого тем или иным образом способствуют Интернет и цифровые технологии. Киберпреступления могут совершаться физическими лицами, группами лиц, коммерческими организациями и государствами. Хотя эти субъекты могут применять схожие тактические методы (например, использовать вредоносное программное обеспечение) и атаковать схожие цели (например, компьютерную систему), они имеют разные мотивы и намерения при совершении киберпреступлений. Были проведены различные исследования киберпреступности (см., например, исследования, опубликованные в журналах «Deviant Behavior» и «International Journal of Cyber Criminology»). В этих исследованиях киберпреступность изучалась через призму психологии, социологии и криминологии, а также других научных дисциплин (для ознакомления с обзором исследований киберпреступности с точки зрения различных дисциплин см. Maras, 2016). В одних публикациях действия преступников истолковываются как результат рационального и свободного выбора, тогда как в других публикациях преступность рассматривается как результат действия внутренних и/или внешних сил (см., например, главные и классические труды по криминологии, включенные в книгу Mclaughlin and Muncie, 2013). В других работах изучалась роль «пространства» в киберпреступности, в частности, роль онлайн-пространств и онлайн сообществ в культурной трансмиссии преступных и/или криминальных ценностей (см. Maras, 2016, Chapter 6). Цель этих научных исследований киберпреступности состоит в том, чтобы пролить свет на

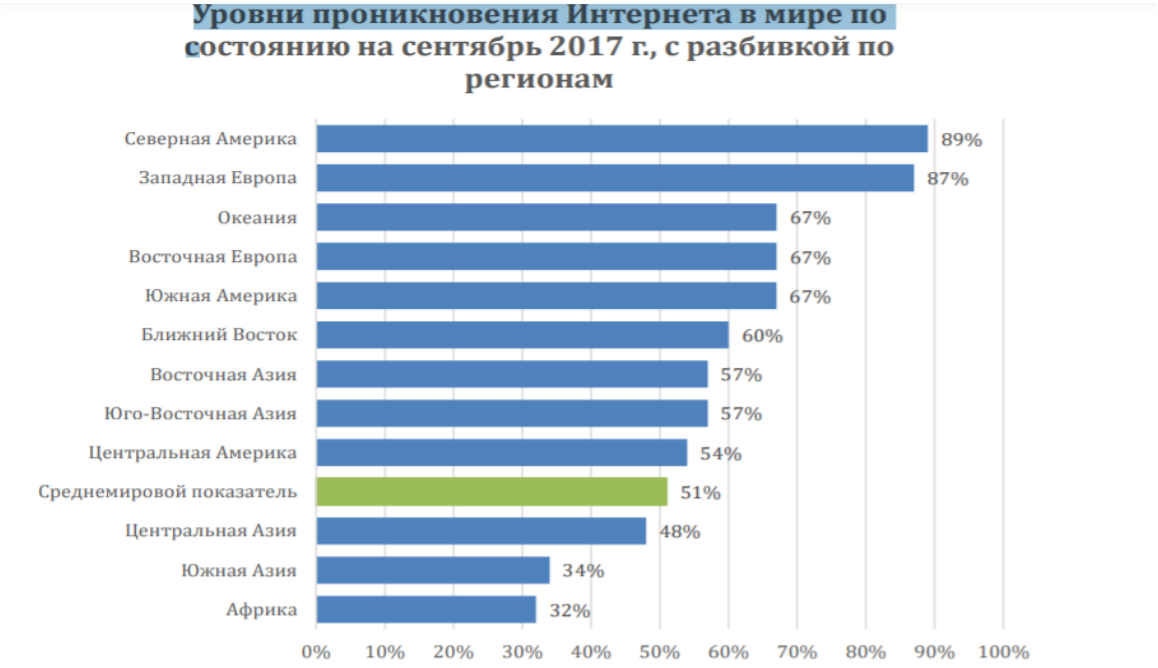
последствия киберпреступности, «характер и масштабы киберпреступности, оценить реакции на киберпреступность и последствия этих реакций, а также оценить эффективность существующих методов, используемых для борьбы с киберпреступностью, смягчения ее последствий и предупреждения киберпреступлений» (Maras, 2016, p. 13)

4. Тенденции в области киберпреступности. Региональные и международные правоохранительные органы (например, Европол и Интерпол) и региональные организации (например, Африканский союз и Организация американских государств) публикуют информацию о тенденциях в области киберпреступности и кибербезопасности. Тенденции в области киберпреступности можно также определить по ежегодным отчетам и/или данным из различных официальных инструментов измерения преступности и исследований проблемы виктимизации: например, Национальная система учета инцидентов (США); Общее социальное исследование (Канада); Обзор преступности в Англии и Уэльсе (Англия и Уэльс). Эти инструменты измерения параметров преступности и исследования проблемы виктимизации различаются с точки зрения типов собираемых и анализируемых данных о киберпреступности, а также методов, используемых для сбора и анализа данных Компании в сфере кибербезопасности и другие частные организации, занимающиеся анализом безопасности, бизнес-рисков и/или угроз по всему миру, публикуют отчеты о тенденциях в области киберпреступности и/или кибербезопасности, основанные на имевших место инцидентах кибербезопасности, их типах, частоте и последствиях. Например, в 2018 году компания Trend Micro определила использование вируса вымогателя в качестве тенденции в области киберпреступности. При совершении такого вида киберпреступления компьютерные системы заражаются вредоносным кодом (вредоносной программой), и данные в них становятся недоступными для владельцев и/или законных пользователей до тех пор, пока киберпреступнику не будут заплачены деньги. Хотя атаки с использованием вируса вымогателя не новы, увеличилось их количество, а также частота, интенсивность и охват. Изначально злоумышленники, совершавшие киберпреступления такого рода, нацеливались на физических лиц и требовали от них небольшие суммы денег, но затем они стали нацеливаться на коммерческие предприятия, компании и организации и, наконец, на других субъектов в частном и государственном секторах, которые предоставляют критически важные услуги (например, больницы). В качестве примера можно привести атаку с использованием вируса-вымогателя Wanna Cry в 2017 году, которая затронула примерно 150 стран (Reuters, 2017), в том числе более 80 «организаций NHS (Национальной службы здравоохранения) в одной только Англии, что повлекло за собой отмену почти 20.000 записей на прием, 600 клиник врачей общей практики были вынуждены вернуться к бумажному документообороту, а пять больниц переадресовывали кареты скорой помощи в другие больницы, поскольку больше не могли оказывать срочную медицинскую помощь» (Hern, 2017). В 2017 году в докладе Европола «Оценка угрозы организованной преступности в Интернете» вирус-

вымогатель был также определен в качестве тенденции в области киберпреступности.

С появлением новых технологий (например, Интернета вещей, дронов, роботов, беспилотных автомобилей) будут выявляться новые тенденции в области киберпреступности. Более того, как отмечено в докладе Европола «Оценка угрозы организованной преступности в Интернете» за 2017 год, меры по охране правопорядка и обеспечению безопасности влияют на киберпреступность и тактику, инструменты и цели киберпреступников. Следовательно, эти меры также будут влиять на будущие тенденции в области киберпреступности.

Рисунок 1: Уровень проникновения Интернета с разбивкой по регионам



Источник: Statista (2018). Уровень проникновения Интернета в мире по состоянию на сентябрь 2017 года с разбивкой по регионам, Statista. https://www.statista.com/statistics/269329/penetration-rate-of-the-internet-by-region/.

5. Технические проблемы. Существует несколько технических причин, которые затрудняют борьбу с киберпреступностью. Первая причина – атрибуция. Любой компьютер, подключенный к Интернету, может взаимодействовать с любым другим компьютером, подключенным к Интернету. Обычно мы видим общедоступный IP-адрес компьютера, когда этот компьютер соединяется с нашим компьютером. IP-адрес – это, как правило, глобальный уникальный номер, который позволяет нам определить, из какой страны подключается этот компьютера, и к какому поставщику Интернет-услуг он подключен. Проблема состоит в том, что у злоумышленника есть много способов скрыть свой IP-адрес или даже притвориться, что он подключается с другого IP-адреса. Более того, преступники могут использовать различные инструменты, чтобы избежать обнаружения правоохранительными органами, затруднить доступ и скрыть

сайты в Даркнете. Вторая техническая проблема связана с программным обеспечением. Компьютерные программы представляют собой программное обеспечение. Приложения на вашем телефоне или планшете являются программным обеспечением. Сервисы, к которым вы подключаетесь в Интернете, например, веб-сайт, также являются программным обеспечением. Очень часто программное обеспечение имеет уязвимости. Уязвимость может быть связана с проблемой в программе или неправильной конфигурацией, которая позволяет злоумышленникам делать то, что они не должны иметь возможность делать (например, загружать данные кредитной карточки клиента). Компаниям-разработчикам программного обеспечения бывает непросто обнаружить уязвимости, особенно те, которые связаны с крупными программными проектами, которые часто меняются. Иногда злоумышленники находят уязвимость раньше компании, производящей программное обеспечение (т.е. уязвимость «нулевого дня). По мнению Билдж и Думитрас (Bilge and Dumitras, 2012), «пока уязвимость остается неизвестной, уязвимое программное обеспечение не может быть исправлено, а антивирусные программы не могут обнаружить атаку с помощью сканирования на основе сигнатур». Компании становится известно об уязвимости такого рода, когда она используется киберпреступниками для атаки на конфиденциальность, целостность или доступность программного обеспечения и пользователей программного обеспечения. В 2017 году Equifax – американское бюро кредитных историй – потеряло «конфиденциальные персональные данные» 143 миллионов американцев из-за уязвимости программного обеспечения. Эта уязвимость эксплуатировалась в течение трех месяцев, пока не была устранена. Уязвимости, приводящие к потере данных, являются относительно распространенными даже для крупных организаций, поскольку задача создания, настройки и защиты цифровых систем надлежащим образом является затруднительной. Еще одной технической проблемой является виртуализированная ИТ-инфраструктура (например, облако). Когда инфраструктура организации перемещается в облако, это означает, что: a) компания перекладывает часть ответственности за кибербезопасность на поставщика облачных услуг (например, безопасность физической системы, безопасность центра обработки данных); b) когда происходят нарушения безопасности, компании приходится работать с поставщиком облачных услуг, чтобы расследовать инциденты, которые могут привести к проблемам технического и правового характера.

6. Правовые проблемы. Киберпреступность является одним из видов транснациональной преступности, исполнители и жертвы которой могут находиться в любой точке мира, где есть подключение к Интернету. В этой связи следователям, ведущим расследования киберпреступлений, зачастую требуется трансграничный доступ к данным и обмен ими. Эта задача может быть выполнена в случае, если запрашиваемые данные сохраняются поставщиками услуг и принимаются меры, позволяющие правоохранительным органам получать доступ к данным. Основными правовыми проблемами при расследовании киберпреступлений и судебном

преследовании киберпреступников являются: разные правовые системы, существующие в разных странах; различия в национальных законодательствах о киберпреступности; различия в нормах доказательственного права и уголовного судопроизводства (например, в процедурах получения доступа к цифровым доказательствам правоохранительными органами; например, на основании законного распоряжения, такого как ордер на обыск, или без него); различия в охвате и географической применимости региональных и многосторонних договоров о борьбе с киберпреступностью; и различия в подходах к защите данных и соблюдению прав человека.

Этические проблемы. Правоохранительные органы должны соблюдать правовые и этические нормы при расследовании преступлений (и киберпреступлений), обработке, анализе и толковании доказательств. Этические проблемы могут возникать не только при осуществлении правоохранительной деятельности, но и при использовании информационно-коммуникационных технологий (ИКТ) отдельными лицами, группами лиц, компаниями, организациями и правительством. Например, этическое поведение при использовании ИКТ подразумевает воздержание от причинения вреда другим людям, системам и данным, а также соблюдение принципа верховенства закона и прав человека. Разоблачения компании Cambridge Analytica убедили всех в необходимости уделять внимание этическим вопросам, связанным со сбором и использованием данных на платформах социальных сетей. В частности, средства массовой информации обнаружили, что компания по обработке данных Cambridge Analytica заплатила за получение личных данных пользователей Facebook через стороннего исследователя Александра Когана, создавшего приложение для сбора данных в форме опросника для проверки личности, которое сообщало пользователям (мелким шрифтом), что информация собирается исключительно в научных целях, причем это утверждение не было проверено компанией Facebook и оказалось ложным. Несмотря на то, что только 305.000 человек приняли участие в опросе и дали согласие на сбор своих личных данных, данные их друзей также были получены из их учетных записей, в результате чего оценочное число пострадавших достигло 87 миллионов человек. Инцидент с Cambridge Analytica пролил свет на неэтичное поведение тех, кто несет ответственность за огромное количество данных, собранных об отдельных лицах и использованных непредвиденным образом для пользователей, которые согласились предоставить (некоторую) информацию, и неправомочным образом для тех, кто вообще не давал никакого согласия на сбор и использование какие-либо своих данных. Даже если то, что сделали Cambridge Analytica и другие причастные лица, не считается незаконным, их действия были неэтичными.

Вопросы для обсуждения:

1. Что такое киберпреступность?
2. Почему киберпреступность изучается с научной точки зрения?
3. Где можно получить информацию о тенденциях в области

киберпреступности? Оцените эти источники.

4. Какие существуют правовые проблемы, связанные с расследованием киберпреступлений и предупреждением киберпреступности?

5. Какие существуют этические проблемы, связанные с расследованием киберпреступлений и предупреждением киберпреступности?

6. Какие существуют технические проблемы, связанные с расследованием киберпреступлений и предупреждением киберпреступности?

7. Какие существуют оперативные проблемы, связанные с расследованием киберпреступлений и предупреждением киберпреступности?

Тема 2. Основные виды киберпреступности.

1. Преступления против конфиденциальности, целостности и доступности компьютерных данных или систем.

К «новым» киберпреступлениям (т.е. *киберзависимым* преступлениям) относятся в первую очередь те преступления, которые нацелены на системы, сети и данные и совершаются с целью нарушения их *конфиденциальности* (т.е. когда системы, сети и данные защищены, и только авторизованные пользователи могут получить к ним доступ), *целостности* (т. е. когда данные являются точными и достоверными и не подвергались изменениям) и *доступности* (т.е. когда данные, услуги и системы доступны по первому требованию). Эти киберпреступления включают в себя хакерские атаки; создание, хранение и распространение вредоносных программ; атаки типа «отказ в обслуживании» (DoS); распределенные атаки типа «отказ в обслуживании» (DDoS); и порча веб-сайтов (то есть форма онлайн-вандализма, нацеленная на содержимое веб-сайтов).

Хакерская атака – это термин, используемый для описания несанкционированного доступа к системам, сетям и данным (далее именуются целью). Хакерские атаки могут совершаться исключительно для получения доступа к цели или для получения и/или сохранения такого доступа после истечения срока действия разрешения на доступ. Примерами национальных и региональных законов, устанавливающих уголовную ответственность за преднамеренный несанкционированный доступ к веб-сайту или информации в обход мер безопасности, являются законы Объединенных Арабских Эмиратов: статья 1 Федерального закона № 2 от 2006 года о предупреждении преступлений в области информационных технологий, и статья 2 Конвенции Совета Европы о киберпреступности (также известной как Будапештская конвенция; далее именуется Конвенцией о киберпреступности).

Хакеры могут также добиваться несанкционированного доступа к системам, чтобы причинить ущерб или иной вред мишени. В 2014 году британский хакер Лори Лав (Lauri Love) взломал веб-сайты, получил несанкционированный доступ к системам правительства США и похитил конфиденциальную информацию из этих систем. Это киберпреступление нарушило конфиденциальность данных (в результате получения

несанкционированного доступа к веб-сайту и системе и кражи информации) и целостность данных (в результате порчи веб-сайтов).

Помимо получения несанкционированного доступа к системам, хакеры могут перехватывать данные по мере их перемещения по сетям. Статья 3 Конвенции о киберпреступности запрещает «умышленно осуществленный с использованием технических средств неправомерный перехват 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». Незаконный перехват данных также запрещен в соответствии со статьей 7 Конвенции Лиги арабских государств о борьбе с преступлениями в области информационных технологий 2010 года и статьей 29(2)(a) Конвенции Африканского союза о кибербезопасности и защите личных данных 2014 года. Примером незаконного перехвата является атака посредника (или атака «человек посередине»), которая позволяет злоумышленнику перехватывать сообщения между отправителем и получателем и/или выдавать себя за отправителя и/или получателя и общаться от их имени. Такое киберпреступление нарушает конфиденциальность данных (в результате перехвата) и целостность данных (в результате того, что преступник выдает себя за отправителя и/или получателя).

В дополнение к совершению хакерских атак, киберпреступники могут вмешиваться в работу компьютерных систем и/или препятствовать доступу к системам, услугам и данным. Вмешательство может включать в себя блокирование, изменение, добавление, передачу, редактирование, удаление или иное повреждение данных, систем и услуг. Конвенция Совета Европы о киберпреступности запрещает *вмешательство в данные*, которое определяется как «умышленное и противоправное повреждение, удаление, ухудшение качества, изменение или блокирование компьютерных данных» (статья 4). Вмешательство в данные также запрещено в соответствии со статьей 29(2)(a) Конвенции Африканского союза о кибербезопасности и защите личных данных 2014 года и статьей 8 Конвенции Лиги арабских государств о борьбе с преступлениями в области информационных технологий 2010 года.

Конвенция Совета Европы о киберпреступности также запрещает *вмешательство в систему*, которое определяется как «умышленное и противоправное создание серьезных помех функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, ухудшения качества, изменения или блокирования компьютерных данных» (статья 5). Этот вид киберпреступления также запрещен статьей 29(1)(d) Конвенции Африканского союза о кибербезопасности и защите личных данных 2014 года. Примером вмешательства в систему *является атака типа «отказ в обслуживании»* (или DoS-атака). DoS-атака создает помехи системам, перегружая серверы и/или посреднические устройства (например, маршрутизаторы) запросами, чтобы препятствовать доступу законного трафика к сайту и/или

использованию системы (Maras, 2016, p. 270).

Распределенная атака типа «отказ в обслуживании» (или DDoS-атака) означает использование нескольких компьютеров и других цифровых технологий для проведения скоординированных атак с целью перегрузки серверов и/или посреднических устройств для препятствования доступу законным пользователям (Maras, 2016, p. 270-271). Принцип действия одного из типов DDoS-атак можно объяснить на следующем примере (CloudFlare, 2018): представьте себе, что большое количество компьютеров пытаются подключиться к одному компьютеру (серверу) одновременно. Этот компьютер имеет ограниченную вычислительную мощность и пропускную способность сети. Если слишком большое количество компьютеров будут пытаться подключиться к нему одновременно, сервер будет не в состоянии реагировать на каждое соединение достаточно быстро. В результате сервер не сможет отвечать на запросы *реальным* пользователям, поскольку он слишком занят *ложными* запросами.

DDoS-атаки могут проводиться отдельным лицом, группой лиц или государством. Государства могут нацеливаться на критические важные объекты инфраструктуры, которые считаются жизненно необходимыми для функционирования общества. Например, Страна А пережила серию DDoS-атак, совершенных Страной Б против ее финансового сектора. В результате этих кибератак граждане страны А были лишены доступа к Интернет-банкингу, а банкоматы в этой стране работали с перебоями.

DDoS-атаки могут осуществляться с использованием цифровых устройств, зараженных вредоносным программным обеспечением (или *вредоносной программой*), для создания возможности удаленного управления этими устройствами и использования их для совершения кибератак. *Бот-сеть* (т.е. сеть зараженных цифровых устройств, именуемых зомби) может использоваться для совершения других киберпреступлений, таких как *криптоджекинг*. *Криптоджекинг* – это способ, при помощи которого вычислительная мощность зараженных компьютеров используется для добычи *криптовалюты* (т.е. зашифрованной цифровой валюты) для извлечения финансовой выгоды лицом (лицами), контролирующим зараженные цифровые устройства (т.е. «*хозяином» бот-сети*) и/или лицами, нанявшими «хозяев» бот-сетей.

Киберпреступники могут также производить, иметь и/или распространять средства неправомерного использования компьютеров, включая технические устройства, вредоносное программное обеспечение (или *вредоносную программу*), а также пароли, коды доступа и другие данные, которые позволяют лицам получать незаконный доступ, перехватывать сообщения или иным образом причинять вред мишени. Статья 9 («правонарушения, связанные с неправомерным использованием средств информационных технологий») Конвенция Лиги арабских государств о борьбе с преступлениями в области информационных технологий предусматривает уголовную ответственность за следующие деяния: (1) производство, продажу, покупку, импорт, распространение или

предоставление: (a) любых инструментов или программ, разработанных или адаптированных для целей совершения преступлений, предусмотренных статьей 6 (преступление, связанное с получением незаконного доступа), статьей 7 (преступление, связанное с незаконным перехватом сообщений) и статьей 8 (преступление против целостности данных), (b) системного пароля, кода доступа или иных аналогичных данных, которые позволяют получить доступ к информационной системе с целью ее использования для совершения любого из преступлений, указанных в статьях с 6 по 8… и (2) приобретение любых средств или программ, упомянутых в двух пунктах выше, с целью их использования для совершения любого из преступлений, указанных в статьях с 6 по 8.

Точно так же Конвенция Совета Европы о киберпреступности запрещает производство, продажу, приобретение для использования, импорт, распространение или иные формы предоставления в пользование: устройств, включая компьютерные программы, разработанные или адаптированные прежде всего для целей совершения какого-либо из правонарушений, предусмотренных статьями 2-5 или 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, а также обладание этими предметами с намерением, чтобы они использовались с целью совершения любого из преступлений, признанных таковыми в статьях 2-5 (статья 6).

В Конвенции Совета Европы о киберпреступности (статья 6) такое незаконное поведение описывается как *противозаконное использование устройств*. В соответствии со статьей 6(3), государства «сохраняют за собой право не запрещать» деяния, перечисленные в статье 6, при условии, что такая оговорка не будет касаться «продажи, распространения или иных форм предоставления в пользование («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»). Кроме того, согласно статье 6(2), ««производство, продажа, приобретение для использования, импорт, владение, распространение или иные формы предоставления в пользование» предметов, перечисленных в статье 6, которые используются «не с целью совершения правонарушений, предусмотренных Статьями 2-5 настоящей Конвенции, а связаны, например, с разрешенным испытанием или защитой компьютерной системы», не влекут за собой уголовной ответственности. Таким образом, в этой статье признается двойное назначение этих средств – они могут, например, использоваться законным образом, а также использоваться неправомерно.

2. Правонарушения, связанные с использованием компьютерных средств.

Правонарушения, связанные с использованием компьютерных средств,

включают в себя преступления, совершаемые посредством кибертехнологий, «в целях извлечения личной или финансовой прибыли или причинения личного или финансового вреда» (УНП ООН, 2013, стр. 17). К этой категории отнесены киберпреступления, «в случае которых использование компьютерной системы или цифрового устройства является частью способа совершения преступления» (УНП ООН, 2013, стр. 19). В Проекте доклада УНП ООН «Всестороннее исследование проблемы киберпреступности» к этой широкой категории отнесены следующие киберпреступления:

Компьютерное мошенничество или подлог;

Компьютерные преступления, связанные с использованием персональных данных;

Распространение или контроль распространения спама;

Компьютерные преступления, касающиеся авторских прав или товарных знаков;

Деяния, предполагающие использование компьютера в целях причинения личного вреда;

Деяния, предполагающие использование компьютера в целях завлечения детей и груминга (УНП ООН, 2013, стр. 17).

Компьютерное мошенничество или подлог.

В соответствии с Конвенцией Совета Европы о киберпреступности, мошенничество и подлог считаются составной частью *правонарушений, связанных с использованием компьютерных средств* (т.е. компьютерного подлога и компьютерного мошенничества). В статье 7 Конвенции Совета Европы о киберпреступности *компьютерный подлог* определяется как «преднамеренные и противоправные ввод, изменение, удаление или блокирование компьютерных данных, влекущие 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». Такой вид киберпреступности также запрещен статьей 10 Конвенция Лиги арабских государств о борьбе с преступлениями в области информационных технологий.

Компьютерный подлог предполагает элементы персонализации, когда преступники выдают себя в сети за легитимных лиц, органы власти, учреждения и прочих субъектов в мошеннических целях. Киберпреступники могут выдавать себя за людей из законных организаций и учреждений, чтобы обманом вынудить их раскрыть личную информацию и предоставить преступникам деньги, товары и/или услуги. Отправитель электронного письма притворяется представителем легитимной организации или учреждения, пытаясь убедить пользователей поверить содержимому письма и следовать изложенным в нем инструкциям. Электронное письмо отправляется либо с ложного адреса электронной почты (который выглядит как подлинное электронное письмо от организации или агентства), либо с доменного имени, схожего с наименованием легитимной организации или учреждения (с незначительными изменениями).

Одним из распространенных методов является рассылка электронных писем, содержащих ссылку на веб-сайт, при нажатии на которую пользователи могут либо загрузить вредоносную программу в свои цифровые устройства, либо могут быть перенаправлены на вредоносный веб-сайт, созданный для кражи учетных данных пользователей (*фишинг*). «Ложный» веб-сайт (или *фальшивый* веб-сайт) выглядит как веб-сайт организации и/или учреждения и подсказывает пользователю, какие учетные данные необходимо ввести для входа на сайт. В электронном письме содержатся различные подсказки, чтобы вызвать страх, панику и/или ощущение срочности, которые заставят пользователя как можно скорее ответить на электронное письмо (и выполнить задачи, запрошенные в этом электронном письме), такие как необходимость обновления личной информации для получения денежных средств или других выплат, предупреждения о мошеннической активности в учетной записи пользователя и другие события, требующие безотлагательного внимания мишени.

Такой метод не носит целенаправленного характера, поскольку электронные письма рассылаются в массовом порядке, чтобы охватить как можно больше жертв. Целенаправленный вариант фишинга известен под названием *адресный фишинг.* При совершении мошенничества такого рода злоумышленники, знакомые с внутренними делами и должностями сотрудников компании, целенаправленно отправляют электронные письма сотрудникам, чтобы обманом их заставить раскрыть информацию и/или отправить деньги злоумышленникам. Еще один метод фишинга заключается в том, что киберпреступники выдают себя за высокопоставленных руководителей компании (входящих в высшее руководство – главный управляющий директор, главный финансовый директор и директор по безопасности), юристов, бухгалтеров и других лиц, занимающих руководящие и ответственные должности, чтобы обманом вынудить сотрудников отправить им денежные средства. Этот метод известен под названием *уэйлинг* (whaling – англ. «китобойный промысел»; *прим. пер.*), поскольку он позволяет преступникам получать от жертв самые большие размеры выплат.

Американская компания по производству игрушек Mattel стала жертвой *уэйлинг-мошенничества*. Киберпреступники, стоявшие за этой атакой, тайно контролировали компьютерные сети и коммуникации компании в течение нескольких месяцев до инцидента. После того как в компании было объявлено о назначении нового генерального директора, киберпреступники использовали личность нового генерального директора Кристофера Синклера (Christopher Sinclair) для совершения атаки. В частности, киберпреступники отправили электронное письмо от имени Кристофера Синклера, в котором просили получателя одобрить перевод на сумму три миллиона долларов в банк Вэньчжоу в Китае на счет китайского поставщика. Поскольку просьба поступила от генерального директора, сотрудница компании перевела деньги, но позже связалась с ним по этому поводу. Генеральный директор сказал, что не давал никаких указаний о переводе денег. После этого

компания Mattel связалась с правоохранительными органами США, Федеральным бюро расследований США, своим банком и правоохранительными органами Китая (Ragan, 2016). Время инцидента (деньги были переведены накануне праздника) позволило китайским властям вовремя заморозить счета до открытия банков, и компания Mattel смогла вернуть свои деньги.

Фишинг с использованием телефонных коммуникаций известен под названием *вишинг* (когда мошенники отправляют голосовое сообщение с просьбой позвонить на указанный номер и раскрыть личные и/или финансовые данные), а фишинг с использованием текстовых сообщений называется *смишингом* (или SMS-фишингом).

Виды компьютерного мошенничества включают в себя различные аферы в Интернете, которые предполагают дачу ложных или вводящих в заблуждение обещаний любви и дружбы (*кэтфишинг*), имущества (посредством аферы с наследством), а также денег и богатства (путем мошенничества с лотереями, мошенничества в инвестиционной сфере, афер с наследством и т.п.). Конечная цель таких мошенников заключается в том, чтобы заставить жертву раскрыть или иным образом предоставить личную информацию и/или средства злоумышленнику (это одна из разновидностей *мошенничества методом социальной инженерии*). Этот прием, как следует из названия, основан на использовании *социальной инженерии* (этот термин был популяризирован американским хакером Кевином Митником (Kevin Mitnick), практике «принуждения людей – путем манипулирования, введения в заблуждение, оказания влияния или обмана – к раскрытию конфиденциальной информации или совершению действий, которые принесут определенную пользу социальному инженеру» (Maras, 2014, p. 141).

Наиболее известным видом компьютерного мошенничества являются письма с просьбой произвести авансовый платеж для завершения операции по переводу денег, депонированию или иной трансакции в обмен на более крупную сумму денег (*мошенничество с авансовым платежом*, также известное под названием «афера 419»). Хотя история, которую рассказывают злоумышленники, постоянно меняется (они выдают себя за правительственных чиновников, банковских служащих, юристов и т.д.), они используют одну и ту же тактику – просят перевести небольшую сумму денег в обмен на более крупную сумму.

Компьютерные преступления, связанные с использованием персональных данных, и спам.

В дополнение к онлайновым схемам, в сети Интернет также совершаются некоторые виды финансового (или экономического) мошенничества, такие как банковское мошенничество, мошенничество с электронной почтой и мошенничество с кредитными и дебетовыми картами. Например, данные дебетовых и кредитных карт, полученные преступниками незаконным путем, продаются ими, передаются друг другу и используются в Интернете. В результате проведенной в 2018 году международной операции

по борьбе с киберпреступностью был закрыт один из самых известных онлайн кардинг-форумов Infraud, на котором преступники продавали данные кредитных и дебетовых карт и банковскую информацию и обменивались ими. Персональная, медицинская и финансовая информация, которая покупается, продается и обменивается в Интернете, может использоваться для совершения других преступлений, таких как *преступления, связанные с использованием персональных данных*, когда преступник неправомерно выдает себя за другого человека и/или незаконно присваивает себе идентификационные данные жертвы и/или использует эти идентификационные и/или личные данные в незаконных целях (UNODC, nd). Данные, которые являются целью преступников, включают в себя личные данные, такие как идентификационные номера (например, номера социального страхования в США), документы, удостоверяющие личность (например, паспорта, национальные идентификационные номера, водительские удостоверения и свидетельства о рождении), а также учетные данные в Интернете (т. е. имена пользователей и пароли) (UNODC, 2011, p. 12-15). Преступление, связанное с использованием персональных данных, может быть финансово-мотивированным или не быть таковым. Например, поддельные удостоверения личности (например, паспорта) могут приобретаться в Интернете для использования во время совершения поездок (UN-CCPCJ, 2017, p. 4). Такие виды преступлений, а также экономическое мошенничество совершаются через Интернет посредством рассылки незапрашиваемых электронных писем (*спама*), информационных бюллетеней и сообщений со ссылками на веб-сайты, которые созданы для того, чтобы вводить пользователей в заблуждение и обманом заставить их открывать электронные письма и информационные бюллетени или нажимать на ссылки в электронных письмах, которые могут содержать вредоносные программы или направлять пользователей на фальшивые веб-сайты.

Деяния, предполагающие использование компьютера в целях причинения личного вреда.

Согласно Проекту доклада УНП ООН «Всестороннее исследование проблемы киберпреступности» за 2013 год, «деяния, предполагающие использование компьютера в целях причинения личного вреда», включают в себя «использование компьютерной системы в целях домогательства, преследования, запугивания или угроз человеку».

Примерами таких видов киберпреступлений являются киберпреследование, кибердомогательство и кибертравля.

Эти киберпреступления не включены в многосторонние и региональные договоры о киберпреступности (например, Конвенцию Совета Европы о киберпреступности; Конвенцию Африканского союза о кибербезопасности и защите личных данных; и Конвенцию Лиги арабских государств о борьбе с преступлениями в области информационных технологий).

Термины киберпреследование, кибердомогательство и кибертравля используются взаимозаменяемо. В некоторых странах любое действие, которое совершается с участием ребенка, выступающего в качестве либо

жертвы, либо правонарушителя, называется кибертравлей (например, в Австралии и Новой Зеландии), в то время как в некоторых штатах США термин «кибертравля» используется для обозначения действий, совершаемых детьми и против детей. Некоторые страны не используют термин «кибертравля» и используют вместо него термин «кибердомогательство» или «киберпреследование», либо другие термины, такие как *кибермоббинг* (в Австрии и Германии), для обозначения кибертравли (European Parliament, Citizens' Rights and Constitutional Affairs, 2016, 24-25), в то время как другие страны не используют ни один из этих терминов. К таким странам относится, например, Ямайка, которая запрещает «злонамеренные и/или оскорбительные сообщения» в соответствии со статьей 9 (1) Закона «О киберпреступлениях» 2015 года, которая предусматривает, что лицо совершает преступление, если оно «(a)… использует компьютер для отправки другому лицу каких-либо данных (будь то в форме сообщения или иным образом), которые являются непристойными, представляют угрозу или носят угрожающий характер; и (b) путем отправки таких данных преднамеренно или по неосторожности причиняет раздражение, неудобство, беспокойство или волнение этому лицу или любому другому лицу».

Киберпреследование. Использование информационно-коммуникационных технологий (ИКТ) для совершения неоднократных действий в течение определенного периода времени с целью домогательства, беспокойства, нападок, угроз, запугивания и/или словесного оскорбления лица (или лиц).

Кибердомогательство. Использование ИКТ для преднамеренных действий с целью унижения, раздражения, нападок, угроз, запугивания, нанесения обиды и/или оскорбления лица (или лиц).

Кибертравля. Использование ИКТ детьми с целью досаждения, унижения, оскорбления, нанесения обиды, домогательства, запугивания, преследования, жестокого обращения или иных нападок в отношении других детей.

Различия между этими видами киберпреступлений заключаются в возрасте преступников (например, только дети осуществляют кибертравлю и являются ее жертвами), а также в интенсивности и частоте случаев совершения киберпреступления (киберпреследование предполагает серию инцидентов в течение определенного времени, в то время как кибердомогательство может включать в себя один или несколько инцидентов).

Завлечение детей или груминг.

Информационно-коммуникационные технологии используются для содействия в совершении «груминга» в отношении детей. *Груминг детей* – это процесс установления взаимопонимания и доверия через развитие эмоциональных отношений с жертвой (Maras, 2016, p. 244). Процесс груминга варьирует в значительных пределах с точки зрения стиля, продолжительности и интенсивности, что зачастую зависит от личных качеств и поведения преступника. Преступник может манипулировать жертвой, используя различные силовые методы и методы контроля, включая (в числе прочего):

лесть, подарки, изоляцию, запугивание, угрозы и/или насилие (Maras, 2016), а также симулирование общих интересов или завоевание доверия путем имитации кажущегося чувства одиночества ребенка. Груминг детей может совершаться на платформах социальных сетей, по электронной почте, в чатах, через службы обмена мгновенными сообщениями, приложения и т.д. Исследование, проведенное британской вещательной корпорацией BBC в 2017 году, показало, что приложение Periscope, которое позволяет вести прямую трансляцию в любой точке мира, использовалось злоумышленниками для груминга детей. Злоумышленники, которые связывались с детьми, участвовавшими в прямых трансляциях, высказывали сексуализированные комментарии о детях, а некоторые даже просили детей снять свою одежду (BBC, 2017).

3. Правонарушения, связанные с содержанием компьютерных данных.

Как видно из заголовка, киберпреступления, включенные в данный раздел, связаны с незаконным контентом. Показательным примером незаконного контента являются *материалы с изображением сексуального насилия над детьми*. Термин «материалы с изображением сексуального насилия над детьми» следует использовать вместо «*детской порнографии*», поскольку термин «детская порнография» минимизирует серьезность преступления. Материал, который просматривает лицо, изображает *не* сексуальную активность между ребенком и взрослым, а сексуальное насилие над ребенком. Тем не менее, в международных, региональных и национальных законах используется термин «детская порнография» вместо термина «материалы с изображением сексуального насилия над детьми». Статья 9 Конвенции Совета Европы о киберпреступности предусматривает уголовную ответственность за правонарушения, связанные с детской порнографией, причем концепция детской порнографии включает в себя визуальные изображения «участия несовершеннолетнего лица в откровенных сексуальных действиях, участия лица, кажущегося несовершеннолетним, в откровенных сексуальных действиях, реалистические изображения несовершеннолетнего лица, участвующего в откровенных сексуальных действиях». Эта концепция детской порнографии не является общепринятой; некоторые государства предусматривают уголовную ответственность за распространение нереалистических изображений детской порнографии, таких как мультфильмы и рисунки (например, Бразилия, Коста-Рика, Доминиканская Республика, Гватемала, Мексика, Никарагуа, Панама и Уругвай), в то время как другие государства предусматривают уголовную ответственность только за распространение изображений с участием реальных детей (например, Аргентина, Боливия, Чили, Колумбия, Эквадор, Сальвадор, Гондурас, Парагвай, Перу и Венесуэла) (ICMEC and UNICEF, 2016).

Коммерческая сексуальная эксплуатация детей – это термин, используемый для описания некоторых видов деятельности и преступлений, связанных с сексуальным насилием над детьми в обмен на какое-либо либо

денежное или неденежное вознаграждение (например, убежище, еда). Примером коммерческой сексуальной эксплуатации детей является *прямая трансляция сексуального насилия над детьми*, которая предполагает передачу и вещание в режиме реального времени сцен сексуального насилия над детьми, когда зрители могут быть пассивными или активными (т.е. они могут наблюдать и/или взаимодействовать с жертвой, просить самого ребенка о совершении определенных действий либо просить взрослых о совершении определенных действий в отношении ребенка) (UNODC, 2015). Эти и другие формы коммерческой сексуальной эксплуатации детей, такие как *торговля детьми в целях сексуальной эксплуатации*, которая предполагает «побуждение, вербовку, укрытие, перевозку, передачу или получение ребенка в возрасте до восемнадцати лет для целей коммерческого секса».

В некоторых странах публикация ложной информации также считается преступлением. В Танзании статья 16 Закона «О киберпреступлениях» 2015 года запрещает публикацию «информации или данных, представленных в виде изображения, текста, символа или в любой другой форме, в компьютерной системе, если лицо, публикующее эти данные и информацию заведомо знает, что они являются ложными, неверными, вводящими в заблуждение или неточными и публикуются с целью опорочивания, угрозы, оскорбления, нанесения обиды либо обмана или введения в заблуждение общественности иным образом, либо с целью пособничества в совершении преступления в виде дачи советов». Закон Кении «О неправомерном использовании компьютерных технологий и киберпреступлениях» 2018 года также предусматривает уголовную ответственность за «заведомое… обнародование ложной информации в печатных и вещательных средствах массовой информации или через компьютерную систему, которая влечет за собой панику, хаос или насилие среди граждан республики или рассчитана на распространение паники, хаоса или насилия, либо может привести к дискредитации репутации лица» (статья 23). Тем не менее, согласно Проекту доклада УНП ООН «Всестороннее исследование проблемы киберпреступности» 2013 года, «страны сообщают о различной степени ограничения свободы выражения мнения, в том числе в отношении диффамации, неуважения, угроз, подстрекательства к ненависти, оскорбления религиозных чувств, непристойных материалов и подрыва государственных устоев» (УНП ООН, 2013, стр. 21). В ряде случаев случаях удаление правительственными структурами Интернет-контента, относящегося к таким формам выражения мнения, вызывало озабоченность в контексте соблюдения прав человека.

В 2005 году Совет безопасности ООН принял резолюцию 1624, которая (в числе прочего) призывает все государства «принять такие меры, которые могут быть необходимы и уместны и будут соответствовать их обязательствам по международному праву, чтобы: … законодательно запретить подстрекательство к совершению террористического акта или актов… и предотвращать такое поведение» (UNSCR 1624 (2005). Меры, которые государства-участники могут принять с целью достижения этой цели,

включают в себя криминализацию подстрекательства к терроризму.

Другие международные органы также призывают государства принять меры по борьбе с подстрекательством к терроризму в рамках своих национальных правовых систем. Например, статья 3 Рамочного решения Совета Европейского союза 2008/919/JHA от 28 ноября 2008 года о внесении поправок в Рамочное решение 2002/475/JHA о борьбе с терроризмом и статья 5 Конвенции Совета Европы о предупреждении терроризма 2005 года обязывают соответствующие государства-участников ввести уголовную ответственность за действия или заявления, представляющие собой подстрекательство к совершению террористических актов. Кроме того, Конвенция Совета Европы о предупреждении терроризма налагает на государства-участников обязательство по криминализации «публичного подстрекательства к совершению террористических преступлений», а также вербовки и подготовки террористов (UNODC, 2012, pp. 39-40).

Хотя в настоящее время в международном праве не существует универсального обязательства, имеющего юридическую силу для всех государств, по криминализации действий, связанных с подстрекательством к терроризму, многие государства используют правовые и уголовно-правовые подходы к борьбе с такими действиям и актами. Примерами подходов, используемых в некоторых странах, являются использование Соединенными Штатами параграфа 373 (a) титула 18 Свода законов США, который запрещает подстрекательство и сговор, для успешного преследования виновных в совершении действий, связанных с подстрекательством к терроризму (например, дело *United States of America v. Emerson Winfield Begolly,* UNODC, 2012, pp. 39-41), а также использование властями Великобритании статьи 1 Закона «О терроризме» 2006 года, который предусматривает уголовную ответственность за «поощрение терроризма» следующим образом:

Лицо совершает преступление, если:

(a) оно публикует заявление, на которое распространяется действие настоящей статьи, или побуждает другое лицо к публикации такого заявления;

(b) в момент, когда оно публикует это заявление или побуждает другое лицо к его публикации, оно:

(i) преследует цель, чтобы это заявление было понято представителями общественности как прямое или косвенное поощрение или иное побуждение к совершению, подготовке или подстрекательству к актам терроризма или преступлениям, предусмотренным Конвенцией;

или безразлично относится к тому, будет ли это заявление понято представители общественности как прямое или косвенное поощрение или иное побуждение к совершению, подготовке или подстрекательству к актам терроризма или преступлениям.

Власти Великобритании уже имеют успешный опыт уголовного преследования деяний, связанных с подстрекательством к терроризму, в соответствии с Законом «О терроризме» 2000 года. См. дело Юниса Тсули (Younes Tsouli) и других лиц, которые были осуждены на основании этого закона за подстрекательство к терроризму за рубежом путем размещения

материалов на веб-сайтах и в чатах, которые они создали, администрировали и контролировали (UNODC, 2012, p. 114).

Несмотря на отсутствие в международном праве какого-либо универсального юридически обязывающего обязательства государств осуществлять меры по борьбе с подстрекательством к терроризму, многие государства приняли такие меры на национальном уровне. Однако некоторые факторы продолжают создавать трудности для принятия согласованного на международном уровне подхода к решению этой проблемы, включая отсутствие общепринятого определения терроризма и различия в национальных конституционных и правовых подходах к основным правам человека, таким как право на свободное выражение мнений и свободу объединений, конфиденциальность и т.д. Поэтому перед законодателями, правоохранительными органами и органами уголовного правосудия всех государств по-прежнему стоит трудная задача принятия и внедрения национальных подходов, которые нацелены на информационные материалы в Интернете, подстрекающие к насильственным актам терроризма, и не оказывают при этом «ограничительного воздействия» на легитимное и законное право на выражение определенных политических или идеологических взглядов (см. UNODC, 2012, pp. 39-41).

Вопросы для обсуждения:

1. Каковы общие категории киберпреступлений?
2. Какие киберпреступления попадают в эти категории?
3. Есть ли преступления, которые подпадают под более чем одну категорию?
4. Если да, то какие?
5. Дайте определение киберпреступности. Как совершается это преступление?
6. Опишите процесс подробно.

Тема 3. Правовая база и права человека.

1. Роль законодательство о киберпреступности. Законодательство о киберпреступности определяет стандарты приемлемого поведения для пользователей информационно-коммуникационных технологий (ИКТ); устанавливает социально-правовые санкции за киберпреступления; защищает пользователей ИКТ в целом и смягчает и/или предотвращает вред, причиняемый людям, данным, системам, сервисам и инфраструктуре в частности; защищает права человека; обеспечивает возможность для проведения расследований и осуществления уголовного преследования в отношении преступлений, совершаемых в сети Интернет (вне пределов реального мира); и содействует сотрудничеству между странами по делам, связанным с киберпреступлениями (УНП ООН, 2013, стр. 57). Законодательство в области киберпреступности предусматривает правила и стандарты поведения при использовании Интернета, компьютеров и

связанных с ними цифровых технологий и действия публичных, государственных и частных организаций; нормы доказательственного права, правила осуществления уголовного судопроизводства и прочие вопросы уголовного права, связанные с киберпространством; положения о снижении риска и/или смягчении вреда, причиненного физическим лицам, организациям и инфраструктуре в случае совершения киберпреступления. Таким образом, законодательство в области киберпреступности включает в себя материальное, процессуальное и превентивное право.

Материальное право. Незаконное деяние должно быть четко прописано в законе и запрещено законом. В соответствии с моральным принципом *«nullum crimen sine lege»* (лат. «нет преступления без предусматривающего его закона»), лицо не может быть подвергнуто наказанию за деяние, которое не было прописано в законе на момент совершения лицом этого деяния (УНП ООН, 2013, стр. 59). *Материальное право* определяет права и обязанности субъектов права, к которым относятся физические лица, организации и государства. Источниками материального права являются нормативно-правовые акты и распоряжения, принимаемые местными и центральными законодательными органами (*статутное право*), федеральные конституции и конституции федеральных единиц, а также судебные решения в системах общего права.

Материальное законодательство в области киберпреступности включает в себя законы, которые запрещают конкретные виды киберпреступлений, и предусматривает наказание за несоблюдение этих законов. К киберпреступлениям относятся традиционные преступления в реальном мире, вне сети Интернета (например, мошенничество, подлог, организованная преступность, отмывание денег и кража), совершаемые в киберпространстве, которые являются «гибридными» преступлениями или «преступлениями с использованием киберсетей», а также «новыми» или «киберзависимыми» преступлениями, которые стали возможными с изобретением Интернета и цифровых технологий, функционирующих через Интернет (Maras 2014; Maras, 2016). Поэтому многие страны разработали законы, которые конкретно предназначены для противодействия киберпреступности. Например, Германия, Япония и Китай внесли поправки в соответствующие положения своих уголовных кодексов с целью борьбы с киберпреступлениями. Некоторые страны также использовали действующие законы, которые были разработаны для борьбы с преступностью в реальном мире (вне сети Интернета), чтобы охватить определенные виды киберпреступности и киберпреступников. В качестве еще одного примера можно привести Ирак, где действующие гражданский кодекс (Гражданский кодекс Ирака №40 от 1951 года) и уголовный кодекс (Уголовный кодекс Ирака №111 от 1969 года) используются для судебного преследования за преступления, совершаемые в реальном мире, например, мошенничество, шантаж, хищение персональных данных с использованием Интернет и цифровых технологий.

Некоторые страны, вместо разработки новых специальных законов по борьбе с киберпреступностью, внесли поправки в свои национальные

законодательства или кодексы, дополнив их отдельными положениями, касающимися киберпреступлений. Эта практика имела любопытные, заслуживающие внимания последствия, которые заключались в том, что некоторые страны решили отдельно криминализировать деяние, связанное с незаконным использованием информационно-коммуникационных технологий для совершения какого-либо преступления. Таким образом, если бы преступник использовал незаконный доступ для совершения подлога или мошенничества, такое деяние образовало бы одновременно два преступления.

Правовые системы. Каждое государство имеет свою собственную правовую систему, которая влияет на создание материального уголовного права в области киберпреступности. Эти системы включают в себя (Maras, 2020) (готовится к публикации):

1) *Общее право*. Страны с системой общего права создают законы на основе *судебных прецедентов* (т.е. решение, вынесенное по делу, является обязательным для суда и нижестоящих судов) и устоявшейся практики. Эти законы существуют в виде отдельных законов и *прецедентного права* (т.е. права, которое формируется на основе решений судов или судебных прецедентов).

2) *Гражданское право.* Страны с такой системой права имеют кодифицированные, консолидированные и всеобъемлющие правовые нормы и законоположения, которые устанавливают границы основных прав, обязательств, обязанностей и ожиданий в отношении поведения. Эти системы основаны преимущественно на законодательстве и конституциях.

3) *Обычное право*. Эти правовые системы включают в себя укоренившиеся и общепринятые модели поведения в рамках культуры, которые воспринимаются носителями этой культуры в качестве закона (*opinio juris – убежденность в правомерности)*. В международном праве обычное право регулирует взаимоотношения и практику между государствами и считается обязательным для всех государств.

4) *Религиозное право.* В системах религиозного права в качестве источника права используются правила, основанные на религиозных учениях или религиозной литературе.

5) *Правовой плюрализм*. В правовой системе такого типа возможно сосуществование двух или более вышеупомянутых правовых систем (т.е. общего, гражданского, обычного или религиозного права).

Материальное право сосредоточено на *существе* преступления, например, элементах состава преступления, которые включают в себя запрещенное деяние (*actus reus* – «виновное действие») и субъективную сторону (*mens rea* – «преступный умысел»). Разные страны могут отдавать предпочтение криминализации различных деяний на основе разных элементов, образующих состав преступления. В качестве альтернативы страны могут криминализовать те же самые деяния, однако законы могут различаться с точки зрения того, какая «субъективная сторона» делает лиц виновными за такое деяние (т.е. с точки зрения степени уголовно-правовой вины). В этой связи законы, которые криминализируют, например,

несанкционированный доступ к компьютерным системам и данным, отличаются в разных странах в зависимости от степени намерения предполагаемого преступника.

Уровни (формы) уголовно-правовой вины. Существуют разные уровни уголовно-правовой вины или уголовной ответственности в зависимости от степени, в которой незаконное действие было преднамеренным (совершенным сознательно или умышленно) или непреднамеренным (совершенным по опрометчивости или по неосторожности), которая в разных правовых системах толкуется по-разному (Maras, 2020):

Сознательно. Лицо *сознательно* совершает преступление, когда оно действует с целью причинения вреда (т.е. лицо имеет *намерение* причинить вред). В качестве примера можно привести Закон Соединенного Королевства о неправомерном использовании компьютерных технологий 1990 года, который криминализирует, в числе прочего, несанкционированный доступ к системам и данным с намерением вызвать изменения и/или повреждения, нарушения нормальной работы систем и сервисов и модификации системных данных и программ.

Умышленно. Лицо *умышленно* совершает преступление, когда ему известно о том, что его действие причинит вред, но оно, тем не менее, совершает такое действие и причиняет вред. В соответствии с Законом «О компьютерном мошенничестве и злоупотреблении» 1986 года, в частности, параграфом 1030(a)(1) раздела 18 Свода законов США, лицу могут быть предъявлены обвинения, если оно:

- сознательно проникнув в компьютер без необходимых на то санкций или преступив границы санкционированного доступа и посредством данного действия получив информацию, которая была определена Правительством Соединенных Штатов согласно указу или акту исполнительной власти как требующая защиты от несанкционированного раскрытия из соображений национальной обороны или международных отношений, либо получив какую-либо закрытую информацию, как это определено в параграфе «y» статьи 11 Закона «Об атомной энергии» от 1954 года, при наличии основания полагать, что полученная таким образом информация может использоваться с целью причинения вреда Соединённым Штатам или в пользу какого-либо иностранного государства, умышленно сообщает, направляет, передает либо принимает меры для сообщения, направления или передачи, либо пытается сообщить, направить, передать или принять меры для сообщения, направления или передачи такой информации любому лицу, которое не имеет права получать ее, либо умышленно сохраняет эту информацию и не передает ее должностному лицу или служащему Соединенных Штатов, которое имеет право на ее получение.

По опрометчивости (или легкомыслию). Лицо совершает преступление *по опрометчивости,* когда оно совершает акт, даже несмотря на то, что оно осознает существенный и неоправданный риск причинения вреда другим лицам, однако демонстрирует пренебрежение или безразличие к

такому риску причинения вреда. В Австралии лицу могут быть предъявлены обвинения на основании положений раздела 477.2(1)(c) Закона «О киберпреступности» 2001 г. (№161, 2001), если «лицо опрометчиво не осознает того, что несанкционированное изменение данных нарушает или нарушит: доступ к этим или любым другим данным, хранящимся в любом компьютере; либо достоверность, безопасность или применимость любых таких данных».

По неосторожности. *Неосторожность* представляет собой самую низкую степень виновности. Лица, совершающие какие-либо действия по неосторожности, не осознают негативных последствий своего поведения. В Сенегале «любое лицо, которое, даже по неосторожности, обрабатывает или организует обработку персональных данных без соблюдения формальных требований, изложенных в Законе «О персональных данных», до использования таких данных, подлежит наказанию» (статья 431-17 Закона №2008-11 «О киберпреступности»)

Здесь важно отметить два момента. Во-первых, местное применение закона (уголовное преследование) возможно лишь в том случае, когда уголовное преследование отвечает интересам общества, при этом большое количество массовых киберпреступлений, таких как мошенничество через Интернет, относятся к малозначительным в соответствии с принципом *de minimis non-curat lex* (лат. закон не заботится о мелочах), в том смысле, что по отдельности они считаются слишком незначительными по своим последствиям, чтобы оправдать расследование полицией или уголовное преследование. Тем не менее, они могут повлечь за собой значительные совокупные последствия в международном масштабе, поэтому они должны подпадать под действие международного права. Во-вторых, «при отсутствии надежного обоснования криминализации определенных деяний возникает риск чрезмерной криминализации. В этом плане международное право в области прав человека является одним из важных инструментов, необходимых для оценки уголовного права в соответствии с внешними, международными стандартами» (УНП ООН, 2013, стр. 60).

Процессуальное право. *Процессуальное право* определяет границы процессов и процедур, которые необходимо соблюдать при применении норм материального права, а также правила, обеспечивающие возможность для применения материального права. Важной частью процессуального законодательства является *уголовно-процессуальное право*, которое включает в себя исчерпывающие правила и руководящие принципы в отношении того, как должны обращаться с подозреваемыми, обвиняемыми и осужденными лицами система уголовного правосудия и ее сотрудники. Наконец, процессуальное законодательство в области киберпреступности включает в себя положения о юрисдикции и следственных полномочиях, нормы доказательственного права и правила осуществления уголовного судопроизводства, которые относятся к процедурам сбора данных, перехвата сообщений, обыска и выемки, сохранения и хранения данных. Киберпреступность создает некоторые уникальные сложности, касающиеся

процедур, особенно тех, которые связаны с юрисдикцией, расследованиями и цифровыми доказательствами.

Юрисдикция. Правоохранительные органы вправе осуществлять расследование киберпреступлений, а национальные суды вправе выносить решения по делам о киберпреступлениях только в тех случаях, если заинтересованное государство обладает соответствующей юрисдикцией. Под юрисдикцией понимается право и полномочия государства применять законы и назначать наказание за несоблюдение законов. Вопрос юрисдикции тесно связан с государственным суверенитетом, т.е. с правом государства осуществлять полномочия на своей собственной территории (УНП ООН, 2013, стр. 61). Юрисдикция обычно связана с географической территорией или *locus commissi deliciti* (место совершения преступления), когда государство заявляет о своей юрисдикции в отношении преступлений, совершенных на его территории и осуществляет преследование виновных в их совершении (*принцип территориальности*). Учитывая отсутствие географических границ и территорий в киберпространстве, местоположение не может использоваться для определения юрисдикции. Поэтому государства используют целый рядиных факторов, чтобы определить юрисдикцию (Maras, 2020) (готовится к публикации). Одним из таких факторов является гражданство правонарушителя (*принцип государственной принадлежности; принцип активной правосубъектности*). Этот принцип признает право государств осуществлять преследование своих граждан, даже если эти граждане находятся за пределами их территории. В меньшей степени (с точки зрения применимости) для установления юрисдикции в отношении преступления может использоваться гражданство потерпевшего (*принцип государственной принадлежности; принцип пассивной правосубъектности*). Государство может также устанавливать юрисдикцию в том случае, когда преступление, совершенное в другом государстве (например, государственная измена или шпионаж), нанесло ущерб интересам и безопасности государства, добивающегося осуществления юрисдикции в отношении этого преступления (*принцип защиты*). Наконец, любое государство может установить юрисдикцию в отношении определенных транснациональных преступлений, таких как массовые злодеяния (например, геноцид), которые рассматриваются как преступления, затрагивающие всех людей, независимо от географического местоположения, когда государство, на территории которого было совершено преступление, не желает или не в состоянии осуществлять преследование виновных лиц (*принцип универсальности*).

Следственные действия и полномочия. Цифровые доказательства киберпреступлений сопряжены с особыми трудностями – как в плане обращения с ними, так и с точки зрения их использования в судебном производстве. Как отмечалось в проекте доклада УНП ООН «Всестороннее исследование проблемы киберпреступности» в 2013 году, «в то время как некоторые такие следственные действия могут быть осуществлены на основании традиционных полномочий, многие процессуальные положения, в основе которых лежит пространственный, объектно-ориентированный

подход, трудно применять в ситуациях, связанных с хранением цифровых данных и потоками данных в режиме реального времени», поэтому для проведения расследования необходимы специальные полномочия (УНП ООН, 2013, стр. 60). Такие специальные полномочия предусматриваются законом и не только распространяются на доступ к необходимой информации, но и включают в себя гарантии для обеспечения того, чтобы данные были получены в соответствии с надлежащими законными распоряжениями и были доступны только в той степени, в которой это необходимо и разрешено законом. Закон США о сохраненных сообщениях (титул 18 Свода законов США, § 2701-2712), представляющий собой титул II Закона «О конфиденциальности электронных сообщений» 1986 года, предусматривает такие гарантии. Например, согласно параграфу 2703(a) титула 18 Свода законов США: государственное учреждение вправе требовать от провайдера услуг электронных коммуникаций раскрытия содержания проводных или электронных сообщений, хранящихся в электронном хранилище системы электронных коммуникаций в течение не более ста восьмидесяти дней, только на основании ордера, выданного в соответствии с процедурами, описанными в Федеральных правилах уголовного производства (или, в случае суда штата, выданного в соответствии с порядком выдачи судебных ордеров, действующим в этом штате), судом компетентной юрисдикции.

Однако эти гарантии, т.е. требование о наличии законного распоряжения требуются не во всех странах. В 2014 году Турция внесла поправки в Закон №5651 «Об Интернете», чтобы требовать от интернет-провайдеров сохранения данных пользователей и предоставлять их властям по первому требованию без необходимости получения законного распоряжения (например, решения суда или ордера на обыск) для получения этих данных. Такие следственные полномочия выходят за рамки обычного сбора доказательств и предполагают получение содействия и взаимодействие с другими представителями системы уголовного правосудия по делам, связанным с киберпреступностью. Такая же ситуация сложилась в Танзании, где Закон «О киберпреступности» 2015 года наделил полицию чрезмерными, неограниченными следственными полномочиями в отношении киберпреступлений. В частности, санкция полиции является единственным требованием для производства обыска и выемки доказательств и принуждения к раскрытию данных. Соответственно, обыск и выемка, а также прочие следственные действия могут производиться без наличия надлежащих законных распоряжений. Кроме того, существует опасность «размывания мандата (отклонения от основного)» или «размывания функций» (эти термины используются для описания случаев распространения законов и/или иных мер на области, находящиеся за пределами их первоначальной сферы действия), когда законы и следственные полномочия, изначально направленные на один вид киберпреступности, впоследствии распространяются на другие, менее тяжкие виды киберпреступлений. В конечном счете полномочия и процедуры, используемые с целью расследования киберпреступлений и судебных разбирательств, должны соответствовать принципам верховенства закона и

стандартам в области прав человека (см., например, статью 15 Конвенции Совета Европы о киберпреступности 2001 года).

Идентификация, сбор, обмен, использование и допустимость цифровых доказательств. Процессуальное законодательство в области киберпреступности охватывает аспекты идентификации, сбора, хранения, анализа и обмена цифровых доказательств. К цифровым доказательствам (или электронным доказательствам) относится «информация любого типа, которую можно извлечь из компьютерных систем или иных цифровых устройств, и которая может использоваться для доказательства или опровержения факта правонарушения» (Maras, 2014). Цифровые доказательства могут подтвердить или опровергнуть показания потерпевшего, свидетеля и подозреваемого, подтвердить или опровергнуть правдивость утверждения о факте, определить мотив, намерение и местоположение правонарушителя, определить поведение правонарушителя (действия и поведение в прошлом) и установить степень уголовно-правовой вины (Maras 2014; Maras, 2016).

Нормы доказательственного права и правила уголовного судопроизводства включают в себя критерии, используемые для определения допустимости цифровых доказательств в суде (Maras, 2014). В них описываются процедуры документирования, сбора, сохранения, передачи, анализа, хранения и защиты цифровых доказательств с целью обеспечения их допустимости в национальных судах. Для того чтобы цифровые доказательства были допустимыми в суде, проводится их аутентификация и устанавливается их целостность. Процедуры аутентификации включают в себя определение источника/автора цифровых доказательств (например, идентификационной информации об источнике) и проверку целостности доказательств (например, на предмет того, что они не были каким-либо образом изменены, подтасованы или повреждены). Важнейшее значение для обеспечения допустимости цифровых доказательств в большинстве судов является *система охраны доказательств*, которая включает в себя подробный учет доказательств, их состояния, процессов сбора, хранения, получения доступа и передачи, а также причин получения доступа и передачи (УНП ООН, 2013, стр. 60; Maras, 2014). В разных странах действуют разные стандарты норм доказательственного права и правил уголовного судопроизводства. Для борьбы с киберпреступностью необходимы схожие нормы доказательственного права и уголовного судопроизводства, поскольку преступления такого типа не знают границ и воздействуют на цифровые доказательства и системы в любой точке мира посредством подключения к сети Интернет.

Превентивное право. Превентивное право основано на регулировании и снижении рисков правонарушений. В контексте киберпреступности цель превентивного законодательства заключается либо в предотвращении киберпреступлений, либо, как минимум, в смягчении ущерба, причиняемого в результате совершения киберпреступлений (УНП ООН, 2013, стр. 61). Законы «О защите данных» (например, Общие положения о защите данных ЕС 2016 года и Конвенция Африканского союза о кибербезопасности и защите

персональных данных 2014 года, и законы о кибербезопасности (например, Закон Украины «Об основных принципах обеспечения кибербезопасности Украины» 2017 года) приняты с целью снижения материального ущерба в результате киберпреступлений, связанных с утечкой личных данных, и/или минимизации уязвимости граждан к киберпреступлениям. Другие законы позволяют сотрудникам системы уголовного правосудия выявлять и расследовать киберпреступления и осуществлять уголовное преследование виновных путем обеспечения возможности для использования необходимых средств, мер и процедур, облегчающих осуществление таких действий (например, инфраструктуры поставщиков телекоммуникационных услуг и услуг электронной связи, которая дает им возможность перехвата сообщений и сохранения данных). В Соединенных Штатах Америки Закон «О содействии правоохранительным органам в области коммуникаций» (CALEA) 1994 года (кодифицирован в титуле 47 Свода законов США, параграф 1001-1010) обязывает провайдеров телефонной связи и производителей оборудования принимать меры для того, чтобы их сервисы и продукты обеспечивали органам власти, имеющим законное разрешение (например, надлежащий судебный ордер), возможность для получения доступа к линиям связи.

2. Унификация законодательства.

Борьба с киберпреступностью может осуществляться и осуществляется путем применения действующих законов, которые охватывают правонарушения, совершаемые вне сети Интернета; внесения поправок в законы для включения положений, касающихся киберпреступлений; и принятия законов, конкретно нацеленных на борьбу с киберпреступностью. Однако действующие законы могут оказаться неприменимыми к киберпреступлениям, поскольку они могли быть приняты до появления Интернета и цифровых технологий и/или могли разрабатываться без учета Интернета и цифровых технологий. Поэтому законы, которые созданы для борьбы с преступлениями, не относящимися к киберпреступности, могут иметь ограниченные последствия для киберпреступников и прочих правонарушителей, действия которых сопряжены с информационно-коммуникационными технологиями (ИКТ) в качестве предмета, либо средства совершения преступления. В связи с этим может возникнуть необходимость в принятии специальных законов, касающихся киберпреступности. Вопрос необходимости принятия законов в области киберпреступности «зависит от характера отдельных деяний, а также от охвата и интерпретации национального законодательства» (УНП ООН, 2013, стр.52).

Рассмотрим случай 2013 года, связанный с сексуальным надругательством с использованием изображений (именуемое в разговорной речи как «порноместь»), которое является одной из форм домогательства в киберпространстве, предполагающего «создание, распространение и угрозу распространения изображений интимного или сексуального характера без соответствующего на то обоюдного согласия» (Henry, Flynn and Powell, 2018, p. 566), чтобы «расстроить, унизить жертву и/или причинить ей вред иного

характера» (Maras, 2016, p. 255), когда лицо, совершившее такое надругательство, не могло быть привлечено к уголовной ответственности на основании действующих законов Нью-Йорка. В частности, преступник выложил фотографии своей подруги (бывшей таковой на момент инцидента) в обнаженном виде в «Twitter» и отправил эти фотографии по электронной почте сестре и работодателю своей подруги (*People v. Barber*, 2014). Ему были предъявлены обвинения, среди которых было обвинение в домогательстве при отягчающих обстоятельствах во второй степени. Согласно статье 240.30(1)(a) Уголовного закона штата Нью-Йорк, «лицо признается виновным в домогательстве при отягчающих обстоятельствах во второй степени, когда, с целью домогательства, причинения беспокойства, угрозы или запугивания другого лица, оно связывается с лицом, анонимно или иным способом, по телефону, телеграфу или по электронной почте, либо путем передачи или доставки письменного сообщения любой иной формы таким способом, который может причинить беспокойство или испуг». Поскольку этот закон распространяется на прямые коммуникации между потерпевшим и правонарушителем, суд, рассматривавший дело *People v. Barber* (2014), постановил, что деяние подсудимого (т.е. отправление фотографий подруги в обнаженном виде по электронной почте сестре и работодателю потерпевшей и размещение этих фотографий в «Twitter») не являются домогательством при отягчающих обстоятельствах. Такой пример ограниченного распространения закона на Интернет-пространство является далеко не единственным. Как отмечалось в проекте доклада УНП ООН «Всестороннее исследование проблемы киберпреступности» в 2013 году, «многие традиционные законы общего права не учитывают особенности информации и информационных технологий, которые применяются для совершения киберпреступлений и преступлений, при совершении которых образуются электронные доказательства».

3. Международные и региональные правовые документы.

Существуют международные и региональные договоры в области борьбы с киберпреступностью. Одним из примеров является Конвенция Совета Европы о киберпреступности 2001 года. Цель этой конвенции заключается в унификации национальных законодательств, совершенствовании методов расследования киберпреступлений и расширении международного сотрудничества. Она также содержит рекомендации для государств-участников конвенции в отношении мер, которые необходимо принять на национальном уровне для борьбы с киберпреступностью, включая внесение поправок и дополнений в нормы материального права (например, введение ответственности за правонарушения, связанные с киберпреступностью, в уголовное законодательство) и уголовно-процессуальное право (например, определение порядка осуществления уголовного расследования и судебного преследования). Конвенция также содержит рекомендации для государств-участников в отношении взаимной помощи и служит в качестве *договора об оказании взаимной правовой помощи* (т.е. соглашения между странами о сотрудничестве в расследовании и

уголовном преследовании по некоторым и/или всем правонарушениям, признанным таковыми в национальных законодательствах обеих сторон; Maras, 2016) для стран, которые не имеют подобного договора со страной, запрашивающей помощь.

Существуют несколько договоров в сфере борьбы с киберпреступностью, имеющих региональный характер.

Соглашение о сотрудничестве в борьбе с преступлениями в сфере компьютерной информации, подписанное странами-членами Содружества Независимых Государств в 2001 году. Это соглашение призывает государства принять национальные законы для выполнения положений соглашения и унификации национальных законодательств в сфере борьбы с киберпреступностью.

Конвенция Лиги арабских государств о борьбе с преступлениями в области информационных технологий, принятая Лигой арабских государств в 2010 году. Основная цель этой конвенции заключается в укреплении сотрудничества между государствами для обеспечения им возможности защиты своего имущества, населения и интересов от киберпреступности.

Соглашение о сотрудничестве в области обеспечения международной информационной безопасности, принятое Шанхайской организацией сотрудничества в 2010 году. Действие этого соглашения выходит за пределы киберпреступности и кибербезопасности и включает в себя меры обеспечения информационной безопасности государств-участников в качестве одной из главных целей соглашения, а также меры по национальному контролю за информационными системами и их контентом.

Конвенция Африканского союза о кибербезопасности и защите персональных данных 2014 года. Эта конвенция содержит, в числе прочих положений, призыв к государствам Африканского союза принимать национальные законы и/или вносить поправки в действующие национальные законы с целью эффективной борьбы с киберпреступностью, унифицировать национальные законодательства, заключать договоры о взаимной правовой помощи (ДВПП), если они еще не заключены, способствовать обмену информацией между государствами, содействовать региональному, межправительственному и международному сотрудничеству и использовать имеющиеся средства для сотрудничества с другими государствами и даже частным сектором.

Региональными организациями и/или региональными межправительственными организациями были также разработаны и имплементированы законы и директивы в сфере борьбы с киберпреступностью. Например, Типовой закон «О компьютерных преступлениях и киберпреступности» Сообщества развития Юга Африки (САДК) 2012 года. Этот закон служит руководством для государств-участников САДК для разработки норм материального и процессуального права в области борьбы с киберпреступностью. Поскольку этот закон является типовым, он не налагает на государства каких-либо юридических обязательств в отношении осуществления сотрудничества. Государства, которые не имеют

и/или не разрабатывают законы о киберпреступности, могут использовать Протокол САДК о взаимной правовой помощи по уголовным делам и Протокол САДК о выдаче для способствования сотрудничеству и координации при осуществлении международных расследований киберпреступлений; - Директива о борьбе с киберпреступностью Экономического сообщества западноафриканских государств (ЭКОВАС) 2011 года. Эта директива требует от государств-участников криминализации киберпреступности в национальном законодательстве и способствует взаимной правовой помощи, сотрудничеству и выдаче преступников в делах, связанных с киберпреступностью и кибербезопасностью. ЭКОВАС принял Конвенцию о взаимной правовой помощи по уголовным делам и Конвенцию о выдаче с целью способствования сотрудничеству в расследовании киберпреступлений и выдаче киберпреступников.

4. Международное право в области прав человека и законодательство о киберпреступности.

Основные положения некоторых законов о борьбе с киберпреступлениями, особенно теми, которые связаны с контентом в Интернете такими как неуважение к властям, оскорбление, диффамация главы государства, непристойность или порнографические материалы, могут чрезмерно ограничивать возможность осуществления определенных прав человека. Процессуальные нормы законов о киберпреступности, обеспечивающие возможность для использования при расследовании киберпреступлений средств и методов, которые позволяют перехватывать сообщения и осуществлять электронное наблюдение, также могут привести к неоправданному ограничению возможностей осуществления прав человека, таких как право на неприкосновенность частной жизни (УНП ООН, 2013, стр. 136). Необходимо соблюдать баланс между борьбой с киберпреступностью и соблюдением прав человека. Международное законодательство в области прав человека позволяет вводить ограничения на осуществление определенных прав человека, которые могут ограничиваться на законных основаниях в особых условиях (некоторые права не могут подлежать ограничению). Эти ограничения являются допустимыми, когда они преследуют законную цель, соответствуют действующему законодательству и являются необходимыми и соразмерными угрозе, которая оправдывает их применение. Конкретный охват законных целей зависит от применимых прав человека и может включать в себя интересы общественной безопасности, национальной безопасности, экономической безопасности, охраны здоровья, защиты нравственности и защиты прав других лиц. В дополнение к необходимости введения ограничений для достижения одной из вышеупомянутых законных целей, ограничение должно вводиться на основании национального закона. Этот закон должен быть доступен гражданам, чтобы они могли соответствующим образом следить за своим поведением, знать о полномочиях властей при применении этого закона, а также о последствиях его несоблюдения. Закон должен быть четко

сформулирован и не должен допускать предоставления государственным органам власти неограниченной свободы действий при применении ограничений. Расплывчатые и чрезмерно широкие оправдания, такие как неконкретные ссылки на «национальную безопасность», «экстремизм» или «терроризм», не подходят под определение четко сформулированных законов. Слово «необходимое» означает, что ограничение должно быть чем-то большим, чем «целесообразное», «разумное» или «желательное» (ЕСПЧ, дело «Санди Таймс» (The Sunday Times) против Соединенного Королевства, постановление суда от 26 апреля 1979 года, пункт 59). Кроме того, должна существовать соответствующая связь между законной целью, которую преследует государство, и действиями государства по достижению этой законной цели. Иными словами, действия должны быть соразмерны защищаемым интересам. Из этого следует, что ограничение является наименее интрузивной мерой по сравнению с другими мерами, с помощью которых можно обеспечить достижение желаемого результата. Государства пользуются некоторой свободой действий при выполнении своих обязательств, принятых в рамках международного законодательства в области прав человека (*свобода усмотрения*).

Более того, даже некоторые права могут препятствовать осуществлению права на свободу слова или свободу выражения мнений, такие как право на свободу от пыток и других видов жестокого, бесчеловечного или унижающего достоинство обращения, право на неприкосновенность частной жизни, право на свободу от дискриминации и право детей на особую защиту.

Вопросы для обсуждения:

1. Каким правам противоречит эта практика?
2. Является ли унижение мерой, соразмерной совершенному деянию?
3. Каковы последствия отсутствия национальных законов о киберпреступности?
4. Существуют ли еще какие-либо страны, где это могло бы произойти сегодня?

Тема 4. Введение в цифровую криминалистику.

1. Цифровые доказательства. Цифровая криминалистика основывается на принципе обмена Эдмона Локара, в соответствии с которым объекты и поверхности вступают в контакт друг с другом, происходит перекрестный перенос материалов (Maras and Miranda, 2014, pp. 2-3). В контексте цифровой криминалистики люди, после использования информационно-коммуникационных технологий (ИКТ), оставляют цифровые следы. В частности, лицо, использующее ИКТ, может оставить цифровые отпечатки, т.е. данные, оставленные пользователями ИКТ, которые могут раскрыть сведения о них, включая информацию о возрасте, половой, расовой и этнической принадлежности, гражданстве, сексуальной ориентации, мыслях, предпочтениях, привычках, хобби, истории болезни и проблемах

здоровья, психологических расстройствах, статусе занятости, принадлежности к какому-либо сообществу, отношениях, геолокации, распорядке дня и прочей активности. Такие цифровые отпечатки могут быть активными или пассивными. Активный цифровой отпечаток создается данными, предоставляемыми пользователем, такими как персональные данные, видео, изображения и комментарии, размещаемые в приложениях, на вебсайтах, электронных досках объявлений, в социальных сетях и других онлайн-форумах. Пассивный цифровой отпечаток – это данные, которые непреднамеренно оставляют люди, пользующиеся Интернетом и цифровыми технологиями, например, история просмотров в браузере. Данные, которые являются частью активных и пассивных цифровых отпечатков, могут использоваться в качестве доказательства совершения преступления, в том числе киберпреступления, т.е. в качестве цифровых доказательств. Такие данные могут также использоваться для доказательства или опровержения утверждения о факте; подтверждения или опровержения показаний потерпевшего, свидетеля и подозреваемого; и/или определения причастности или непричастности подозреваемого к совершению преступления. Данные хранятся в цифровых устройствах, например, компьютерах, смартфонах, планшетах, телефонах, принтерах, «умных» телевизорах (Smart TV) и любых других устройствах, которые имеют цифровую память), внешних запоминающих устройствах, например, внешних жестких дисках и USB-флеш-накопителях, сетевых компонентах и устройствах, например, маршрутизаторах, серверах и облачном хранилище данных где данные хранятся «в нескольких центрах данных в различных географических точках» (УНП ООН, 2013, стр. 26). Извлекаемые данные могут представлять собой данные, относящиеся к контенту т.е. слова в письменных сообщениях или произнесенные слова в аудиофайлах; например, видео, текст электронных писем, текстовые сообщения, мгновенные сообщения и содержание социальных сетей, и данные, не относящиеся к контенту, или мета-данные (т.е. данные о содержании; например, личность и местоположение пользователей и данные об операциях, такие как информация об отправителях и получателях телекоммуникационных и электронных сообщений). Данные, получаемые в режиме онлайн и/или извлекаемые из цифровых устройств, могут содержать большое количество информации о пользователях и событиях. Например, игровые приставки, которые работают как персональные компьютеры, хранят личную информацию о пользователях устройств (например, имена и адреса электронной почты), финансовую информацию (например, данные кредитной карты), информацию об истории посещений Интернета (например, о посещенных вебсайтах), изображения, видео и другие данные. Данные, извлеченные из игровых приставок, использовались при расследовании дел, связанных с сексуальной эксплуатацией детей и размещением в Интернете материалов со сценами сексуального насилия над детьми (Read et al., 2016; Conrad, Dorn, and Craiger, 2010). Еще одним цифровым устройством, которое накапливает значительный объем данных о его пользователях, является Amazon Echo (с голосовым помощником Alexa). Данные, накапливаемые этим

устройством, могут содержать ценные сведения о пользователях/владельцах, такие как информация об их интересах, предпочтениях, запросах, покупках и прочих видах активности, а также об их местонахождении (чтобы, например, определить, находятся ли они дома или вне дома, путем просмотра меток времени и аудиозаписи взаимодействий с речевым помощником Alexa). Данные, извлеченные из Amazon Echo, использовались в Соединенных Штатах Америки при расследовании дела об убийстве. Хотя обвинения против подозреваемого были в конечном итоге сняты, это дело наглядно продемонстрировало, что данные, собираемые с использованием новых цифровых технологий, неизбежно будут представлены в суде в качестве доказательства. Данные могут добываться и использоваться в целях получения оперативно-розыскных сведений (для получения дополнительной информации см. UNODC 2011 Criminal Intelligence Manual for Analysts (УНП ООН, 2011 год, «Оперативная информация о преступной деятельности: пособие для аналитиков») могут представляться в суде в качестве цифровых доказательств. В последнем случае цифровые доказательства могут служить прямыми доказательствами путем «установления факта» либо косвенными доказательствами путем «выведения заключения об истинности данного факта» (Maras, 2014, pp. 40-41). Рассмотрим следующий гипотетический случай: материал расистского содержания был опубликован от имени учетной записи в Twitter (Учетная запись А). Прямым доказательством является тот факт, что Учетная запись А была использована для публикации расистского материала. Косвенным доказательством является тот факт, что материал был размещен владельцем учетной записи. Для того чтобы доказать, что владелец учетной записи опубликовал этот материал, необходимо получить дополнительные подкрепляющие доказательства. Прежде чем цифровые доказательства могут быть представлены в суде в качестве прямых или косвенных доказательств, их необходимо аутентифицировать т.е. необходимо показать, что доказательства соответствуют предполагаемой цели. Для наглядной демонстрации практики аутентификации рассмотрим следующие общие категории цифровых доказательств: контент, генерируемый одним или несколькими лицами (например, текст, электронное письмо или мгновенное сообщение и документы текстового редактора, такого как Microsoft Word); контент, генерируемый компьютером или цифровым устройством без участия пользователя например, журналы регистрации данных, который считается одной из форм вещественного доказательства, например, в Соединенном Королевстве (см. дело Regina (O) v. Coventry Magistrates Court, 2004); и контент, генерируемый одновременно пользователем и устройством (например, динамические таблицы в таких программах, как Microsoft Excel, которые включают в себя данные, вводимые пользователем, и расчеты, осуществляемые программой). Контент, генерируемый пользователем, может считаться допустимым доказательством, если он является достоверным и правдоподобным (т.е. можно установить его принадлежность к какому-либо лицу). Контент, генерируемый устройством, может считаться допустимым доказательством, если можно доказать, что устройство функционировало

должным образом в момент генерирования данных, и если можно показать, что в момент генерирования данных действовали механизмы обеспечения защиты для предотвращения изменения данных. В случаях, когда контент генерируется одновременно устройством и пользователем, необходимо установить достоверность и правдоподобность каждого из них. По сравнению с традиционными доказательствами, например, бумажными документами, оружием, контролируемыми веществами и т.д., цифровые доказательства создают уникальные сложности при аутентификации из-за объема доступных данных, их скорости (т.е. скорости, с которой они создаются и передаются), неустойчивости (т.е. они могут быстро исчезнуть при перезаписи или удалении) и уязвимости (т.е. их легко можно обработать, изменить или повредить). В то время как одни страны внедрили нормы доказательственного права, включающие в себя требования в отношении аутентификации, которые конкретно относятся к цифровым доказательствам, другие страны для аутентификации традиционных доказательств и цифровых доказательств используют схожие требования. Во Франции, например, как бумажные, так и электронные документы должны аутентифицироваться путем проверки личности создателя документов и целостности документов. Проверка целостности документов означает не только проверку их точности, но и способности сохранять точность (т.е. непротиворечивость) с течением времени. Более того, для того чтобы унифицировать режимы обращения с нецифровыми и цифровыми доказательствами, Сингапур внес поправки в нормы доказательственного права, приняв Закон «О доказательствах» (с поправками) 2012 года, чтобы обеспечить одинаковую практику аутентификации для нецифровых и цифровых доказательств. В дополнение к определению подлинности цифровых доказательств, многие страны также проводят оценку того, является ли полученное доказательство наилучшим доказательством (т.е. подлинным доказательством или точной копией подлинного доказательства), и/или может ли оно быть допустимым в соответствии с исключениями из требований соблюдения запрета на показания с чужих слов (т.е. заявлений, сделанных вне суда). В качестве примера можно привести Танзанию (Закон «О доказательствах» 1967 года, Закон «О письменных законах» (с различными поправками) 2007 года и Закон «Об электронных операциях» 2015 года); Белиз (Закон «Об электронных доказательствах» 2011 года); Индонезию (Закон №11 от 2008 года «Об электронной информации и операциях» и Постановление Правительства № 82 от 2012 года); Малайзию (Закон «О доказательствах» 1950 года); Индию (Закон «Об информационных технологиях» 2000 года); Сингапур (Закон «О доказательствах» (с поправками) 2012 года) и другие страны. Кроме того, оценка подлинности цифровых доказательств также предполагает изучение процессов, методов и инструментов, использованных для сбора, получения, сохранения и анализа цифровых доказательств, чтобы убедиться в том, что данные не были изменены каким-либо образом.

2. Цифровая криминалистика. Процесс цифровой судебной экспертизы включает в себя: поиск, получение, сохранение и хранение

цифровых доказательств; описание, объяснение цифровых доказательств и установление их происхождения и значимости; анализ доказательств и их убедительности, достоверности и относимости к делу; и представление доказательств, имеющих отношение к делу (Maras, 2014). Были разработаны и приняты различные методологии цифровой криминалистики. В 2001 году «Digital Forensic Research Workshop», «некоммерческая добровольная организация, специализирующаяся на финансировании деятельности технических рабочих групп, проведении ежегодных конференций и решении комплекса задач с целью оказания помощи в определении направления исследований и разработок», разработала модель, основанную на протоколе Федерального бюро расследований Соединенных Штатов Америки для производства обыска на физическом месте преступления, который включает в себя семь этапов: идентификация, сохранение, сбор, исследование, анализ, представление доказательств и принятие решения.

В 2002 году была предложена еще одна модель цифровой криминалистики, которая была основана на модели «Digital Forensic Research Workshop» 2001 года и протоколе Федерального бюро расследований Соединенных Штатов Америки для производства обыска на месте преступления. Эта модель («Абстрактная модель цифровой криминалистики») состояла из девяти этапов:

1. Идентификация (т.е. «распознание инцидента по признакам и определение его типа»);
2. Подготовка (т.е. «подготовка средств, методов, ордеров на обыск и мониторинг процесса получения разрешений и поддержки руководства»);
3. Стратегия подхода (т.е. «разработка процедуры, которая будет использоваться с целью сбора максимального объема безупречных доказательств при минимизации воздействия на потерпевшего»);
4. Сохранение (т.е. «изолирование, защита и сохранение состояния вещественных и цифровых доказательств»);
5. Сбор (т.е. «составление протокола осмотра физического места преступления и дублирование цифровых доказательств с использованием стандартизированных и утвержденных процедур»);
6. Исследование (т.е. «углубленный систематический поиск доказательств, относящихся к предполагаемому преступлению»);
7. Анализ (т.е. «определение значимости, восстановление фрагментов данных и выведение заключения на основе обнаруженных доказательств»);
8. Представление (т.е. «краткое изложение и объяснение выводов»);
9. Возвращение доказательств (т.е. «возвращение физического и цифрового имущества законному владельцу»).

В 2006 году Национальный институт стандартов и технологий США в своем Руководстве по интеграции криминалистических методов в планы реагирования на инциденты предложил модель цифровой криминалистики, состоящую из четырех этапов: этап сбора доказательств, который включает в себя идентификацию доказательств на месте преступления, маркировку, документирование и, наконец, собирание доказательств; этап исследования,

на котором определяются соответствующие криминалистические средства и методы, которые будут использоваться для извлечения соответствующих цифровых доказательств и сохранения их целостности; этап анализа, на котором извлекаемые доказательства оцениваются для определения их практической пригодности и применимости к делу; и этап отчетности, который включает в себя описание действий, выполненных в процессе цифровой криминалистики, и представление результатов.

Еще одна модель расследования была предложена Национальным институтом правосудия (NIJ) Министерства юстиции США в 2001 году и пересмотрена в 2008 году. В частности, в пособии NIJ основное внимание уделено действиям на физическом месте преступления, таким как ограждение и оценка места преступления (например, для определения имеющих отношение к делу устройств с потенциальными цифровыми доказательствами), документирование места преступления, выемка соответствующих устройств, упаковка, транспортировка и, наконец, обеспечение сохранности этих устройств. Вышеупомянутые модели основаны на предположениях о том, что при расследовании каждого преступления и киберпреступления все этапы должны быть пройдены в полном объеме. Однако на практике это происходит не всегда. Поскольку объемы данных и количество цифровых устройств, накапливающих, хранящих и передающих данные, растут в геометрической прогрессии, что ведет к увеличению числа уголовных дел, связанных с цифровыми устройствами того или иного типа, все чаще признается практически нецелесообразным проводить доскональные проверки каждого цифрового устройства. Как отметили Кейси, Феррaро и Нгуен, «немногие лаборатории цифровой криминалистики все еще могут позволить себе создавать дубликат каждого носителя информации и проводить углубленную судебную экспертизу всех данных на этих носителях… Не имеет особого смысла ждать завершения анализа каждого отдельного носителя информации, если лишь некоторые из них позволят получить данные, имеющие доказательную ценность» (Casey, Ferraro, Nguyen, 2009, p. 1353). В этой связи были разработаны модели процессов цифровой криминалистики, учитывающие эту проблему. Например, модель процесса киберкриминалистической сортировки данных на местах (CFFTPM), основанная на проведении цифровой судебной экспертизы «на месте» с целью «обеспечения идентификации, анализа и интерпретации цифровых доказательств в короткие сроки без необходимости транспортировки систем(ы)/носителей информации в лабораторию для углубленного исследования или создания полного образа для судебно-экспертного анализа» (p.19). На основе этой модели Кейси, Феррaро и Нгуен (Casey, Ferraro, Nguyen) (2009) предложили «три уровня судебной экспертизы», которые можно использовать на местах или в лаборатории:

1. Судебно-экспертный осмотр на основе обследования/сортировки. Такой осмотр проводится с целью быстрого изучения потенциальных источников доказательств и определения приоритетных источников для дальнейшего исследования на основе значимости доказательств, которые они

могут содержать, и изменчивости этих доказательств (Casey, Ferraro, and Nguyen, 2009, p. 1353 and 1356).

2. Предварительная судебная экспертиза. Для ускорения процесса цифровой судебной экспертизы проводится предварительная судебная экспертиза источников, выбранных на этапе судебно-экспертного осмотра на основе обследования/сортировки, чтобы обнаружить информацию, которая может быть использована в расследовании для получения прямых, косвенных или других подкрепляющих доказательств предполагаемого преступления (Casey, Ferraro, and Nguyen, 2009, pp. 1353 and 1356-1359). Неспособность обнаружить артефакты для судебно-экспертного анализа (т.е. данных, которые могут иметь значение для цифровой судебной экспертизы) во время этого осмотра, что может произойти в результате упущения их из виду, не означает автоматически, что углубленная судебная экспертиза проводиться не будет (это зависит от конкретного дела и от политики и процедур лиц, проводящих экспертизу).

3. Углубленная судебная экспертиза. Исследуются все источники доказательств. Экспертиза такого типа зачастую проводится в случаях, «когда есть подозрение на уничтожение доказательств, когда возникают дополнительные вопросы, и когда дело близится к судебному разбирательству» (Casey, Ferraro, and Nguyen, 2009, p. 1359). В настоящее время продолжаются дебаты относительно жизнеспособности и актуальности каждой модели и ее компонентов. Реальность такова, что каждая страна следует своим собственным стандартам, протоколам и процедурам в области цифровой криминалистики. Однако различия в этих процессах служат препятствием для осуществления международного сотрудничества в проведении расследований правоохранительными органами.

3. Стандарты и передовые практические методы в области цифровой криминалистики. Международная организация по стандартизации (ИСО), международная неправительственная организация, и Международная электротехническая комиссия (МЭК), международная некоммерческая организация, разрабатывают и публикуют международные стандарты для унификации практики, используемой в разных странах. В 2012 году Международная организация по стандартизации (ИСО) и Международная электротехническая комиссия (МЭК) опубликовали международные стандарты, касающиеся обращения с цифровыми доказательствами.

Это руководство охватывает только начальный процесс обращения с цифровыми доказательствами. Предлагаются следующие четыре этапа обращения с цифровыми доказательствами: Идентификация. Этот этап включает в себя поиск и распознавание соответствующих доказательств, а также их документирование. На этом этапе приоритетные задачи сбора доказательств определяются на основе ценности и изменчивости доказательств.

Сбор. Этот этап предполагает сбор всех цифровых устройств, которые могут содержать данные, имеющие доказательную ценность. Эти устройства

затем транспортируются в лабораторию судебной экспертизы или другое учреждение для сбора и анализа цифровых доказательств. Этот процесс именуется сбором данных в статическом режиме. Однако бывают случаи, когда сбор данных в статическом режиме является практически неосуществимым. В таких ситуациях осуществляется сбор данных в реальном времени. Рассмотрим, к примеру, системы критически важных объектов инфраструктуры, например, системы управления производственными процессами. Эти системы не могут быть отключены от питания, поскольку они предоставляют критически важные услуги. Поэтому в этих случаях осуществляется сбор данных в реальном времени, когда изменчивые и неизменчивые данные извлекаются из систем, работающих в реальном времени. Однако такой сбор данных в реальном времени может мешать нормальному функционированию систем управления производственными процессами, например, замедлять их работу.

Получение. Цифровые доказательства необходимо получать без ущерба для целостности данных. Национальный совет начальников полиции Соединенного Королевства (NPCC), ранее известный как Ассоциация руководителей полицейских служб Соединенного Королевства, придает этому требованию большое значение и выделяет его в качестве важного принципа в практике цифровой криминалистики (принцип №1: «Никакие действия, предпринимаемые правоохранительными органами, лицами, работающими в этих органах, или их представителями, не должны приводить к изменению данных, которые впоследствии могут использоваться в суде») (UK Association of Chief Police Officers, 2012, p. 6). Такое получение данных без их изменения осуществляется путем создания копии содержимого цифрового устройства, процесс, известный как создание неискаженного образа с использованием устройства блокировщика записи, которое предназначено для предотвращения изменения данных в процессе копирования. Для того чтобы определить, является ли дубликат точной копией оригинала, значение хэш-функции рассчитывается с использованием математических вычислений; здесь для получения значения хэш-функции используется криптографическая хэш-функция. Если значения хэш-функции для оригинала и копии совпадают, то содержимое копии является точно таким же, что и в оригинале. Признавая возможность существования определенных «обстоятельств, при которых какое-либо лицо считает необходимым получить доступ к исходным данным т.е. осуществить сбор данных в реальном времени», Национальный совет начальников полиции Соединенного Королевства отмечает, что «лицо, получающее доступ к этим данным, должно быть компетентным для таких действий и быть в состоянии представить доказательства, объясняющие целесообразность своих действий и их последствия» (Принцип №2).

Сохранение. Целостность цифровых устройств и цифровых доказательств может быть обеспечена с использованием системы охраны доказательств, которая определяется как «процесс, при помощи которого следователи обеспечивают охрану места преступления (или происшествия) и сохранность доказательств на протяжении всего периода производства по

делу. В журнал регистрации записывают информацию о том, кто осуществлял сбор доказательств, где и каким образом они были собраны, какие лица получили эти доказательства, и когда они их получили» (Maras, 2014, p. 377). Тщательное документирование процесса цифровой судебной экспертизы на каждом этапе имеет важное значение для обеспечения допустимости доказательств в суде. Национальный институт стандартов и технологий США имеет доступную для поиска базу данных инструментов цифровой криминалистики, которая содержит информацию об инструментах с различными функциями (например, инструменты для проведения криминалистической экспертизы баз данных, облачных хранилищ, беспилотных летательных аппаратов, транспортных средств и т.п.). Национальные правоохранительные органы разных стран имеют разные предпочтения в отношении использования инструментов для цифровой криминалистической экспертизы. Используемые инструменты должны быть надежными с точки зрения криминалистики. При этом процесс сбора и последующего анализа цифровых данных с помощью этих инструментов должен быть в состоянии сохранить данные в том состоянии, в котором они были впервые обнаружены, и никоим образом не уменьшать доказательную ценность электронных данных из-за технических или процедурных ошибок либо ошибок в интерпретации. Проще говоря, полученные данные не должны быть каким-либо образом изменены, то есть их целостность должна быть сохранена. В 17 рамках Программы тестирования инструментов компьютерной криминалистики Национального института стандартов и технологий США была принята методология тестирования программных средств компьютерно-технической экспертизы на основе разработки общих спецификаций инструментов, процедур испытаний, критериев испытаний, наборов тестов и оборудования для тестирования. Тестирование дает возможность получить информацию, которая необходима разработчикам для совершенствования разрабатываемых инструментов, позволяет пользователям делать осознанный выбор в отношении приобретения и использования инструментов компьютерно-технической экспертизы и способствует пониманию возможностей инструментов всеми заинтересованными сторонами. Цифровая криминалистика включает в себя процессы идентификации, получения, сохранения, анализа и представления цифровых доказательств. Цифровые доказательства должны быть аутентифицированы, чтобы обеспечить их допустимость в суде. В конечном счете артефакты для судебно-экспертного анализа и используемые криминалистические методы, например, сбор данных в статическом режиме или в реальном времени зависят от устройства, его операционной системы и его средств защиты. Запатентованные операционные системы с которыми следователи могут быть незнакомы и средства защиты (например, шифрование служат препятствиями для проведения цифровой судебной экспертизы. Например, шифрование, которое блокирует доступ третьих лиц к информации о пользователях и их сообщениям, может помешать правоохранительным органам получить доступ к данным, содержащимся в цифровых устройствах, таких как смартфоны.

Вопросы для обсуждения:

1. Какие данные хранит это устройство?
2. К какому типу относятся эти данные?
3. Где расположены эти данные?
4. Как можно определить местоположение этих данных?

Тема 5. Расследование киберпреступлений.

1. Сообщения о киберпреступлениях.

Прежде чем начать расследование, необходимо зафиксировать факт совершения киберпреступления и сообщить о нем. Хотя это кажется простым первым шагом в расследовании киберпреступления, реальность такова, что значительная часть случаев киберпреступлений во всем мире не сообщается (УНП ООН, 2013).

Нежелание сообщать о преступлениях можно объяснить *теорией ожидаемой полезности,* выдвинутой экономистом Гэри Беккером (1968), которая гласит, что люди участвуют в каких-либо действиях, когда ожидаемая полезность (т.е. выгода) от этих действий превосходит ожидаемую полезность участия в других действиях (Maras, 2016, p. 25). В контексте киберпреступности, жертвы киберпреступлений не сообщают о киберпреступлении, если ожидаемая полезность такого сообщения является низкой (Maras, 2016, p. 25). Однако готовность лица или организации сообщить о киберпреступлении зависит и от типа киберпреступления. Проводимые в настоящее время исследования определяют несколько причин, в силу которых киберпреступления не сообщаются,, включая чувство стыда и смущения, испытываемые жертвами определенных видов киберпреступлений (например, романтической аферы); репутационные риски, связанные с преданием гласности факта совершения киберпреступления (например, если жертвой киберпреступления является коммерческое предприятие, или если есть угроза утраты доверия со стороны потребителей); отсутствие осознания того, лицо стало жертвой преступления; низкую степень уверенности или ожиданий в отношении способности правоохранительных органов оказать помощь; необходимость расходования слишком большого количества времени и усилий для сообщения о киберпреступлении; и отсутствие осведомленности о том, кому следует сообщать о киберпреступлениях (УНП ООН, 2013; McGuire and Dowling, 2013; Tcherni et al., 2016; Maras, 2016).

В качестве меры реагирования на заниженную частоту сообщений о киберпреступлениях правительственные и неправительственные организации реализовали инициативы, направленные на повышение количества сообщений путем оптимизации процедуры представления информации о киберпреступлениях, которая обычно предполагает участие нескольких учреждений в зависимости от типа совершенного киберпреступления (например, сообщения о финансовом мошенничестве в сети Интернет могут получать полиция, банки и прочие финансовые учреждения, а также

государственные органы, участвующие в расследовании финансовых киберпреступлений), и привлечения внимания к механизмам сообщения информации о киберпреступлениях, таким как веб-сайты или горячие линии. Например, в Новой Зеландии NetSafe – независимая некоммерческая организация, работающая в сфере обеспечения безопасности в Интернете, – разработала, в сотрудничестве с государственными органами, веб-сайт Orb для предоставления гражданам страны единого и безопасного места, где они могут оставить сообщение о киберпреступлении. В Южной Африке Южноафриканский портал ресурсов и информации о киберпреступлениях позволяет пользователям сообщать о киберпреступлениях на своем портале. Кроме того, в 2018 году в США Федеральное бюро расследований (ФБР) инициировало информационно-разъяснительную кампанию по киберпреступности с участием актрисы из американского телесериала «Мыслить как преступник», которая информировала общественность о возможности направления сообщений о киберпреступлениях в Центр приема жалоб на Интернет-преступления (IC3) (FBI, Reporting CyberCrime is as Easy as IC3).

Необходимо оценивать влияние таких инициатив на частоту сообщений о киберпреступлениях. В Австралии была создана *Австралийская сеть* Интернет-сообщений о *киберпреступности* (ACORN), чтобы упростить процедуру приема сообщений о киберпреступлениях. В 2016 году Австралийский институт криминологии опубликовал отчет об оценке ACORN, который показал, что эта инициатива оказала лишь незначительное влияние на частоту сообщений о киберпреступлениях и уровень осведомленности общественности о том, куда следует направлять такие сообщения (Morgan et al., 2016). Оценка таких инициатив имеет важное значение, поскольку она позволяет правительствам вкладывать средства в те проекты, которые приносят желаемые результаты и помогают вносить изменения и дополнения в программы и инициативы, которые не приносят ожидаемых результатов.

2. Кто проводит расследования по киберпреступлениям?

Лица, принимающие первые ответные меры при расследовании киберпреступлений, отвечают за «сохранность» цифровых доказательств на «месте» совершения киберпреступления (например, это может быть объект или объекты киберпреступления или устройства информационно-коммуникационных технологий, использованные для совершения преступления с использованием киберсетей или киберзависимого преступления). Таким лицом, принимающим первые меры реагирования, может быть сотрудник правоохранительных органов, эксперт по цифровой криминалистике, офицер военной полиции, частный следователь, специалист по информационным технологиям или другое лицо, например, работник по найму, которому поставлена задача реагировать на происшествия, связанные с киберпреступностью. Это говорит о том, что расследования киберпреступлений проводят государственный и частный секторы, а также органы национальной безопасности с той или иной степенью участия.

Независимо от того, кто принимает первые ответные меры, процедуры поиска и изъятия устройств информационно-коммуникационных технологий (ИКТ) должны соответствовать национальному законодательству, а методы, используемые для получения цифровых доказательств из устройств ИКТ, должны быть обоснованными и надежными, чтобы обеспечить допустимость доказательств в суде.

Органы уголовного правосудия.

Работники системы уголовного правосудия, такие как сотрудники правоохранительных органов, прокуроры и судьи, несут ответственность за профилактику, смягчение негативных последствий, выявление, расследование киберпреступлений, а также уголовное преследование и вынесение судебных решений по делам, связанным с киберпреступностью. Конкретные органы, ответственные за расследование киберпреступлений, различаются в зависимости от страны. Например, в Великобритании расследования киберпреступлений проводят несколько органов, в том числе региональные правоохранительные органы и Национальное подразделение по борьбе с киберпреступностью, которое входит в состав Национального агентства по борьбе с преступностью (Global Cyber Security Capacity Centre, 2016 c). В отличие от Великобритании, лишь одно учреждение занимается расследованием киберпреступлений в таких странах, как Сьерра-Леоне, где расследования проводит отдел полиции по предупреждению киберпреступности (Global Cyber Security Capacity Centre, 2016 d), Эквадор, где «Отдел по расследованию технологических преступлений Национальной дирекции судебной полиции и расследований несет ответственность за расследование киберпреступлений» (Inter-American Development Bank, 2016, p. 72), и Исландия, где такими расследованиями занимается подразделение цифровой судебной экспертизы полиции Рейкьявика (Global Cyber Security Capacity Centre, 2017 c).

Более того, в некоторых странах в расследовании одного и того же киберпреступления могут участвовать несколько учреждений. Участие того или иного учреждения зависит от типа расследуемого киберпреступления. Например, на Кипре преступления, связанные с финансовым мошенничеством в Интернете, расследуются Отделом криминальных расследований, а также Группой по расследованию финансовых преступлений Главного управления полиции Кипра (Global Cyber Security Capacity Centre, 2017 b). В связи с тем, что в разных странах ответственность за борьбу с киберпреступностью и проведение расследований дел о киберпреступлениях несут разные органы, во многих странах создаются официальные контактные пункты. Например, на Кипре круглосуточным контактным пунктом является Управление по борьбе с киберпреступностью (Global Cyber Security Capacity Centre, 2017 b).

Сотрудники органов уголовного правосудия должны обладать специальными знаниями (т.е. информацией, относящейся к предметной области, которая необходима для выполнения задачи), навыками (т.е. профессиональным опытом в предметной области) и способностями (т.е. умением применять знания и навыки для выполнения задачи) (все вместе они

именуются ЗНС (знания, навыки, способности); в дополнение к тем знаниям, навыкам и способностям, которые необходимы для расследования, уголовного преследования и/или разбирательства дел, связанных с преступлениями совершаемыми вне сети Интернет. Например, сотрудники правоохранительных органов должны быть в состоянии расследовать киберпреступления и/или иные преступления, которые так или иначе связаны с использованием устройств информационно-коммуникационных технологий (например, смартфонов, в которых хранятся доказательства преступления), и надлежащим образом обращаться с ИКТ в ходе расследования (например, выявлять, получать, сохранять и анализировать цифровые доказательства таким способом, чтобы обеспечить их допустимость в суде) (National Initiative for Cybersecurity Careers and Studies, n.d.). Возможности правоохранительных органов расследовать киберпреступления зависят от страны и варьируются в зависимости от конкретного учреждения внутри страны. Например, в Кыргызской Республике правоохранительные органы имеют ограниченные возможности для расследования киберпреступлений из-за отсутствия специализированных знаний, навыков, способностей, подготовки, а также нехватки кадровых и финансовых ресурсов (Global Cyber Security Capacity Centre, 2017a). На Мадагаскаре отчет за 2017 год показал, что, хотя в структуре правоохранительных органов «не было специализированного подразделения по борьбе с киберпреступностью, ... вопросами киберпреступности занимались некоторые специально назначенные для этой цели сотрудники Национальной полиции и жандармерии» (Global Cyber Security Capacity Centre, 2017 a, p. 33). Для сравнения, во Франции существует несколько подразделений, сотрудники которых имеют специальную подготовку для проведения расследований киберпреступлений (например, Les investigateurs en Cybercriminalité (следователи по делам о киберпреступности) (ICC) и N-TECH (следователи со специальной подготовкой в сфере новых технологий), которые входят в состав Национальной жандармерии)

Другие сотрудники системы уголовного правосудия, такие как прокуроры и судьи, также должны владеть специальными знаниями о киберпреступности и *цифровой криминалистике* (являющейся «одной из отраслей криминалистики, которая специализируется на уголовно-процессуальном праве и доказательствах применительно к компьютерам и связанным с ними устройствам». Как и в случае правоохранительных органов, уровень подготовки прокуроров и судей варьируется между странами и даже внутри стран. Например, в Великобритании Королевская прокурорская служба имеет все возможности для судебного преследования виновных в совершении киберпреступлений, в то время как, по состоянию на 2016 год, прокуроры на местном уровне не имели такой же подготовки и ресурсов для осуществления судебного преследования в связи с киберпреступлениями (Global Cyber Security Capacity Centre, 2016c). В 2017 году власти Сьерра-Леоне сообщили, что прокуроры и судьи не обладают необходимыми знаниями, навыками, способностями и ресурсами для судебного

преследования и разбирательства дел, связанных с киберпреступностью (Global Cyber Security Capacity Centre, 2016d). Схожая ситуация наблюдается в Исландии, где прокуроры и судьи проходят только специальную подготовку по вопросам киберпреступности на добровольной основе (Global Cyber Security Capacity Centre, 2017c). Сотрудники органов правосудия должны проходить подготовку для ознакомления с базовой информацией о киберпреступности и цифровой криминалистике, изучения вопросов, относящихся к показаниям экспертов по делам о киберпреступлениях и допустимости цифровых доказательств в суде. В 2017 году власти Сенегала сообщили, что судьи не проходят подготовку подобного типа (Global CyberSecurity Capacity Centre, 2016b).

Помимо национальных органов уголовного правосудия, региональные учреждения, такие как Агентство Европейского Союза по сотрудничеству правоохранительных органов (Europol) (для развития сотрудничества между правоохранительными органами в Европейском союзе) и Eurojust (для развития сотрудничества между судебными органами стран-членов Европейского союза), и международные агентства, такие как INTERPOL (Международная организация уголовной полиции, способствующая международному сотрудничеству между правоохранительными органами), оказывают содействие и/или способствуют проведению трансграничных расследований киберпреступлений. Например, в результате обмена оперативными данными и ресурсами между Европолом и государствами-членами Европейского союза был арестован преступник, известный тем, что продавал фальшивые банкноты номиналом 50 евро на незаконных рынках в темном Интернете (Europol, 2018c).

Органы национальной безопасности.

Органы национальной безопасности могут принимать участие в расследованиях киберпреступлений (например, в некоторых странах расследования киберпреступлений могут проводиться с участием военных органов, тогда как в других странах такие расследования могут проводиться разведывательными органами или национальными управлениями кибербезопасности). Однако участие органов национальной безопасности в расследованиях киберпреступлений зависит от расследуемого киберпреступления, объекта (объектов) киберпреступления и/или исполнителей киберпреступления. Например, военные органы могут расследовать киберпреступления, имеющие какую-либо связь с вооруженными силами, то есть киберпреступления, совершенные против военнослужащих, военного имущества и/или военной информации, и/или киберпреступления, совершенные военнослужащими. В качестве примера можно привести Соединенные Штаты, где сотрудники военной полиции расследуют случаи нарушения Единого кодекса военной юстиции. В дополнение к расследованию таких киберпреступлений (или, как минимум, к участию в расследовании киберпреступлений в том или ином качестве), военные органы и прочие органы национальной безопасности могут отвечать за выявление, смягчение негативных последствий, предотвращение

киберпреступлений, направленных на системы, сети и данные этих органов, системы, содержащие секретную информацию, а также за принятие ответных мер реагирования на такие киберпреступления. Органы национальной безопасности по всему миру развили и/или в настоящее время развивают свои *кибероборонительные* возможности (т.е. меры, которые предназначены для обнаружения и предотвращения киберпреступлений и смягчения последствий этих киберпреступлений в случае их совершения) и *кибернаступательные* возможности. Именно признание киберпространства в качестве еще одной сферы ведения боевых действий, привело к расширению деятельности органов национальной безопасности в киберпространстве (Smeets, 2018; Kallender and Hughes, 2017). Например, в Соединенных Штатах такое признание пятой сферы ведения боевых действий повлекло за собой создание Кибернетического командования США (USCYBERCOM). По примеру Соединенных Штатов другие страны, такие как Нидерланды, Германия, Испания, Республика Корея и Япония, также создали аналогичные кибернетические командования и/или кибернетические центры или подразделения.

Частный сектор.

Частный сектор играет важную роль в деле выявления, предотвращения, смягчения последствий и расследования киберпреступлений, поскольку в большинстве случаев именно частный сектор владеет *критически важной инфраструктурой* (т.е. инфраструктурой, считающейся необходимой для функционирования общества) и управляет ею и является одной из основных мишеней многих киберзависимых преступлений (т.е. киберпреступлений, цель которых заключается в нарушении конфиденциальности, целостности и доступности систем, сетей, сервисов и данных, таких как взлом, распространение вредоносных программ и распределенные атаки типа «отказ в обслуживании» или DDoS-атаки) и преступлений с использованием киберсетей (например, финансовое мошенничество в Интернете, преступления, связанные с использованием персональных данных, кража данных и коммерческой тайны и многие другие). Согласно Резолюции 2341 (2017) Совета Безопасности Организации Объединенных Наций, «каждое государство само определяет, какие объекты его инфраструктуры являются критически важными» на его территории. Поскольку такой статус инфраструктуры определяется самим государством, между странами существуют различия в отношении того, какие объекты инфраструктуры относятся к критически важным. Например, Австралия в качестве критически важной инфраструктуры определила объекты, относящиеся к восьми секторам (а именно: здравоохранение; энергетика; транспорт; водоснабжение; связь; производство продовольствия и розничная торговля продуктами питания; банковское дело и финансы; и правительство Австралийского союза) (Australian Government, Department of Home Affairs, n.d.), в то время как Соединенные Штаты определили 16 типов объектов критически важной инфраструктуры (химические объекты; торговые предприятия; объекты связи; критически важные промышленные объекты; плотины; производственная база

оборонной промышленности; аварийные службы; энергетика; финансовые услуги; продовольствие и сельское хозяйство; государственные учреждения; здравоохранение и санитарно-эпидемиологические службы; информационные технологии; ядерные реакторы, материалы и отходы; транспортные системы; и системы водоснабжения и удаления сточных вод) (US Department of Homeland Security, n.d.).

Поскольку в большинстве случаев критически важной инфраструктурой владеет частный сектор, который управляет ею и является одной из основных мишеней киберпреступников, он располагает всеми возможностями для принятия мер обеспечения безопасности, предназначенных для выявления киберпреступлений и киберпреступников в упреждающем порядке в целях предотвращения или, как минимум, смягчения последствий киберпреступлений, а также реагирования на киберпреступления, которые совершаются или были совершены. Термин «критически важная инфраструктура» используется не всеми странами для описания базовой инфраструктуры (Исполнительный директорат Контртеррористического комитета Совета Безопасности Организации Объединенных Наций и Контртеррористическое управление Организации Объединенных Наций, 2018 год). Например, вместо термина «критически важная инфраструктура» Новая Зеландия использует термин «жизненно важные коммуникации» для обозначения своих важных объектов жизнеобеспечения, которые включает в себя энергетику, связь, транспорт и водоснабжение (New Zealand Lifelines Council, 2017). Масштабы таких мер, принимаемых частным сектором, зависят от конкретной организации, ее сферы деятельности или организационно-правовой формы, ее людских, финансовых и технических ресурсов и возможностей.

Частный сектор также проводит частные расследования киберпреступлений. Частный сектор уязвим как к *внутренним угрозам* (например, к киберпреступлениям, совершаемым сотрудниками или руководителями коммерческого предприятия или организации), так и к *внешним угрозам* (например, к киберпреступлениям, совершаемым лицами, каким-либо образом связанными с коммерческим предприятием или организацией, например, поставщиками или заказчиками, или лицами, никак не связанными с предприятием или организацией) (Maras, 2014, p. 253). Когда совершается киберпреступление, предприятия и организации зачастую не обращаются в правоохранительные органы. Это, однако, зависит от вида киберпреступления, людских, технических и финансовых ресурсов частной организации, а также воздействия киберпреступления на организацию с точки зрения последствий сообщения о совершенном киберпреступлении для этой организации (например, потенциальный ущерб репутации и/или утрата доверия потребителей).

Государственно-частные партнерства и целевые группы.

Частный сектор обладает людскими, финансовыми и техническими ресурсами для проведения расследований киберпреступлений и может оказать помощь органам национальной безопасности, правоохранительным органам и

другим государственным учреждениям по делам, связанным с киберпреступностью. В этой связи на международном уровне было разработано множество проектов в рамках государственно-частного партнерства с целью усиления возможностей стран для расследования киберпреступлений. В качестве примера можно привести Центр обработки данных о киберпреступности (Cyber Fusion Centre) Интерпола, где работают как сотрудники правоохранительных органов, так и отраслевые эксперты по кибербезопасности, которые собирают ценную оперативную информацию и обмениваются ей с соответствующими заинтересованными сторонами (INTERPOL, n.d.). Trend Micro (компания-разработчик программ обеспечения кибербезопасности и киберзащиты), Лаборатория Касперского (разработчик программ кибербезопасности и защиты от компьютерных вирусов) и другие частные компании, которые занимаются вопросами, связанными с киберпреступностью или кибербезопасностью, и/или являются поставщиками Интернет-услуг и Интернет-контента или оказывают иные услуги, связанные с Интернетом, тесно сотрудничают с Интерполом (INTERPOL, n.d.). Организация Североатлантического договора (НАТО) также сотрудничает с союзниками в целом и с Европейским союзом и частной промышленностью в частности на основе Технического соглашения о киберзащите и Киберпартнерства НАТО с промышленностью.

Механизмы государственно-частного партнерства (ГЧП) также создаются на национальном уровне. В Соединенных Штатах Национальный альянс киберкриминалистики и киберподготовки (NCFTA) объединяет специалистов по киберпреступности из государственных органов, научных кругов и частного сектора с целью выявления и смягчения последствий киберпреступлений и борьбы с ними (NCFTA, n.d.). В Японии в рамках ГЧП была создана схожая с NCFTA структура – Центр по борьбе с киберпреступностью (JC3, 2014). В Европе проект 2 Centre (2 Центр) осуществляется на основе сотрудничества между правоохранительными органами, образовательными организациями и частным бизнесом. Реализация этого проекта в рамках ГЧП началась с создания национальных центров в Ирландии и Франции, и впоследствии национальные центры были созданы в других странах; по состоянию на 2017 год, такие центры функционируют в Греции, Испании, Бельгии, Эстонии, Литве, Болгарии и Англии.

3. Препятствия для расследования киберпреступлений.

При проведении расследований киберпреступлений могут возникать различные препятствия. Одним из таких препятствий является анонимность, которую обеспечивают пользователям средства информационно-коммуникационных технологий. *Анонимность* позволяет людям заниматься какой-либо деятельностью, не раскрывая информации о своей личности и/или своих действиях другим лицам. Существуют несколько методов анонимизации, которые используют киберпреступники. Одним из таких методов является использование прокси-серверов. *Прокси-сервер* – это промежуточный сервер, который используется для соединения клиента (т.е. компьютера) с сервером, с которого клиент запрашивает ресурсы (Maras,

2014, p. 294). *Анонимайзеры* или анонимные прокси-серверы скрывают идентифицирующие данные пользователей, маскируя их IP-адреса и заменяя их другими IP-адресами. Методы анонимизации используются как на законных, так и незаконных основаниях. Существуют законные основания для того, чтобы оставаться анонимным и сохранять защиту анонимности в сети. Например, анонимность способствует свободному потоку информации и сообщений без опасений последствий за высказывание нежелательных или непопулярных мыслей. Киберпреступники могут также использовать анонимные сети для шифрования (т.е. блокирования доступа) трафика и скрытия адреса Интернет-протокола (или *IP-адреса*), «уникального идентификатора, присваиваемого компьютеру или другому подключенному к Интернету цифровому устройству поставщиком услуг Интернета при подключении к сети» (Maras, 2014, p. 385), чтобы скрыть свою активность в Интернете и свое местонахождение. Хорошо изученными примерами анонимных сетей являются Tor, Freenet и Invisible Internet Project (проект «Невидимый Интернет», известный как I2P). Луковый маршрутизатор (или Tor), который обеспечивает анонимные доступ, коммуникацию и обмен информацией в Интернете, был первоначально разработан Военно-морской исследовательской лабораторией США для защиты разведывательных данных (Maras, 2014a; Maras, 2016). После того как Tor стал доступен для широкой публики, он стал использоваться отдельными лицами для защиты от частного и государственного надзора за их активностью в сети. Однако при этом Tor и другие анонимные сети также использовались киберпреступниками для совершения преступлений с использованием киберсетей и киберзависимых преступлений и/или для обмена информацией и/или инструментами с целью совершения таких преступлений (Europol, 2018). Эти анонимные сети не только «маскируют идентифицирующие данные пользователей, но и размещают их веб-сайты на своих ресурсах, используя возможности своих «скрытых сервисов», что означает, что эти сайты могут быть доступны лицам только» в этих анонимных сетях. Таким образом, эти анонимные сети используются для доступа к сайтам в Даркнет (или Темной паутине).

Всемирная паутина: основные сведения.

Для наглядного представления Всемирной паутины чаще всего используют образ айсберга в океане. Часть айсберга над поверхностью воды именуется видимым Интернетом (или видимой паутиной или видимой сетью). Эта часть паутины включает в себя индексированные сайты, которые доступны и готовы к использованию для широкой публики, и которые можно найти с использованием традиционных поисковых систем, таких как Google или Bing (Maras, 2014b). Глубокая сеть – это часть айсберга, которая находится ниже уровня поверхности воды. Она включает в себя сайты, которые не индексируются поисковыми системами и не являются легкодоступными и/или готовыми к использованию для широкой публики, например, сайты, защищенные паролем (Maras, 2016). К этим сайтам можно получить прямой доступ, если известен единый указатель ресурса (URL; т.е. адрес веб-сайта) и/или предоставлены учетные данные пользователей (т.е.

имена пользователей, пароли, парольные фразы и т.д.) для получения доступа к защищенным паролем веб-сайтам и онлайн-форумам. Для доступа к сайтам в темной паутине необходимо специализированное программное обеспечение, поскольку в ней используются инструменты, повышающие анонимность, чтобы препятствовать доступу и скрыть сайты.

Атрибуция является еще одним препятствием, затрудняющим расследования киберпреступлений. Атрибуция – это определение того, кто и/или что является ответственным за совершение киберпреступления. Цель атрибуции заключается в отнесении киберпреступления на счет конкретного цифрового устройства, пользователя устройства и/или других лиц, виновных в совершении киберпреступления (например, если киберпреступление финансируется или направляется государством). Использование инструментов, повышающих анонимность, может затруднить идентификацию устройств и/или лиц, ответственных за совершение киберпреступления. Процесс атрибуции еще более усложняется из-за использования зараженных вредоносными программами компьютеров-зомби (или *бот-сетей*) или цифровых устройств, управляемых при помощи *инструментов удаленного доступа* (т.е. вредоносной программой, которая используется для создания бэкдора на зараженном устройстве, позволяющего распространителю вредоносной программы получить доступ к системам и управлять ими). Эти устройства могут использоваться – без ведома пользователя, чье устройство заражено, – для совершения киберпреступлений. Обратное прослеживание (или *прослеживание в обратном направлении*) – это процесс прослеживания незаконных действий для установления источника (т.е. исполнителя и/или цифрового устройства) киберпреступления. Прослеживание в обратном направлении осуществляется после совершения киберпреступления или при его выявлении. Предварительное расследование проводится с целью обнаружения информации о киберпреступлении путем изучения файлов журналов (т.е. *журналов событий*, отображающих активность файловых систем), которые могут помочь обнаружить информацию о киберпреступлении (т.е. о том, *как* оно было совершено). Например, журналы событий «автоматически регистрируют события, происходящие в компьютере, чтобы получить контрольный след, который можно использовать для отслеживания, понимания и диагностики активности и проблем в системе» (Maras, 2014, p. 382). Примерами таких журналов являются *журналы приложений*, которые записывают «события, регистрируемые программами и приложениями», и *журналы безопасности*, которые «регистрируют все попытки входа в систему (как корректные, так и некорректные), а также создание, открытие или удаление файлов, программ или других объектов пользователем компьютера» (Maras, 2014, p. 207). Эти журналы событий могут помочь обнаружить IP-адрес, использованный при совершении киберпреступления.

Процесс прослеживания в обратном направлении может быть длительным. Время, необходимое для выполнения этой процедуры, зависит от знаний, навыков и способностей исполнителей преступления и мер, которые

они приняли для сокрытия своей личности и деятельности. В зависимости от тактических приемов, использованных киберпреступниками для совершения незаконных действий, отслеживание может не привести к единственному идентифицируемому источнику. Например, это может наблюдаться в тех случаях, когда для совершения киберпреступления используются зараженные вредоносной программой компьютеры-зомби, или, когда несколько злоумышленников одновременно проводят распределенную атаку типа «отказ в обслуживании». Следователи, расследующие киберпреступления, также сталкиваются с проблемами технического характера. Например, во многих цифровых устройствах используются патентованные операционные системы и программное обеспечение, которые требуют применения специализированных инструментов для идентификации, сбора и сохранения цифровых доказательств. Более того, следователи могут не иметь необходимого оборудования и инструментов цифровой криминалистики, необходимых для надлежащего проведения расследований киберпреступлений, предполагающих использование цифровых устройств.

К прочим препятствиям для расследования киберпреступлений можно отнести ограниченные возможности правоохранительных органов для проведения таких расследований. В странах, где существуют национальные специализированные подразделения, они расследуют лишь ограниченное число случаев киберпреступлений. Широкое применение информационно-коммуникационных технологий в расследованиях уголовных преступлений делает такую практику неэффективной (УНП ООН, 2013). Подготовка сотрудников национальных правоохранительных органов, занятых в неспециализированных областях полицейской деятельности и нетехнических специализированных подразделениях (например, по борьбе с преступлениями, связанными с наркотиками, организованной преступностью, преступлениями против детей), по вопросам киберпреступности, расследований, связанных с ИКТ, и цифровой криминалистики является одним из способов укрепления национального потенциала (УНП ООН, 2013). Кроме того, эти ограниченные возможности правоохранительных органов еще больше усугубляются коротким сроком актуальности профессиональных знаний следователей по делам о киберпреступлениях. Дело в том, что информационно-коммуникационные технологии непрерывно развиваются. Поэтому следователи, расследующие киберпреступления, должны учиться на протяжении всей жизни, постоянно идти в ногу с развитием технологий, не отставать от киберпреступников, знать их мотивы, цели, тактические приемы и способы совершения преступлений. Кроме того, правительственные и национальные службы безопасности сталкиваются с проблемой так называемой «утечки мозгов», когда высококвалифицированные и опытные следователи, специализирующиеся на киберпреступлениях, увольняются из этих органов и переходят в частный сектор, где им предлагают более высокое денежное вознаграждение за их знания, навыки и способности. Эти проблемы, связанные с потенциалом и кадровыми ресурсами, должны быть внимательно

изучены странами, поскольку они являются серьезным препятствием для расследований киберпреступлений.

4. Управление знаниями.

Концепция *управления знаниями* продвигается в качестве способа устранения препятствий, возникающих при расследовании киберпреступлений, которые связаны с кадровыми и техническими ресурсами, а также знаниями, навыками и способностями, необходимыми для проведения этих расследований. Цель управления знаниями заключается в «создании, сохранении и применении широкого спектра ресурсов знаний, таких как люди и информация», для улучшения процесса или конечного результата (Weiping and Chung, 2014, p. 8).

Процесс управления знаниями может применяться – и уже применялся – к расследованиям киберпреступлений (Weiping and Chung, 2014, p. 10-11). В контексте расследований киберпреступлений, процесс управления знаниями включает в себя выявление и оценку потребностей в знаниях для расследования киберпреступлений общего и специального характера. После выявления и оценки таких потребностей определяются и оцениваются знания соответствующего органа в области киберпреступности. При сравнении потребностей в знаниях с текущим уровнем знаний, которыми обладают следователи, определяются пробелы в знаниях. После выявления пробелов в знаниях предлагаются меры для их устранения. Практические методы управления знаниями могут использоваться для заполнения этих пробелов в знаниях.

Управление знаниями осуществляется с участием людей, которые получают, используют, создают знания, управляют и/или делятся ими, а также процессов и технологий, которые способствуют управлению знаниями. Обмен знаниями, являющийся неотъемлемой частью процесса управления знаниями в правоохранительной деятельности, происходит с участием как внешних сил, которые *продвигают* знания среди других людей (например, просветительские и информационные кампании), так и внутренних факторов, побуждающих других людей к получению знаний (факторы *притяжения*), например, к поиску экспертных знаний или содействия по тому или иному вопросу. Европол создал Dark Web Team (команду темной сети), которая служит примером такой формы обмена знаниями. В частности, Dark Web Team обменивается информацией, предоставляет оперативную поддержку и услуги специалистов в различных областях преступности (тем, кто их запрашивает) и… разрабатывает… инструменты, тактические приемы и методы проведения расследований в темной сети и выявления самых главных угроз и целей. Эта команда также преследует цель повышения эффективности совместных технических и следственных мероприятий, организации инициатив по обучению и наращиванию потенциала одновременно с проведением кампаний по профилактике и повышению осведомленности в рамках всесторонней стратегии борьбы с преступностью в темной сети (Europol, 2018b).

Процесс управления знаниями также ориентирован на обеспечение доступа к знаниям и источникам знаний (например, к людям) для тех, кто в них нуждается. Например, Федеральное бюро расследований США создало команду кибердействий (Cyber Action Team, CAT), состоящую из группы киберэкспертов, которая может быть оперативно развернута в любом месте в Соединенных Штатах в течение 48 часов для оказания поддержки в расследовании дел, связанных с киберпреступностью (FBI, n.d.).

Существуют два основных вида знаний, которыми можно управлять и обмениваться: явные знания и неявные знания (Dean, Filstad, and Gottschalk, 2006). *Явное знание* – это формальное знание, которое систематизируется, документируется и легко поддается определению (например, документы, судебные дела, законы и т.д.). *Системы управления контентом*, которые были созданы для хранения явных знаний, могут управлять знаниями о киберпреступлениях и расследованиях киберпреступлений, делая их доступными через веб-сайт и/или доступную для поиска базу данных. Примером может служить портал управления знаниями Управления ООН по наркотикам и преступности (UNODC) – Распространение электронных ресурсов и законов о борьбе с преступностью (SHERLOC). На этом портале размещены справочник по компетентным национальным органам (Справочник по КНО), которые уполномочены получать, рассматривать и отвечать на просьбы стран об оказании помощи по вопросам, касающимся взаимной правовой помощи (ВПП) и выдачи, а также база данных по прецедентному праву, база данных о законодательстве и библиографическая база данных (UNODC, n.d.). УНП ООН также имеет репозиторий данных о киберпреступности (Cybercrime Repository), который включает в себя базы данных по прецедентному праву, законодательству и выводам, сделанным по итогам расследований киберпреступлений (UNODC, n.d.). Также были созданы национальные системы управления контентом. Например, в Литве был создан портал электронных услуг литовских судов, чтобы обеспечить судебным органам доступ к базе данных судебных решений и гражданских дел (Global Cyber Security Capacity Centre, 2017d). В Украине Единый государственный реестр судебных решений предоставляет возможность доступа ко всем судебным решениям и постановлениям, принятым в стране с 2006 года, и представляет собой доступную для поиска базу данных с двумя типами доступа: общим (для всех) и полным (для судебных органов). Национальные и международные базы данных и репозитории позволяют отдельным лицам осуществлять поиск и получать явные знания, хранящиеся в этих базах данных, тем самым способствуя обмену такими явными знаниями.

В отличие от явного знания, *неявное знание* – это ноу-хау, которое нелегко поддается определению и основано на опыте. Обмен неявными знаниями подразумевает обмен этими знаниями через социализацию, зачастую в неструктурированной форме. Неявными знаниями можно поделиться через наставничество, преподавание и неформальное общение, а также во время программ обучения и семинаров. В некоторых случаях

международные организации делают упор на обмен неявными знаниями. Например, УНП ООН организовывает подготовку прокуроров, следователей и работников правоохранительных органов по вопросам сбора цифровых доказательств и проведения расследований киберпреступлений. Кроме того, Глобальный инновационный комплекс Интерпола (IGCI) оказывает поддержку в проведении транснациональных расследований киберпреступлений (например, обеспечивает координацию расследований киберпреступлений и операций по борьбе с киберпреступностью), содействует обмену оперативными данными между правоохранительными органами и делится передовым опытом в проведении расследований киберпреступлений (INTERPOL, n.d.). Так же, как и УНП ООН, Глобальный инновационный комплекс Интерпола организует курсы подготовки по вопросам расследования киберпреступлений и тенденций в области киберпреступности (например, проводит курсы повышения квалификации и разрабатывает учебные программы, такие как программы обучения навыкам расследования в темной сети) (INTERPOL, nd), а эксперты из Европола, Евроюста, Интерпола и других агентств делятся неявными знаниями об инструментах, тактических приемах и методах расследования, используемых, например, при проведении расследований в темной сети (Europol, 2018b). На национальном уровне обмен неявными знаниями пока не получил широкого распространения на практике.

Средства информационно-коммуникационных технологий (ИКТ), такие как программное обеспечение совместной работы для синхронного, т.е. в режиме реального времени и асинхронного взаимодействия, например, системы видеоконференцсвязи и совместного использования файлов и интерактивные рабочие пространства для совместной работы (например, документы Google, где участники коллективной работы могут обмениваться загруженными документами, редактировать и/или комментировать их), могут использоваться для объединения людей из разных мест и осуществления обмена неявными знаниями. Несмотря на предпринимавшиеся усилия по использованию ИКТ для содействия обмену неявными знаниями, эта практика не получила широкого распространения на международном и национальном уровнях. Например, в 2017 году Литва сообщила, что «не существует механизма, позволяющего осуществлять обмен информацией и передовой практикой между прокурорами и судьями для обеспечения действенного и эффективного судебного преследования по делам о киберпреступности» (Global Cyber Security Capacity Centre, 2017d, p. 47).

Вопросы для обсуждения:

1. Куда направляется сообщение о киберпреступлении?
2. Информировали ли вас о том, куда следует направлять сообщения о киберпреступлении? Если да, то когда и кто вас об этом проинформировал?
3. Проводятся ли какие-либо национальные разъяснительные и/или информационные кампании для поощрения сообщений о киберпреступлениях? Оценивались ли эти кампании?

4. Кто расследует киберпреступления в вашей стране?

5. Какова роль каждого ответственного и вовлечённого в проведение расследования киберпреступлений ведомства/субъекта?

6. Какие киберпреступления расследуют эти ведомства/субъекты?

7. Существуют ли механизмы государственно-частного партнерства для расследования киберпреступлений? Если да, то какие это механизмы?

8. Применяются ли какие-либо методы управления знаниями к расследованиям киберпреступлений? Если да, то какие?

Тема 6. Практические аспекты расследования киберпреступлений и цифровой криминалистики.

1. Правовые и этические обязательства.

Следователи, расследующие киберпреступления и специалисты по цифровой криминалистике должны учитывать правовые и этические аспекты при расследовании киберпреступлений, обработке, анализе и при толковании цифровых доказательств и представлении результатов. В то время как правовые обязательства предписываются национальными, региональными и международными нормами права этические обязательства во всех применимых случаях налагаются добровольно и/или устанавливаются государственными органами и/или частными профессиональными организациями. В случаях, когда существует *кодекс этики*, т.е. руководящие принципы, которые определяют правильное и неправильное поведение в процессе принятия решений, он зачастую включает в себя описание того, что следователи по делам о киберпреступлениях или специалисты по цифровой криминалистике *должны делать* во всех случаях, и что они *никогда не должны делать* ни при каких обстоятельствах. Например, Международное общество судебных экспертов по компьютерам (ISFCE) приняло кодекс этики, которому должны следовать его члены, чтобы обеспечить соблюдение стандартов, а также точность и достоверность результатов цифровой судебной экспертизы. Этот кодекс этики включает в себя описание видов поведения, которого должны придерживаться члены общества (например, соблюдение законных распоряжений и проведение всестороннего исследования доказательств в соответствии с действующими законами, стандартами, процедурами и руководящими принципами), и запрещенных видов поведения (например, сокрытие доказательств, предвзятость при анализе или представлении доказательств и представление заведомо ложных сведений о своей квалификации).

2. Обращение с цифровыми доказательствами. Цифровые доказательства являются неустойчивыми и недолговечными, и ненадлежащее обращение с такими доказательствами может привести к их изменению. В связи с неустойчивостью и недолговечностью доказательств необходимо соблюдать протоколы, чтобы не допустить изменения данных в процессе обращения с ними (то есть во время получения доступа к данным, их сбора, упаковки, передачи и хранения). В этих протоколах описываются действия,

которые необходимо выполнять при обращении с цифровыми доказательствами. Начальный процесс обращения с цифровыми доказательствами состоит из четырех этапов: идентификация, сбор, получение и сохранение.

Существуют протоколы для сбора *неустойчивых доказательств*. Сбор неустойчивых доказательств должен осуществляться в порядке возрастания степени устойчивости, то есть в первую очередь следует собирать доказательства с наименьшей степенью устойчивости, а доказательства с наибольшей степенью устойчивости следует собирать в последнюю очередь. В документе под названием «Запрос комментариев (RFC) 3227» (Request for Comments (RFC) 3227) приведен следующий пример порядка сбора неустойчивых данных (от наименее устойчивых к наиболее устойчивым) для стандартных систем (Brezinski and Killalea, 2002) реестры, кэш таблица маршрутизации, кэш (протокола определения адреса или ARP), таблица процессов, ядро (статистика), память системы для временных файлов диск данные удаленного журнала и данные мониторинга, имеющие отношение к исследуемой системе физическая конфигурация, топология сети архивный носитель данных.

Идентификация. На этапе идентификации до начала сбора цифровых доказательств необходимо получить предварительную информацию о совершенном киберпреступлении. Эта предварительная информация схожа с той, которая собирается во время традиционного уголовного расследования. Следователь пытается ответить на вопросы: кто причастен к киберпреступлению, что произошло, когда было совершено киберпреступление, где было совершено киберпреступление, как было совершено киберпреступление. Ответы на эти вопросы подскажут следователям, с чего следует начать расследование дела. Например, ответ на вопрос: «Где было совершено киберпреступление?» - т.е. было ли оно совершено на территории страны или за ее пределами. На этапе идентификации следователи по делам о киберпреступлениях используют большое количество традиционных методов расследования, особенно на этапе сбора информации и доказательств. Например, с целью сбора информации и доказательств расследуемого киберпреступления проводится допрос жертв, свидетелей и подозреваемых. Правоохранительные органы также проводят негласные расследования с целью установления личности, розыска и уголовного преследования киберпреступников. Кроме того, следователи, расследующие киберпреступление, проводят скрытое наблюдение. Такое наблюдение является «в высокой степени интрузивным методом сбора доказательств. Использование скрытого (негласного) наблюдения требует тщательного баланса между правом подозреваемого на частную жизнь и необходимостью расследовать тяжкие преступления. Положения о скрытом наблюдении должны полностью учитывать права подозреваемого. Международные органы и суды по правам человека приняли ряд решений о недопустимости негласного наблюдения и его параметрах, которые должны выполняться». Правоохранительные органы даже используют вредоносные

программы для осуществления наблюдения с целью сбора информации о киберпреступлении и доказательств его совершения. Например, правоохранительные органы США используют методику проведения следственных действий в компьютерных сетях (NIT) - «специально разработанные эксплойты или вредоносные программы» - в своих расследованиях дел, связанных с сексуальной эксплуатацией детей и сексуальным насилием над детьми в сети Интернет. Прежде чем начать сбор цифровых доказательств, следователь должен определить типы искомых доказательств. Цифровые доказательства можно обнаружить в цифровых устройствах, таких как компьютеры, внешние жесткие диски, *флеш-накопители*, маршрутизаторы, смартфоны, планшеты, камеры, «умные» телевизоры, бытовые приборы с выходом в Интернет (например, холодильники и стиральные машины), игровые приставки (и многие другие), а также на общедоступных ресурсах (например, платформы социальных сетей, веб-сайты и дискуссионные форумы) и частных ресурсах (например, журналы интернет-провайдеров об активности пользователей; деловые документы провайдеров коммуникационных услуг; журналы провайдеров облачного хранения с регистрацией активности пользователей и пользовательских материалов). Многие приложения, веб-сайты и цифровые устройства используют сервисы облачного хранения. Таким образом, данные о пользователях могут храниться целиком или в виде фрагментов различными провайдерами на серверах в нескольких местах (УНП ООН, 2013). Поэтому задача получения данных от этих провайдеров является трудновыполнимой. Тип искомых доказательств зависит от расследуемого киберпреступления. Если расследуемое киберпреступление представляет собой мошенничество с использованием персональных данных, то на изымаемых цифровых устройствах будет проводиться поиск доказательств этого преступления (например, доказательств мошеннических транзакций).

Сбор. При расследовании киберпреступления место преступления не ограничивается физическим местоположением цифровых устройств, которые использовались для совершения киберпреступления и/или были целью киберпреступников. Место совершения киберпреступления также включает в себя цифровые устройства, которые могут содержать цифровые доказательства, и охватывает несколько цифровых устройств, систем и серверов. В случаях, когда наблюдается факт совершения киберпреступления, поступает сообщение о киберпреступлении и/или имеется подозрение в совершении киберпреступления, принимаются меры по охране места преступления. Лицо, принимающее первые ответные меры определяет место преступления, защищает его от загрязнения и обеспечивает сохранность неустойчивых доказательств, изолировав пользователей от всех цифровых устройств, обнаруженных на месте преступления, например, переместив их в отдельное помещение или место. Пользователи должны быть лишены возможности дальнейшей эксплуатации цифровых устройств. При этом ни лицо, принимающее первые ответные меры, ни следователь не должны обращаться за помощью к какому-либо пользователю в процессе обыска и

документирования. Следователь, если он не является лицом, принимающим первые ответные меры, обыскивает место преступления и идентифицирует доказательства. До начала сбора доказательств место преступления документируется. *Документирование* является необходимым на протяжении всего процесса расследования (до, во время и после получения доказательств). Документация должна включать в себя подробную информацию о собранных цифровых устройствах, в том числе о рабочем состоянии устройства, было ли оно включено, выключено или находилось в режиме ожидания, - и его физических характеристиках, таких как марка, модель, серийный номер, соединения, любые отличительные знаки или какие-либо повреждения. В дополнение к письменным заметкам, для документирования места преступления и доказательств необходимы также схемы, фотографии и/или видеозаписи места преступления и доказательств. Сбор неустойчивых данных может изменить содержимое памяти цифровых устройств и данные внутри них. Следователь или эксперт-криминалист собирает доказательства. Процедуры варьируются в зависимости от типа цифрового устройства, а также общедоступных и частных ресурсов, где находятся цифровые доказательства (например, компьютеры, телефоны, социальные сети и облачное хранилище; для ознакомления с различными практическими методами цифровой судебной экспертизы мультимедийных, видео- и мобильных устройств см. веб-сайт Научной рабочей группы по цифровым доказательствам (Scientific Working Group on Digital Evidence (SWGDE). Правоохранительные органы используют *стандартные оперативные процедуры*, в которых подробно описываются действия, которые необходимо выполнить при обращении с цифровыми доказательствами на мобильных устройствах, объектах с выходом в Интернет (например, часы, фитнес-мониторы и бытовые приборы), облачном хранилище и платформах социальных сетей. Стандартная оперативная процедура (СОП) предназначена для оказания помощи следователям, поскольку в ней описываются методы и последовательность действий, которые следует соблюдать при расследовании киберпреступления таким образом, чтобы обеспечить допустимость собранных доказательств в суде; в ней также описываются инструменты и другие ресурсы, необходимые для проведения расследования. Таким образом, СОП включает в себя описание процедур, которые необходимо соблюдать во время проведения расследования.

Необходимо определить уникальные ограничения, с которыми могут столкнуться следователи в ходе расследования. Например, при расследовании киберпреступления следователи могут иметь дело с множеством цифровых устройств, операционных систем и сложных сетевых конфигураций, что потребует наличия специальных знаний, изменения в процедурах сбора доказательств и содействия в выявлении соединений между системами и устройствами (например, топологии сетей). Во время расследования следователь может также сталкиваться с методами *антикриминалистики*, такими как *стеганография* (т.е. сокрытие секретных данных, когда содержимое сообщения скрывается и делается невидимым)

и *шифрование* (т.е. «физическое блокирование доступа третьих сторон к файлу путем использования пароля либо путем приведения файла или элементов файла в непригодное для использования состояние». Поэтому следователь должен быть готов к таким ситуациям и располагать необходимыми людскими и техническими ресурсами, необходимыми для устранения этих ограничений. Действия, предпринимаемые следователем в таких случаях, например, способность следователя получить пароли к этим устройствам и/или расшифровать файлы, если они вообще предпринимаются, зависят от национальных законов. Инструменты цифровой криминалистики могут оказаться полезными в таких ситуациях и помочь, например, обнаружить стеганографию и расшифровать файлы, а также выполнить другие важные задачи цифровой судебной экспертизы. Примеры таких инструментов включают в себя программные обеспечения для проведения компьютерных экспертиз, такие как Forensic Toolkit (FTK) производства компании AccessData, Volatile Framework, X-Ways Forensics. Наряду с этими ресурсами необходим комплект криминалистических инструментов, который включает в себя предметы, используемые для документирования места преступления, инструменты, необходимые для разборки устройств и удаления прочих видов доказательств с места преступления, а также материалы, необходимые для маркировки и упаковки доказательств (например, для транспортировки смартфонов используются экранирующая сумка Фарадея, которая блокирует прием и передачу беспроводных сигналов цифровым устройством, и зарядное устройство питания), и другие инструменты. Процесс сбора доказательств предполагает сохранение неустойчивых доказательств и отключение питания цифровых устройств. Рабочее состояние обнаруженных цифровых устройств определяет процедуры сбора доказательств. Например, если обнаружен компьютер во включенном состоянии, неустойчивые доказательства (например, временные файлы, регистр, кэш, состояние сети, соединения и т.п.) сохраняются до отключения питания и изъятия компьютера. Если устройство выключено, то оно остается в выключенном состоянии и изымается. Существуют обстоятельства, при которых цифровые устройства не могут быть изъяты (например, из-за размера и/или сложности систем и/или конфигураций их аппаратного и программного обеспечения, поскольку эти системы обеспечивают критически важные услуги). В таких ситуациях неустойчивые и устойчивые данные собираются с использованием специальных процедур, которые требуют *сбора данных в реальном времени.* Для получения неустойчивых данных из систем, находящихся в рабочем состоянии, могут использоваться специальные команды. Например, для операционных систем Windows команда *ipconfig* используется для получения информации о сети, тогда как для операционных систем Unix используется команда *ifconfig*. И для Windows, и для Unix команда *netstat* используется для получения информации об активных сетевых соединениях. Помимо цифровых устройств также необходимо собрать другие предметы, имеющие отношение к делу (например, заметки и/или записные книжки, которые могут содержать пароли или иную информацию о сетевых учетных данных, телефонах, факсимильных

аппаратах, принтерах, маршрутизаторах и т.д.). Действия, предпринимаемые следователем при сборе доказательств, должны документироваться. Каждое устройство должно быть промаркировано (вместе с соединительными кабелями и сетевыми шнурами), упаковано и отправлено в лабораторию цифровой судебной экспертизы. После транспортировки предметов в лабораторию, они «инвентаризируются, регистрируются и передаются на хранение в запираемое помещение, защищенное от экстремальных температур, влажности, пыли и прочих возможных загрязнителей».

Получение. Существуют различные методы получения доказательств. Используемый метод зависит от типа цифрового устройства. Например, процедура получения доказательств с жесткого диска компьютера отличается от процедуры, необходимой для получения цифровых доказательств с мобильных устройств, таких как смартфоны.

Кроме случаев, когда осуществляется сбор данных в реальном времени, доказательства извлекаются из изъятых цифровых устройств в лаборатории судебной экспертизы (т.е. осуществляется *сбор данных в статическом режиме*). В лаборатории судебной экспертизы цифровые доказательства должны быть получены таким образом, чтобы сохранить *целостность* доказательств (обеспечить, чтобы данные остались без изменений), то есть *надежным с точки зрения криминалистики* способом. Для этого инструменты и методы, используемые для получения цифровых доказательств, должны предотвращать изменения данных или, когда это невозможно, по крайней мере минимизировать изменения. Используемые инструменты и методы должны быть обоснованными и надежными. Прежде чем использовать эти инструменты и методы, необходимо определить и учесть пределы их возможностей. Национальный институт стандартов и технологий США имеет доступную для поиска базу данных инструментов цифровой криминалистики (digital forensics tools database), в которой описываются инструменты с различными функциональными возможностями (например, инструменты для судебной экспертизы облачных хранилищ и т.п.)

Изъятые цифровые устройства считаются основным источником доказательств. Эксперт по цифровой криминалистике получает данные не из первичного источника. Вместо этого создается дубликат содержимого этого устройства, и эксперт работает с копией. Дубликат содержимого цифрового устройства создается (такой процесс именуется *созданием неискаженного образа*) до начала сбора данных в статическом режиме для сохранения целостности цифровых доказательств. Для того чтобы определить, является ли дубликат точной копией оригинала, значение криптографической хэш-функции рассчитывается с использованием математических вычислений; если значения хэш-функции для оригинала и копии совпадают, то содержимое копии является зеркальным отображением (т.е. дубликатом) содержимого оригинала. *Блокировщик записи*, который предназначен для предотвращения изменения данных в процессе копирования, следует использовать до извлечения данных во всех случаях, когда это возможно, для того чтобы не допустить изменений данных во время копирования. Важно отметить, что

описанный выше процесс получения данных применим в основном к компьютерам. При получении данных с мобильных телефонов и схожих с ними устройств, где память не может быть физически отделена от устройства для создания неискаженного образа, применяется иная процедура. Существуют два способа извлечения данных: физическое и логическое. *Физическое извлечение* предполагает поиск и получение доказательств из такого места в цифровом устройстве, где хранятся доказательства, например, из жесткого диска компьютера (Maras, 2014). Физическое извлечение может осуществляться путем использования *поиска по ключевым словам* (на основе терминов, предоставленных следователем), метода *вычленения однородных массивов данных* (т.е. поиска «на основе верхних и нижних колонтитулов и других идентификаторов») и путем изучения нераспределенного пространства (т.е. «пространства в системе, являющегося свободным, потому что оно никогда не использовалась, или потому что информация из него была удалена»; Maras, 2014, p. 36) и разделов, которые отделяют сегменты жесткого диска друг от друга (Maras, 2014). *Логическое извлечение* предполагает поиск и получение доказательств из места, в котором они «находятся относительно файловой системы компьютерной операционной системы, используемой для отслеживания имен и местоположений файлов, которые хранятся на носителе данных, таком как жесткий диск» (Maras, 2014, p. 36). Способ логического извлечения зависит от цифрового устройства, файловой системы, приложений на устройстве и операционной системы. *Логическое извлечение* предполагает получение данных из активных и удаленных файлов, файловых систем, нераспределенного и неиспользуемого пространства, а также сжатых, зашифрованных и защищенных паролем данных. Весь процесс получения доказательств должен документироваться. При этом документация должна включать в себя подробную информацию о цифровых устройствах, из которых были извлечены доказательства, аппаратном и программном обеспечении, использованном для получения доказательств, способе, при помощи которого были получены доказательства (т.е. о том, как они были получены), а также о том, когда, где и почему они были получены, какие доказательства были получены и по какой причине они были получены.

Сохранение. Цель сохранения доказательств заключается в защите цифровых доказательств от изменений. Целостность цифровых доказательств должна сохраняться на каждом этапе обращения с цифровыми доказательствами (ИСО/МЭК 27037). Лица, принимающие первые ответные меры, следователи, эксперты-техники, изучающие место преступления, и/или эксперты по цифровой криминалистике должны по возможности продемонстрировать, что цифровые доказательства не были изменены на этапе идентификации, сбора и получения; разумеется, что способность продемонстрировать это зависит от цифрового устройства (например, компьютера и мобильных телефонов) и обстоятельств, с которыми они сталкиваются (например, необходимость быстрого сохранения данных). Для этого необходимо поддерживать *систему охраны доказательств*. *Система*

охраны доказательств - это «процесс, при помощи которого следователи обеспечивают сохранность места преступления (или происшествия) и доказательств на протяжении всего периода производства по делу. В журнал регистрации вносится информация о том, кто осуществлял сбор доказательств, где и каким образом они были собраны, какие лица получили эти доказательства, и когда они их получили». В документах, которые ведутся в системе охраны доказательств, необходимо указывать имена, должности и контактную информацию лиц, которые идентифицировали, собрали и получили доказательства, а также любых других лиц, кому были переданы доказательства, подробную информацию о доказательствах, которые были переданы этим лицам, о времени и дате передачи, а также о цели передачи.

Анализ и отчётность. В дополнение к этапу обращения с цифровыми доказательствами, процесс цифровой судебной экспертизы также предполагает изучение и толкование цифровых доказательств (этап *анализа*) и представление результатов анализа (этап *отчетности*). На этапе *анализа* цифровые доказательства извлекаются из устройства, данные анализируются, а события реконструируются. До начала анализа цифровых доказательств эксперт по цифровой криминалистике в лаборатории должен быть проинформирован о целях поиска и получить некоторые сведения справочного характера о расследуемом деле и любую другую информацию, полученную в ходе расследования, которая может помочь эксперту-криминалисту на этом этапе (например, IP-адрес или MAC-адреса). Применяются различные виды анализа в зависимости от типа искомого цифрового доказательства, например, анализ сети, файловой системы, приложения, видеоматериалов, изображений и носителя (т.е. анализ данных в запоминающем устройстве). Файлы анализируются для установления их происхождения, а также определения того, когда и где эти данные были созданы, изменены, когда и откуда происходило обращение к ним, когда и где они были загружены или выгружены, и для определения возможного подключения этих файлов, находящихся в запоминающих устройствах, например, к удаленному хранилищу, такому как облачное хранилище. Тип искомых цифровых доказательств (например, электронные письма, текстовые сообщения, геолокация, документы текстового редактора, изображения, видео и журналы чата) зависит от конкретного вида киберпреступления.

Существуют четыре основных типа анализа, которые могут быть выполнены на компьютерах: анализ временных рамок; анализ собственности и владения; анализ приложений и файлов; и анализ метода сокрытия данных. Цель *анализа временных рамок* заключается в создании временной шкалы или временной последовательности действий с использованием меток времени (даты и времени), которые привели к событию, или в установлении времени и даты, когда пользователь совершил определенное действие (US National Institute of Justice, 2004b). Такой анализ проводится с целью отнесения преступления на счет его исполнителя или, как минимум, отнесения деяния, которое привело к преступлению, на счет конкретного лица (US National Institute of Justice, 2004b); однако существуют определенные трудности,

связанные с проверкой результатов анализа временных рамок. *Анализ собственности и владения* используется для установления лица, которое создало файлы в компьютерной системе, получило к ним доступ и/или изменило их (US National Institute of Justice, 2004b). Например, такой анализ может помочь обнаружить материалы со сценами сексуального насилия над детьми на устройстве подозреваемого. Одной этой информации недостаточно, чтобы доказать, кто является собственником материалов со сценами сексуального насилия над детьми. Для этого необходимы дополнительные доказательства, такие как факт исключительного пользования компьютером, на котором были обнаружены материалы. *Анализ приложений и файлов* выполняется для исследования приложений и файлов в компьютерной системе, чтобы установить заведомость, умысел и возможности преступника в отношении совершения киберпреступления (например, ярлык или имя файла могут указывать на содержимое файла; в частности, имя файла может оказаться именем жертвы киберпреступления). Можно также использовать *анализ метода сокрытия данных*. Как следует из названия, анализ метода сокрытия данных предполагает поиск скрытых данных в системе. Преступники используют несколько методов сокрытия данных, чтобы скрыть свою противоправную активность и идентифицирующую информацию, например, путем использования метода шифрования. Целью этих типов анализа является *реконструкция преступления* (или реконструкция событий). *Реконструкция событий* проводится для того, чтобы установить, *кто* несет ответственность за событие, *что* произошло, *где* произошло это событие, *когда* оно произошло, и *как* оно развивалось, путем идентификации, сопоставления и увязывания данных для раскрытия «общей картины» или сути события. Процесс реконструкции событий может включать в себя *временной анализ* (т.е. установление времени и последовательности событий), *реляционный анализ* (т.е. определение участников событий, их действий, а также связей и отношений между ними) и *функциональный анализ* (т.е. оценка производительности и возможностей систем и устройств, задействованных во время событий). Следователи должны участвовать в предварительных мероприятиях по реконструкции событий на этапах идентификации и сбора доказательств. Выполнение этих задач может помочь следователям выявить новые потенциальные источники цифровых доказательств. В конечном счете, для реконструкции событий на этапе анализа используются неполные знания для выведения заключений в отношении расследуемого дела на основе имеющихся доказательств и результатов анализа этих доказательств. Поэтому важно, чтобы следователи, расследующие киберпреступление, и эксперты по цифровой криминалистике признавали такие ограничения и избегали предвзятых толкований результатов анализа, например, толкований, являющихся следствием *предвзятости подтверждения*, когда люди ищут и поддерживают результаты, которые подтверждают их рабочую гипотезу, и отклоняют результаты, которые противоречат их рабочей гипотезе. Результаты анализа документируются в отчете. Отчеты должны

быть максимально четкими и точными. Они должны включать в себя иллюстративные материалы (например, рисунки, графики, выходные данные инструментов) и вспомогательные документы, такие как документация системы охраны доказательств, а также подробное разъяснение использованных методов и действий, предпринятых для исследования и извлечения данных (US National Institute of Justice, 2004b). Результаты должны разъясняться с учетом целей анализа (т.е. цели расследования и расследуемого дела). Информация об ограниченности полученных результатов также должна быть включена в отчет. Содержание отчета варьируется в зависимости от юрисдикции и национальной политики (если таковая имеется) в отношении расследований и цифровой криминалистики. Во избежание неверного толкования или определения неправильного весового значения цифровых доказательств, в отчете должно быть сказано об известных ошибках и неопределенности результатов.

3. Допустимость цифровых доказательств. Для обеспечения допустимости цифровых доказательств в суде должны быть соблюдены определенные правовые и технические требования. Что касается правовых требований, то суд рассматривает такие вопросы, как наличие законного разрешения на производство обыска и изъятия устройств информационно-коммуникационных технологий и связанных с ними данных, а также относимость к делу, подлинность, целостность и достоверность цифровых доказательств. При рассмотрении вопроса о соответствии техническим требованиям суд критически оценивает процедуры и инструменты цифровой криминалистики, использованные для извлечения, сохранения и анализа цифровых доказательств; лаборатории цифровой судебной экспертизы, в которых проводятся анализы; отчеты экспертов по цифровой криминалистике; и академические и профессионально-технические квалификации экспертов по цифровой криминалистике и свидетелей-экспертов (если это необходимо).

В 2017 году Антви-Боасиако (Antwi-Boasiako) и Вентер (Venter) разработали структуру под названием *Унифицированная модель оценки допустимости цифровых доказательств (Harmonized Model for Digital Evidence Admissibility Assessment (HMDEAA),* которая включает в себя основные технические и юридические требования, определяющие допустимость доказательств. В частности, модель HM-DEAA предусматривает три этапа для оценки допустимости доказательств, включая этапы оценки, рассмотрения и принятия решения в отношении допустимости цифровых доказательств.

Оценка цифровых доказательств. На этом этапе суды определяют, были ли использованы надлежащие законные разрешения на производство обыска и изъятие устройств информационно-коммуникационных технологий (ИКТ) и связанных с ними данных. К законным разрешениям относятся ордер на обыск, распоряжение суда или повестка в суд. Тип юридического документа, необходимый для изъятия устройств ИКТ и связанных с ними данных, варьируется в зависимости от юрисдикции и определяется национальным законодательством. На этом этапе также оценивается значимость цифровых

доказательств с точки зрения криминалистики. *Значимость с точки зрения криминалистики* определяется тем, могут ли цифровые доказательства: установить или исключить связь между преступником и мишенью (например, жертвой, цифровым устройством, веб-сайтом и т.д.) и/или местом преступления (местом, где было совершено преступление или киберпреступление); подтвердить или опровергнуть показания преступника, потерпевшего и/или свидетеля; установить личность исполнителя (исполнителей) киберпреступления; позволить выдвинуть следственные версии; обеспечить получение информации о способе действий (способе совершения преступления (*modus operandi* или М.О.), использованном преступником (т.е. о привычках, методах и особенностях поведения преступника); и показать, что преступление действительно имело место. Цифровые доказательства могут помочь выявить характерные признаки поведения (почерк) киберпреступников, таких как разработчики вредоносных программ и хакеры. *Почерк преступника* - это распознаваемый и различимый характер деятельности (например, конкретные методы, инструменты и прозвище), который можно отнести на счет конкретного источника, и который обеспечивает киберпреступнику определенное психологическое или эмоциональное удовлетворение (например, одобрение и признание со стороны коллег).

Рассмотрение цифровых доказательств. На этом этапе оценивается целостность цифровых доказательств путем изучения процедур и инструментов цифровой судебной экспертизы, использованных для получения доказательств, компетенции и квалификации экспертов по цифровой криминалистике, которые получили, сохранили и проанализировали цифровые доказательства и лабораторий цифровой судебной экспертизы, где рассматривались и исследовались доказательства. По сути, цель такой оценки заключается в том, чтобы определить, использовались ли научные принципы для сохранения, получения и анализа цифровых доказательств, и соблюдались ли стандарты при обращении с цифровыми доказательствами и их исследовании (например, были ли инструменты цифровой криминалистики аттестованы, были ли они современными, поддерживались ли они в исправном состоянии и испытывались ли они перед использованием, чтобы обеспечить их надлежащее функционирование).

Эксперты по цифровой криминалистике дают показания в суде, чтобы рассказать о своей квалификации и разъяснить следующие вопросы: как работают цифровые устройства, Интернет-платформы и другие источники, связанные с ИКТ; процесс цифровой судебной экспертизы; почему использовался тот или иной инструмент цифровой криминалистики, а не другие инструменты; каким образом были сохранены, получены и проанализированы цифровые доказательства; толкование результатов проведенного анализа и точность этих толкований; и любые изменения данных, которые имели место, и почему они имели место.

Принятия решения в отношении допустимости цифровых доказательств. На этом этапе подлинность, целостность и достоверность цифровых доказательств оценивается на основе результатов оценки процедуры цифровой судебной экспертизы, проведенной на предыдущем этапе (т.е. на этапе *рассмотрения цифровых доказательств*); например, оценивается использование надежных с точки зрения криминалистики методов и инструментов для получения цифровых доказательств и показания свидетелей-экспертов и экспертов по цифровой криминалистике для подтверждения подлинности, целостности и достоверности этих доказательств. Цифровое доказательство является допустимым, если оно устанавливает фактические обстоятельства дела, остается без изменений на протяжении всего процесса цифровой судебной экспертизы, а результаты экспертизы являются достоверными, надежными и прошли экспертную оценку. Для того чтобы результаты были признаны допустимыми, они должны толковаться непредвзято, и должна быть раскрыта информация об ошибках и неопределенностях в результатах, а также ограничениях в толковании результатов.

Таким образом, эта трехэтапная модель объединяет общие правовые и технические требования в отношении допустимости доказательств в разных юрисдикциях. Стандартизация практики цифровой судебной экспертизы является ключом к обеспечению допустимости цифровых доказательств в разных странах. Учитывая транснациональный характер киберпреступности, унификация практических методов проведения цифровой судебной экспертизы не только имеет первостепенное значение для расследования киберпреступлений, но также является необходимой для осуществления международного сотрудничества по делам, связанным с киберпреступностью.

Вопросы для обсуждения:

1. Что было включено в СОП?
2. Какие процедуры обращения с цифровыми доказательствами были охвачены?
3. Были ли охвачены в СОП какие-либо уникальные ограничения, которые могут встречаться во время расследования? Если да, то какие?
4. Какие требования предъявляются к квалификации экспертов по цифровой криминалистике?
5. Оцениваются ли эти квалификации? Если да, то каким образом?
6. Почему необходимо привлекать квалифицированных экспертов по цифровой криминалистике?

Тема 7. Международное сотрудничество в борьбе с киберпреступностью.

1. Суверенитет и юрисдикция. *Территориальный суверенитет* означает полное и исключительное осуществление государством своих прав и полномочий в отношении своей географической территории.

Защита суверенитета занимает видное место в международных и региональных правовых документах в области борьбы с киберпреступностью. В качестве примера можно привести Конвенцию Лиги арабских государств о борьбе с преступлениями в области информационных технологий 2010 года. В частности, статья 4 этой конвенции гласит: «Каждое государство-участник обязуется, руководствуясь своими собственными законами или конституционными принципами, осуществлять свои обязательства согласно настоящей конвенции в соответствии с принципами суверенного равенства и территориальной целостности государств и принципом невмешательства во внутренние дела других государств».

Территориальный суверенитет может распространяться на киберпространство, в частности, на инфраструктуру информационно-коммуникационных технологий (ИКТ) государств. Государственный суверенитет может быть нарушен, когда третьи стороны получают несанкционированный доступ к ИКТ в зарубежных странах без ведома и разрешения страны, в которой расположены ИКТ, и/или ее правоохранительных органов. Суверенитет считается нарушенным даже в том случае, если такой несанкционированный доступ осуществляется в рамках расследования киберпреступления, совершенного в другой стране, когда эта страна пытается определить источник кибератаки и/или предотвратить ее совершение (тактика, известная как *обратный взлом* или *хакерская контратака*).

Юрисдикция, которая имеет привязку к суверенитету (УНП ООН, 2013, примечание 9, стр. 205), обеспечивает государствам права и полномочия определять и сохранять обязанности и права людей на своей территории, обеспечивать соблюдение законодательства и наказывать за нарушения законов. Государства в первую очередь заявляют о своей юрисдикции в отношении преступлений, совершенных на их территории (*принцип территориальности*). Статья 22(1) Конвенции Совета Европы о компьютерных преступлениях 2001 года гласит: «Каждая Сторона принимает законодательные и иные меры, необходимые для установления юрисдикции в отношении любого правонарушения, предусмотренного в настоящей Конвенции, когда такое правонарушение совершено на ее территории». Тем не менее, как справедливо отмечают Бреннер и Купс (Brenner and Koops, 2004), определение того, «было ли преступление совершено на территории страны, является, однако, непростой задачей, когда преступление было связано с использованием киберпространства» (стр. 10).

Юрисдикция в отношении киберпреступлений определяется другими факторами, такими как гражданство правонарушителя (принцип гражданства; активный персональный принцип), гражданство жертвы (принцип гражданства; пассивный персональный принцип) и последствия киберпреступления для интересов и безопасности государства (принцип защиты), если только можно установить «наличие «достаточной или подлинной связи» между киберпреступлением и государством, осуществляющим юрисдикцию» (процитировано в УНП ООН, 2013, стр. 206).

Например, в Великобритании Апелляционный суд в деле R v. Sheppard and Anor (2010 г.) оставил в силе решение о применении положений Закона «Об общественном порядке» 1986 года к материалам, подстрекающим к расовой ненависти, которые были выложены на веб-сайте, размещенном на сервере в США, и обвинительный приговор в отношении двух жителей Великобритании за публикацию этих материалов.

Юрисдикция в отношении киберпреступлений устанавливается в соответствии с национальным законодательством о киберпреступности. Например, в Малайзии Закон «О компьютерных преступлениях» 1997 года установил юрисдикцию государства в отношении киберпреступлений. В частности, статья 9 этого Закона гласит, что «положения настоящего Закона в отношении любого лица, независимо от его гражданства или подданства, имеют юридическую силу как на территории Малайзии, так и за ее пределами, и в случаях, когда преступление, предусмотренное настоящим Законом, совершается любым лицом, находящимся в любом месте за пределами Малайзии, это лицо может быть привлечено к ответственности за такое преступление, как если бы оно было совершено в любом месте на территории Малайзии». Для сравнения, Танзания заявляет о своей юрисдикции в отношении киберпреступления в случаях, когда действие или бездействие, составляющее преступление, совершено полностью или частично - на территории Объединенной Республики Танзании; на борту морского или воздушного судна, зарегистрированного в Объединенной Республике Танзании; гражданином Объединенной Республики Танзании; гражданином Объединенной Республики Танзании, который проживает за пределами Объединенной Республики Танзании, если действие или бездействие в равной степени представляет собой преступление согласно законодательству этой страны; или любым лицом, независимо от его гражданства, подданства или местонахождения, когда преступление совершено с использованием компьютерной системы, устройства или данных, находящихся на территории Объединенной Республики Танзании; или совершено в отношении компьютерной системы, устройства или данных либо лица, находящихся в Объединенной Республике Танзании (статья 30 Закона «О киберпреступлениях» 2015 года).

При этом Кения устанавливает свою юрисдикцию в отношении киберпреступлений следующим образом: действие или бездействие, совершенное за пределами Кении, которое, если совершено в Кении, является преступлением в соответствии с настоящим Законом, считается совершенным в Кении, если - лицо, совершившее действие или бездействие, является гражданином Кении; или обычно проживает в Кении; и действие или бездействие совершено против гражданина Кении; против имущества, принадлежащего правительству Кении за пределами Кении; или чтобы заставить правительство Кении совершить какие-либо действия или воздержаться от их совершения; или лицо, совершившее действие или бездействие, после его совершения находится на территории Кении (статья 66 Закона «О неправомерном использовании компьютерных технологий и

киберпреступлениях» 2018 года).

В соответствии с этими и другими национальными законами о киберпреступности юрисдикция устанавливается в основном по признаку местонахождения преступников или жертв и последствий киберпреступлений.

2. Официальные механизмы международного сотрудничества.

Успех международного сотрудничества зависит от наличия унифицированных национальных законодательств в области борьбы с киберпреступностью, предусматривающих уголовную ответственность за совершение киберпреступлений, и национальных процессуальных законодательств о киберпреступности, которые устанавливают нормы доказательственного права и правила осуществления уголовного судопроизводства. Международному сотрудничеству может также способствовать унификация двусторонних, региональных и многосторонних правовых документов, касающихся киберпреступности. Присоединение к региональным и многосторонним документам о борьбе с киберпреступностью и их ратификация также необходимы для придания этим документам обязательной юридической силы.

Международному сотрудничеству также способствуют двусторонние, региональные и многосторонние договоры в области борьбы с киберпреступностью при условии признания соответствующего деяния преступлением, т.е. пункта в договорах, в соответствии с которым предполагаемое деяние должно считаться противозаконным в сотрудничающих странах. При отсутствии обоюдного признания соответствующего деяния преступлением и унифицированных законов создаются «безопасные убежища» для лиц, совершивших киберпреступления, в которых исполнители киберпреступлений не могут подвергаться судебному преследованию. Это можно было наблюдать в 2000 году на примере случая с создателем и распространителем компьютерного вируса «LOVE BUG», которого невозможно было привлечь к уголовной ответственности, поскольку на момент инцидента его действия не считались преступлением в стране его проживания на Филиппинах.

Тем не менее, международное сотрудничество все еще возможно даже без строгого толкования требования относительно обоюдного признания соответствующего деяния преступлением. Более того, «когда применительно к вопросам международного сотрудничества требуется соблюдение принципа обоюдного признания соответствующего деяния преступлением, этот принцип считается соблюденным независимо от того, включает ли законодательство запрашиваемого Государства-участника соответствующее деяние в ту же категорию преступлений или описывает ли оно его с помощью таких же терминов, как запрашивающее Государство-участник, если деяние, образующее состав преступления, в связи с которым запрашивается помощь, признано уголовно наказуемым в соответствии с законодательством обоих Государств-участников» (статья 43(2), Конвенция ООН против коррупции 2003 года).

Однако существуют исключения из требования в отношении обоюдного признания соответствующего деяния преступлением. Например, статья 29(3) Конвенции Совета Европы о компьютерных преступлениях 2001 года не требует обоюдного признания соответствующего деяния преступлением при необходимости «неотложного обеспечения сохранности компьютерных 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» по основным правонарушениям, перечисленным в настоящей Конвенции (в статьях с 2 по 11). Статья 29(4) предусматривает право государств отказывать в просьбе об обеспечении сохранности в случаях, если в рамках взаимной правовой помощи условие о квалификации правонарушения как уголовно наказуемого обеими Сторонами выдвигается для правонарушений, не перечисленных в конвенции.

В дополнение к требованию относительно обоюдного признания соответствующего деяния преступлением другим существенным требованием для международного сотрудничества является соблюдение обязательств международного права в области прав человека (УНП ООН, 2013, стр. 229). Просьба об оказании международной помощи может быть отклонена, если в результате удовлетворения этой просьбы запрашиваемое государство нарушит свои международные обязательства в области прав человека.

Официальные механизмы международного сотрудничества включают в себя двусторонние, региональные и многосторонние договоры в области борьбы с киберпреступностью. Вопросы сотрудничества занимают видное место в этих договорах. Например, Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации 2001 года содержит несколько статей, посвященных международному сотрудничеству (статьи 5-7), в которых перечислены формы сотрудничества, охватываемые этим соглашением, именно: обмен информацией; предоставление правовой помощи в соответствии с международными документами; предупреждение, выявление, пресечение и расследование преступлений в сфере компьютерной информации и т.п., а также способы, при помощи которых государства-члены могут запрашивать помощь, и руководящие указания для государств-членов в отношении исполнения запросов. В статье 8 данного Соглашения указаны обстоятельства, при которых в просьбе об оказании помощи может быть отказано (а именно: когда исполнение запроса противоречит национальному законодательству запрашиваемого государства), и требование, в соответствии с которым государство, отказывающееся исполнять запрос, обязано письменно уведомить запрашивающее государство об отказе с указанием причин отказа.

Кроме того, статьи 32 и 34 Конвенции Лиги арабских государств о борьбе с преступлениями в области информационных технологий 2010 года

содержат положения об оказании взаимной помощи, процедурах сотрудничества и подачи запросов об оказании взаимной помощи. Более того, статья 28 Конвенции Африканского союза о кибербезопасности и защите персональных данных 2014 года включает в себя положения об унификации, взаимной правовой помощи по делам, связанным с киберпреступностью, и обмене информацией. В положении об обмене информацией содержится призыв к государствам создавать учреждения, которые могут содействовать обмену информацией об угрозах кибербезопасности и уязвимостях, такие как группы реагирования на компьютерные инциденты (CERT) или группы реагирования на инциденты в сфере компьютерной безопасности (CSIRT). В соответствии со статьей 28(4) государствам предписано «использовать существующие механизмы международного сотрудничества», которые могут включать в себя «международные, межправительственные, региональные или государственно-частные партнерства», для принятия мер реагирования на киберпреступность.

Другими механизмами, которые способствуют международному сотрудничеству в расследовании киберпреступлений и судебном преследовании киберпреступников, являются договоры об оказании взаимной правовой помощи и выдаче. Договоры о взаимной правовой помощи (ДВПП) представляют собой соглашения между странами, которые применяются к преступлениям из перечня, приведенного в этих соглашениях, и определяют виды помощи, оказываемой каждой страной (например, сбор доказательств) при проведении расследований (Maras, 2016, p. 78). Подход, основанный на перечне преступлений, является весьма устаревшим и не учитывает эволюционирующий характер киберпреступности. Учитывая изменяющийся характер преступности (и киберпреступности), в некоторых ДВПП вместо указания перечней преступлений стороны договариваются сотрудничать в расследованиях и судебном преследовании в отношении всех преступлений, считающихся таковыми по их внутреннему законодательству за некоторыми исключениями.

Запросы об оказании взаимной помощи должны составляться в письменной форме и включать в себя следующую информацию: наименование запрашивающего органа; цель запроса; описание запроса; расследование или судебное разбирательство, к которому относится запрос об оказании помощи; описание правонарушения или правонарушений и нарушенных законов; любые просьбы в отношении процедур, которые необходимо соблюсти для получения, обеспечения сохранности и передачи вещественных и цифровых доказательств запрашивающему органу; сроки обеспечения сохранности данных и исполнения запроса; и любая другая информация, которая поможет запрашиваемому государству исполнить запрос (см., например, статью 5 Конвенции об оказании взаимной помощи по уголовным вопросам 1992 года Экономического сообщества западноафриканских государств (ЭКОВАС).

В исполнении запросов об оказании взаимной помощи может быть отказано при определенных обстоятельствах. Например, если запрос «нанесет ущерб суверенитету, безопасности и общественному порядку» (статья 4

Конвенции ЭКОВАС об оказании взаимной помощи по уголовным вопросам; см. также статью 2 Европейской конвенции о взаимной правовой помощи по уголовным делам 1959 года, статью 25(4) Конвенции Совета Европы о компьютерных преступлениях и статью 18 Закона Алжира No.09-04 от 14 числа месяца Шаабан 1430 года от 5 августа 2009 года соответственно, содержащую специальные правила предотвращения преступлений в сфере информационных технологий и связи и борьбы с ними). В просьбах об оказании взаимной правовой помощи может быть отказано, если, например, запрос «касается правонарушения, рассматриваемого запрашиваемой Стороной как политическое преступление или как правонарушение, связанное с политическим преступлением» (статья 25(4) Конвенции о компьютерных преступлениях). В просьбе о предоставлении данных также может быть отказано, если исполнение запроса или раскрытие данных приведет к нарушению запрашиваемым государством международных обязательств в области прав человека. Значительные временные задержки, т.е. когда «речь идет о нескольких месяцах» также имеют место при использовании иных официальных механизмов сотрудничества. Такие задержки являются весьма проблематичными, учитывая неустойчивость цифровых доказательств. Хотя некоторые страны издают руководства по составлению запросов об оказании взаимной правовой помощи и судебных поручений и даже составляют образцы запросов, эта практика не является общепринятой. С целью оказания содействия странам в составлении запросов об оказании взаимной помощи, Управление Организации Объединенных Наций по наркотикам и преступности (УНП ООН) разработало Программу составления просьб об оказании взаимной правовой помощи, чтобы упорядочить эту процедуру путем унификации форматов запросов и, тем самым, ускорить процессы подачи запросов и их исполнения.

Договоры о выдаче, такие как Европейская конвенция о выдаче 1957 года и Межамериканская конвенция ОАГ об экстрадиции 1981 года, представляют собой соглашения о задержании и выдаче лиц запрашивающей стране в случаях, когда преступление, влекущее выдачу, соответствует установленному минимальному порогу наказания. Например, в соответствии со статьей 3 Конвенции ЭКОВАС о выдаче 1994 года порог наказания составляет «минимум два года». Региональные ордеры на арест, такие как европейский ордер на арест, обеспечивают возможность для ареста преступников за преступления, связанные с компьютерами, которые «караются в выдающем ордер государстве наказанием или мерой безопасности, связанными с лишением свободы с верхним пределом не менее трех лет… без проведения проверки на предмет двойной преступности деяния обоюдного признания деяния преступлением» (статья 2(2), Рамочное решение Совета Европейского союза 2002/584/ПВД от 13 июня 2002 года «О европейском ордере на арест и о процедурах передачи лиц между государствами-членами» - заявления, сделанные некоторыми государствами-членами в связи с принятием рамочного решения).

Наличие договора о выдаче не гарантирует, что лицо будет выдано

запрашивающей стране. Это наблюдалось в случае с Лори Лав (Lauri Love), британским хакером, в выдаче которого США было отказано (Parkin, 2017), несмотря на существование подписанного в 2003 году договора об экстрадиции между Великобританией и США.

Кроме того, договоры о выдаче включают в себя условия, при которых выдача не производится. Например, в соответствии с Межамериканской конвенцией ОАГ об экстрадиции запросы о выдаче отклоняются, когда наказанием за преступление является пожизненное заключение или смертная казнь (статья 9). В выдаче также будет отказано в случаях, когда лицо, подлежащее выдаче, будет подвергнуто бесчеловечному или унижающему достоинство обращению или наказанию (например, статья 5 Конвенции ЭКОВАС о выдаче и статья 9 Межамериканской конвенции ОАГ об экстрадиции). Запросы о выдаче могут также отклоняться по иным причинам, таким как отсутствие достаточных доказательств, обосновывающих выдачу (например, Закон Ботсваны о выдаче 1990 года), когда запрос связан с преступлением, не влекущим выдачу (например, военное преступление, статья 7 Конвенции ЭКОВАС о выдаче), или когда запрашивается выдача лица, являющегося гражданином запрашиваемой страны (например, статья 698 Уголовно-процессуального кодекса Алжира и статья 5 (LI) Конституции Бразилии). Что касается выдачи граждан запрашиваемых государств, то принцип невыдачи собственных граждан закреплен в конституции, а также в региональных и международных договорах. Независимо от этого принципа, «международное публичное право закрепляет за государствами юридическое обязательство выдавать или осуществлять судебное преследование (*aut dedere aut judicare*) лиц, совершивших серьезные международные преступления». Некоторые договоры об ордерах на арест могут также исключать из сферы своего действия определенные правонарушения, такие как политические преступления (например, см. статью 3 Договора о признании ордеров на арест Карибского сообщества или КАРИКОМ 2008 года).

3. Неофициальные механизмы международного сотрудничества.

Неофициальные механизмы международного сотрудничества, такие как обмен информацией между правоохранительными органами, также используют в борьбе киберпреступлений (James and Gladyshev, 2016). Тип информации, которой обмениваются правоохранительные органы по неофициальным каналам, варьирует в зависимости от конкретного государства. В Австралии «органы власти имеют возможность предоставлять следующие виды помощи в рамках межведомственного сотрудничества: взятие добровольных показаний свидетелей, проведение добровольных опросов свидетелей, взятие добровольных свидетельских показаний по видеосвязи, принятие сотрудников иностранных полицейских органов, проводящих расследования в Австралии, обмен оперативными данными, осуществление физического наблюдения, получение сведений о судимости или получение общедоступных материалов» (UNODC, «Informal cooperation channels: Australia»). Другие страны договариваются о совместном

использовании некоторых данных личного характера. Существует механизм неофициального международного сотрудничества в области судебного преследования по делам, связанным с киберпреступностью: Глобальная прокурорская сеть по противодействию электронным преступлениям (GPEN) Международной ассоциации прокуроров.

Неофициальные механизмы сотрудничества способствуют оперативному обмену информацией между правоохранительными органами т.е. в течение дней, а не месяцев (УНП ООН, 2013, стр. 239). Кроме того, сети 24/7 создаются с целью получения неотложных запросов о предоставлении цифровых доказательств и содействия международному сотрудничеству. Неофициальные каналы сотрудничества в основном используются для получения юридических и технических консультаций и содействия по делам, связанным с киберпреступностью, а не для запросов о сборе цифровых доказательств (УНП ООН, 2013, стр. 239). Например, в Японии запросы о предоставлении информации по неофициальным каналам разрешается исполнять только в том случае, если запрашивающая страна не намерена использовать эту информацию в качестве доказательств (UNODC, «International cooperation: Japan»). Если страна намеревается использовать эту информацию в качестве доказательства, необходимо направить официальный запрос об оказании взаимной правовой помощи. Цифровые доказательства, полученные по этим каналам, могут быть признаны недопустимыми в национальных судах запрашивающего государства, если не поддерживается система охраны доказательств. Если информация неофициально передается правоохранительными органами Соединенных Штатов Америки, Парагвая, Аргентины (и других стран), запрашивающие страны должны действовать по официальным каналам. Международные и региональные организации также оказывают содействие неофициальному международному сотрудничеству. Например, срочные запросы об оказании взаимной помощи могут направляться в Организацию американских государств (UNODC, «Channels for urgent requests»). Срочные запросы об оказании помощи можно также направлять через ИНТЕРПОЛ (UNODC, «Channels for urgent requests for MLA in cybercrime cases: Liechtenstein»), крупнейшую в мире международную полицейскую организацию, которая своей глобальной полицейской телекоммуникационной сетью I-24/7 охватывает более 190 стран. Посредством этой сети национальные правоохранительные органы делятся опытом, технологиями и ресурсами для борьбы с транснациональными преступлениями.

Интерпол выступает в качестве узла связи между странами, помогая им распространять информацию, например, *уведомления*, и даже оказывая им содействие в координации совместных операций. Например, в 2012 году Интерпол помог местным властям в Испании, Аргентине, Чили и Колумбии арестовать 25 членов международной хакерской группы Anonymous в рамках операции «Разоблачение» (Operation Unmask) (Whiteman, 2012; Interpol, «Operation Unmask»). В 2017 году «операция, проведенная под руководством Интерпола, с участием правоохранительных органов Индонезии, Малайзии,

Мьянмы, Филиппин, Сингапура, Таиланда и Вьетнама», а также Китая и организаций частного сектора позволила «идентифицировать около 9.000 командных серверов (C2) и сотни скомпрометированных веб-сайтов, включая правительственные порталы» (INTERPOL, 2017).

В статье Уайтмена (Whiteman, 2012) говорится, что подозреваемых арестовал Интерпол. Это ошибка. Интерпол не имеет полномочий арестовывать преступников. Интерпол может помочь создать нечто вроде *совместной следственной группы* (Europol, n.d.), которая может оказать содействие в проведении расследований уголовных дел, но только местные следователи имеют полномочия производить аресты на территории своих стран. К сожалению, средства массовой информации зачастую неправильно изображают Интерпол как международную полицию, обладающую *полномочиями на местах*. Вместо наделения Интерпола полномочиями производить аресты в стране, каждое государство создает свое национальное центральное бюро (НЦБ) (INTERPOL, 2018). Штаб-квартира Интерпола может предоставлять информацию и рекомендации НЦБ, но она не может принудить их предпринять какие-либо действия. Кроме того, сотрудниками НЦБ в некоторых случаях - но не всегда - являются местные кадровые полицейские или прокуроры.

4. Хранение и обеспечение сохранности данных и доступ к данным.

Запросы о помощи в рамках международного сотрудничества также могут отклоняться из-за процедурных требований. Рассмотрим, например, практические методы хранения, обеспечения сохранности данных и получения к ним доступа. Исполнение просьбы о предоставлении данных, которые хранят поставщики услуг Интернета и связи, зависит от условий предоставления услуг, политики конфиденциальности и практики ведения бизнеса провайдера услуг. В связи с этим провайдеры услуг отличаются между собой не только типом данных, которые они хранят (например, журналы регистрации IP-адресов или информация о деактивированных учетных записях), но и периодом их хранения дни, недели, месяцы или годы (см., например, «Guidelines for Law Enforcement» («Руководящие принципы обеспечения законности») Twitter и «Data Policy» («Политика использования данных») Facebook для получения дополнительной информации). Политика в отношении хранения данных, а также получения к ним доступа также варьирует в зависимости от национальных, региональных и международных законов в области защиты данных.

Просьбы об *обеспечении сохранности данных* направляются поставщикам услуг правоохранительными органами в целях сохранения данных до того, как они будут удалены или каким-либо образом изменены. Процедура получения доступа к сохраненным данным прописывается в национальном законодательстве. Законные распоряжения (например, судебное постановление или ордер на обыск), если таковые вообще предусмотрены, необходимые для получения разнообразных данных от поставщиков услуг, варьируют в зависимости от конкретной страны. Например, в то время как в Соединенных Штатах повестки и судебные

постановления необходимы для получения *данных, не относящихся к контенту* или *метаданных*; например, данных абонента и IP-адресов, а ордера на обыск - для получения *данных, относящихся к контенту,* например, текстов электронных писем или других сообщений (Закон США «О сохраненных сообщениях» 1986 года; титул II Закона «О конфиденциальности электронных сообщений» 1986 года), турецким правоохранительным органам не требуются законные распоряжения для получения доступа к данным, не относящимся к контенту, и данным, относящимся к контенту (Закон №5651 «Об Интернете»).

Более того, органы, которые могут получить доступ к хранящимся и/или сохраненным данным, также различаются в зависимости от конкретной страны. Например, в Кении сотрудник правоохранительных органов или другое уполномоченное лицо (а именно «эксперт по кибербезопасности, который назначается секретарем Кабинета министров по вопросам национальной безопасности») может получить доступ к хранящимся и/или сохраненным данным в соответствии с Законом Кении «О неправомерном использовании компьютерных технологий и киберпреступлениях» 2018 года, тогда как на Ямайке только сотрудники правоохранительных органов имеют право получать доступ к данным (см. Закон «О киберпреступлениях» 2015 года).

Кроме того, в определенных ситуациях, определяемых национальным законодательством, допускается добровольное раскрытие информации поставщиками Интернет-услуг без наличия законных распоряжений. В качестве примера такой ситуации можно привести экстренный запрос о предоставлении данных с целью предотвращения серьезных телесных повреждений или смерти. Если поставщики услуг отказываются предоставлять запрашиваемые данные добровольно, то при определенных обстоятельствах и в зависимости от конкретного случая, искомых доказательств, бремени доказывания и национального законодательства, эти поставщики услуг могут быть принуждены в предусмотренном законом порядке к предоставлению этой информации.

5. Проблемы, связанные с экстерриториальными доказательствами.

Даже при наличии официальных и неофициальных механизмов международного сотрудничества возникают проблемы при идентификации и сборе цифровых доказательств, хранящихся в облачных хранилищах и у других поставщиков услуг. Проблема облачных вычислений заключается в том, что сложно узнать, где хранятся данные. Без такой информации невозможно определить «соответствующую юрисдикцию, в которую должен направляться запрос о сотрудничестве для получения цифровых доказательств» (УНП ООН, 2013, стр. 241).

Облачные данные могут быть разбиты на фрагменты и храниться в разных местах и в нескольких странах. Такую проблему фрагментации данных можно проиллюстрировать на примере дела *United States v. Microsoft* (2018). В рамках расследования этого дела правительство США выдало ордер на обыск

в соответствии с Законом США о сохраненных сообщениях (SCA) 1986 года, чтобы получить доказательства по делу о незаконном обороте наркотиков. Компания Microsoft удовлетворила этот запрос, передав соответствующие данные, не относящиеся к контенту, которые хранились на серверах в США, например, адресную книгу подозреваемого, но не предоставила правительству США соответствующие данные, относящиеся к контенту, например, содержимое электронных писем этого лица, поскольку эти данные хранились в дата-центре Microsoft в Дублине (Ирландия).

Суть спора, который лежал в основе дела *United States v. Microsoft* (2018), заключалась в том, позволяют ли положения Закона «О сохраненных сообщениях» получать доступ к данным, находящимся на серверах в другой стране, и считается ли такой доступ юридически необоснованным экстерриториальным применением закона. Сейчас этот вопрос потерял свою актуальность в связи с принятием в США Закона, разъясняющего порядок законного использования данных за рубежом (Закон «Cloud» - «Облако») 2018 года. С его принятием в параграф 2713 Закона «О сохраненных сообщениях» (главы 18 Свода законов США) были внесены следующие поправки: «Поставщик услуг электронной связи или услуг дистанционной обработки данных должен соблюдать обязательства настоящей главы по сохранению, резервному копированию или раскрытию содержимого телеграфных или электронных сообщений и любой записи или иной информации, относящихся к клиенту или подписчику, которые находятся в ведении, распоряжении или под контролем такого поставщика услуг, независимо от того, находится ли такое сообщение, запись или иная информация не территории или за пределами территории Соединенных Штатов». Закон «Cloud» обеспечивает прямой доступ к экстерриториальным данным. Однако «общих стандартов и гарантий, касающихся обстоятельств, если таковые имеются, в соответствии с которыми правоохранительные органы могут иметь прямой доступ к экстерриториальным данным» (УНП ООН, 2013, стр. 240), по состоянию на 2018 год, пока не существует.

6. Национальный потенциал и международное сотрудничество.

Эффективность международного сотрудничества зависит от способности государств исполнять запросы о предоставлении доказательств таким образом, чтобы обеспечить допустимость этих доказательств в суде. Для этого необходимо наличие квалифицированных специалистов в области киберпреступности, которые могут обеспечить получение доказательств в соответствии с национальными нормами доказательственного права и правилами уголовного судопроизводства. Однако таких специалистов не хватает. Более того, страны во всем мире испытывают нехватку национального потенциала, необходимого для борьбы с киберпреступностью (УНП ООН, 2013).

Такой дефицит национального потенциала является результатом нехватки кадровых, финансовых и технических ресурсов (УНП ООН, 2013). Во-первых, во многих странах отсутствует достаточное количество квалифицированных специалистов для проведения расследований

киберпреступлений, а также для судебного преследования киберпреступников и рассмотрения запросов о помощи в рамках международного сотрудничества по делам, связанным с киберпреступностью. Во-вторых, странам может не хватать финансовых ресурсов, необходимых для подбора, найма и удержания квалифицированного персонала, а также для организации регулярной и современной подготовки для следователей, занимающихся киберпреступлениями, и других соответствующих специалистов. В-третьих, в странах отсутствует необходимая материальная база для анализа цифровых доказательств и испытывается нехватка средств для приобретения необходимого оборудования и инструментов цифровой криминалистики для надлежащего проведения расследований киберпреступлений.

Для решения проблемы дефицита национального потенциала были созданы и продолжают создаваться партнерства с национальными, региональными и международными организациями, например, Министерством юстиции США, Организацией американских государств и Международным союзом электросвязи, а также частными компаниями с целью предоставления финансовой, кадровой и технической помощи по вопросам, связанным с киберпреступностью, странам, нуждающимся в такой помощи, и оказания поддержки их усилиям по развитию национального потенциала в области борьбы с киберпреступностью.

Вопросы для обсуждения:

1. Каким образом киберпреступность может нарушать территориальный суверенитет?
2. Какой закон в вашей стране регулирует доступ к хранящимся и/или сохраненным данным?
3. Кто имеет право доступа к этим данным? При каких обстоятельствах?
4. Требуется ли законное распоряжение для получения доступа к данным, относящимся к контенту? Если да, то какое?
5. Требуется ли законное распоряжение для получения доступа к метаданным? Если да, то какое?

Тема 8. Кибербезопасность и предупреждение киберпреступности: стратегии, политика и программы.

1. Управление Интернетом.

По мнению Керра, существуют «два преобладающих взгляда на Интернет»: с одной стороны, Интернет рассматривается как «глобальная мета сеть, которая служит в качестве открытой платформы для передачи информации между конечными пользователями, подключающими свои компьютеры к сети»; с другой стороны, Интернет рассматривается «в контексте приложений, которым он обеспечивает возможность функционирования, и того, как эти приложения влияют на конечных пользователей» (Frischmann, 2003; pp. 205-206; см. также Kerr, 2003, p. 359-

360). Именно последнее из перечисленных представлений об Интернете «приводит к восприятию киберпространства как некоей виртуальной реальности» или среды, в которой ведется онлайновая активность (Frischmann, 2003, p. 206).

В литературе, посвященной теориям регулирования применительно к управлению Интернетом и киберпространством, основное внимание уделяется тому, какие лица, группы, предприятия, организации и государственные учреждения регулируют Интернет и киберпространство, а также способам регулирования киберпространства и Интернета. Эта точка зрения находит подтверждение в литературе, в которой утверждается, что киберпространство и Интернет регулируются, например, законами, кодом компьютерной программы, системной архитектурой и архитектурой Интернета физическими лицами, предприятиями и организациями с некоторым участием государства или без участия государства (т.е. на основе саморегулирования); и физическими лицами, предприятиями и организациями, несущими совместную ответственность за управление (т.е. на основе распределенной защиты).

Интернет влияет на глобальные интересы, и процесс управления им «включает в себя не только вопросы, связанные с присвоением имен и адресов в сети Интернет, которыми занимается Корпорация по распределению имен и номеров в Интернете (ICANN); он также включает в себя другие важные вопросы государственной политики, такие как критически важные интернет-ресурсы, безопасность и защита Интернета, а также аспекты и проблемы развития, связанные с использованием Интернета» (WGIG, 2005, p. 4). Поэтому какая-либо одна организация не может быть назначена - и не была назначена - в качестве единого международного органа управления. Вместо этого процесс управления Интернетом в основном осуществляется на международном уровне несколькими участниками - правительством, частным сектором, научным сообществом и гражданским обществом - и охватывает целый ряд технических и нетехнических вопросов. Тем не менее, страны расходятся во мнениях относительно того, какие участники должны играть основную роль в управлении Интернетом. В то время как некоторые страны полагают, что ответственность за управлением Интернетом должны нести несколько участников, другие страны считают, что управление Интернетом должно входить в сферу исключительной компетенции государства. Даже если страны договорятся о составе участников, ответственных за управление Интернетом, существуют другие препятствия для принятия всеобщих принципов управления Интернетом, которые связаны с различиями в системах уголовного правосудия и законах, действующих в разных странах. Хотя главной целью управления Интернетом является совместное регулирование Интернета всеми странами, реальность такова, что страны расходятся во мнениях относительно того, как должно осуществляться такое регулирование. Это можно наблюдать на примере того, как разные страны относятся к некоторым основополагающим принципам работы Интернета, таким как свобода, т.е. доступ к информации и обмен информацией могут

осуществляться «без обоснованных ограничений», открытость, т.е. беспрепятственный поток информации в сети, функциональная совместимость, т.е. способность различных цифровых устройств и компьютерных систем соединяться, передавать данные и обмениваться данными, безопасность, т.е. защита конфиденциальности, целостности и доступности систем, сетей, услуг и данных и устойчивость, т.е. поддержание работы во время сбоев и изменения условий (Руководящие принципы ОЭСР по разработке политики в области Интернета 2014 года; Африканская декларация о правах и свободах в Интернете 2014 года; ЮНЕСКО, 2015). Из платформы для распространения информации и обмена информацией - в соответствии с принципом открытости - Интернет эволюционировал в платформу для социальных взаимодействий, торговли и коммерции и предоставления государственных услуг. В то же время Интернет и ИКТ использовались и продолжают использоваться неправомерно и злонамеренно людьми и организациями, представляющими угрозу, и другими злоумышленниками, что способствует росту киберпреступности, и, следовательно, вызывает необходимость усиления мер обеспечения безопасности.

2. Стратегии кибербезопасности: основные особенности.

Стратегии обеспечения кибербезопасности и стратегии противодействия (или предупреждения) киберпреступности являются терминами, которые используются взаимозаменяемо. Хотя стратегии обеспечения кибербезопасности и стратегии противодействия киберпреступности дополняют друг друга и местами пересекаются, между ними существуют различия. В стратегиях противодействия киберпреступности описаны усилия, которые прямо или косвенно связаны с борьбой с киберпреступностью, такие как меры реагирования, принимаемые правоохранительными органами, и содействие национальному и международному сотрудничеству между правительствами, деловыми кругами, научно-образовательными учреждениями, организациями и общественностью в целях контроля и/или снижения уровня киберпреступности. Проще говоря, стратегии противодействия киберпреступности сосредоточены исключительно на мерах политики, программах и практике в области уголовного правосудия и предупреждения преступности. В отличие от них, стратегии обеспечения кибербезопасности содержат руководящие указания по вопросам кибербезопасности которые могут включать в себя указания по предупреждению киберпреступности и определяют задачи, а также планы действий, меры и обязанности учреждений, необходимые для достижения этих целей. Эти стратегии предусматривают принятие правовых, процедурных, технических и институциональных мер, предназначенных для защиты систем, сетей, услуг и данных.

Национальные стратегии кибербезопасности отражают устремления стран в области обеспечения кибербезопасности и предупреждения киберпреступности на национальном и международном уровнях. В этих стратегиях излагаются принципы, на которых основана стратегия,

описываются интересы, которые эта стратегия призвана защищать, определяются инструменты, используемые для продвижения и защиты этих интересов, обозначаются киберугрозы и проблемы, которые эти угрозы представляют для национальной и экономической безопасности, определяются приоритетные задачи политики кибербезопасности и ресурсы, выделяемые для выполнения этих задач. Эти стратегии «призывают органы, ответственные за разработку политики, обозначить стратегические задачи («цели»), определить ресурсы, имеющиеся для выполнения этих задачи («средства»), и разработать руководящие указания относительно того, как следует использовать такие ресурсы для выполнения поставленных задач («способы»)».

В стратегиях кибербезопасности подробно объясняется, почему стратегия является важной и необходимой (контекст), чего нужно добиться (задачи), в чем она состоит, и на что и кого она повлияет (сфера действия) (МСЭ, 2018, стр.30). Ключевыми компонентами этих стратегий являются задачи, приоритетные действия, ожидаемые результаты и механизмы оценки.

Задачи стратегий кибербезопасности включают в себя задачи, связанные с национальной безопасностью, а также задачи, связанные с информационно-коммуникационными технологиями. Например, стратегия кибербезопасности Швеции «основана на целях обеспечения безопасности Швеции: защита жизни и здоровья населения, функционирование общества и его способность поддерживать фундаментальные ценности, такие как демократия, верховенство закона и права и свободы человека. Стратегия также базируется на общей цели политики в области информационных технологий (ИТ) - сделать Швецию мировым лидером в деле реализации возможностей цифровой трансформации» (Swedish Ministry of Justice, 2017, p. 1; см. также: Министерство юстиции Швеции, Национальная стратегия кибербезопасности, «A National Cyber Security Strategy»).

В Нигерии задачами стратегии кибербезопасности 2014 года (Cybersecurity Strategy) являются следующие:

- всеобъемлющее законодательство о киберпреступности и меры противодействия киберугрозам, которые могут быть приняты на национальном уровне и являются актуальными на региональном и глобальном уровнях в контексте обеспечения безопасности киберпространства страны;

- реализация мер по защите критически важной информационной инфраструктуры, а также снижение факторов национальной уязвимости с помощью механизма обеспечения кибербезопасности;

- определение возможностей в сфере эффективного реагирования на компьютерные инциденты;

- национальные механизмы по созданию потенциала, информированию общественности и расширению возможностей повышения квалификации, что необходимо для укрепления нашей способности оперативно и эффективно реагировать на кибератаки;

- надежный механизм для обеспечения участия национальных заинтересованных сторон и международных партнеров в коллективных

усилиях по борьбе с киберугрозами;

- защита правительства от всех форм кибератак и сдерживание таких кибератак;

- координация инициатив в области обеспечения кибербезопасности на всех уровнях правительства страны;

- создание национальных возможностей для противодействия киберугрозам на основе последовательного сотрудничества в рамках государственно-частного партнерства и взаимодействия всех заинтересованных сторон;

- популяризация национальной концепции кибербезопасности путем повышения осведомленности, развития партнерства на основе совместной ответственности и участия надежных заинтересованных сторон;

- содействие координации, сотрудничеству и взаимодействию региональных и глобальных участников в деле обеспечения кибербезопасности (статья 3.3.2).

Цель приоритетных действий заключается в выполнении поставленных задач. Например, в Европейском союзе большинство национальных стратегий обеспечения кибербезопасности в качестве приоритетных действий определяют создание стандартов, норм и законов в области кибербезопасности где это необходимо, поощрение культуры кибербезопасности не только среди соответствующих заинтересованных сторон (например, государственных учреждений, научно-образовательных учреждений, компаний и организаций), но и широкой общественности, а также развитие национального и международного сотрудничества и взаимодействия между соответствующими заинтересованными сторонами (ENISA, 2014). Приоритетные действия, перечисленные в Стратегии национальной кибербезопасности США за 2018 год, включают в себя: «приоритет разработки и внедрения инноваций»; «поощрение всеобщего соблюдения норм в киберпространстве»; «лидерство с объективными и коллективными разведданными»; «совершенствование системы задержания преступников за рубежом» и многие другие действия.

Ожидаемые результаты этих приоритетных действий включают в себя показатели, которые должны быть достигнуты после их осуществления (например, разработка стандартов кибербезопасности). Например, в Стратегии национальной кибербезопасности США 2018 года ожидаемые результаты включают в себя: успешное устранение уязвимостей в структуре кибербезопасности; снижение ущерба от «деструктивной, вредоносной и подрывной хакерской деятельности, направленной против интересов Соединенных штатов, или ее предотвращение» и сдерживание «деятельности, противоречащей ответственному поведению в киберпространстве при помощи мер принуждения, сетевого и иного характера»; и способность Соединенных Штатов «использовать кибер возможности для достижения целей национальной безопасности» (US White House, 2018, p. 3).

3. Национальные стратегии кибербезопасности: жизненные циклы, передовая практика и репозитории.

Жизненный цикл национальной стратегии кибербезопасности состоит из пяти этапов (ITU, 2018, pp. 16-27):

Первый этап - инициирование, который предусматривает определение соответствующих заинтересованных сторон и их ролей в процессе разработки стратегии, а также подготовку плана разработки стратегии.

Второй этап - обзор и критический анализ имеющегося опыта, предусматривает оценку положения дел в стране в области кибербезопасности, выявление угроз кибербезопасности и анализ текущих и будущих рисков кибербезопасности.

Третий этап - разработка национальной стратегии кибербезопасности. Этот этап предусматривает подготовку проекта стратегии, консультации с соответствующими заинтересованными сторонами, окончательную доработку стратегии с учетом замечаний и публикацию стратегии.

Четвертый этап - имплементация, предусматривает разработку плана действий, определение того, какие инициативы, основанные на задачах стратегии, будут реализованы, определение ресурсов, необходимых для реализации этих инициатив, и определение конкретных действий и сроков выполнения этих действий. На этом этапе также разрабатываются параметры и ключевые показатели деятельности для оценки эффективности т.е. своевременности и результативности т.е. позитивного результата инициатив.

Как правило, в планах действий указываются решения или меры, которые могут быть реализованы для достижения целей, заинтересованные стороны, ответственные за выполнение задач, параметры, которые будут использоваться для оценки сроков выполнения задач и достижения желаемых результатов. Планы действий реализуются на национальном уровне (например, Национальная служба безопасности, План действий по реализации концепции кибербезопасности Словацкой Республики на 2015-2020 годы) и региональном уровне (например, План действий по обеспечению кибербезопасности и предупреждению киберпреступности КАРИКОМ).

Пятый этап - мониторинг и оценка, предусматривает оценку соответствия плана действий задачам стратегии кибербезопасности, а также анализ стратегии и плана действий, чтобы установить, сохраняют ли они свою актуальность, удовлетворяют ли они потребностям страны в области обеспечения кибербезопасности, и могут ли они противодействовать новым рискам кибербезопасности. Если задачи стратегии кибербезопасности не выполняются в результате реализации плана действий, в план действий вносятся изменения. Изменения могут также вноситься в стратегию в случае, если она более не является актуальной и не может применяться для противодействия новым угрозам кибербезопасности.

4. Международное сотрудничество по вопросам кибербезопасности.

Международный союз электросвязи (МСЭ), учреждение Организации Объединенных Наций, являющееся «главным всемирным форумом, в рамках которого стороны могут добиваться консенсуса по широкому кругу вопросов, влияющих на будущее направление развития отрасли ИКТ», инициировал Глобальную программу кибербезопасности, которая

представляет для МСЭ «основу международного сотрудничества, цель которого состоит в том, чтобы предложить стратегии для поиска решений в области укрепления доверия и безопасности в условиях информационного общества». В Глобальной программе кибербезопасности МСЭ определены пять стратегических принципов: правовые меры, технические меры, организационные меры, создание потенциала и сотрудничество.

Правовой принцип сосредоточен на унификации регламентов и законов, касающихся кибербезопасности и киберзависимых преступлений, а также преступлений, совершаемых с использованием киберпространства. В качестве примера можно привести законы о борьбе с киберпреступностью.

Технический принцип охватывает существующие технические учреждения, стандарты и протоколы кибербезопасности, а также меры, необходимые для борьбы с угрозами кибербезопасности. Примером технического учреждения является группа реагирования на нарушение компьютерной защиты (CERT), которая определяется как «организация или группа, которая предоставляет четко определенному кругу клиентов услуги и поддержку как для предупреждения инцидентов, связанных с компьютерной безопасностью, так и для реагирования на них».

Принцип, связанный с *организационными мерами*, включает в себя организационные структуры и меры политики в сфере кибербезопасности и учреждения, ответственные за координацию политики обеспечения кибербезопасности. В этот принцип включены национальные стратегии кибербезопасности и национальные механизмы обеспечения кибербезопасности, а также регулирующие органы, которые осуществляют надзор за реализацией этих стратегий и механизмов.

Принцип *создания потенциала* охватывает усилия по поощрению осведомленности, образования и обучения в сфере кибербезопасности. Примерами могут служить кампании по информированию общественности, исследования и разработки в области кибербезопасности, профессиональная подготовка, а также национальные образовательные программы и учебные планы. Принцип *сотрудничества* сосредоточен на межучрежденческих и государственно-частных партнерствах, сетях обмена информацией и соглашениях о сотрудничестве. В качестве примера можно привести австралийскую стратегию международного взаимодействия в киберпространстве (International Cyber Engagement Strategy), целью которой является развитие государственно-частного партнерства и укрепление сотрудничества между странами.

5. Состояние дел в области кибербезопасности.

Состояние дел в области кибербезопасности является термином, используемым для описания возможностей страны, организации или компании для обеспечения кибербезопасности. Существует несколько инструментов, используемых для оценки состояния дел в области кибербезопасности. Одним из таких инструментов является Глобальный индекс кибербезопасности (ГИК) Международного союза электросвязи. Согласно МСЭ, ГИК является инструментом наращивания потенциала,

который оценивает приверженность стран делу обеспечения кибербезопасности, определяет их состояние дел в области кибербезопасности и аспекты, требующие улучшения. Состояние дел стран в области кибербезопасности может оцениваться на основе пяти принципов (правовые, технические, организационные меры, создание потенциала и сотрудничество), определенных в Глобальной программе кибербезопасности МСЭ. В частности, страны получают баллы ГИК в зависимости от уровня их приверженности этим пяти принципам. Эти оценки относят страны в группы *начинающих* т.е. стран, которые делают первые шаги, демонстрирующие их приверженность этим принципам, *развивающихся* т.е. стран, которые привержены этим принципам и *ведущих* стран т.е. стран, принявших высокие обязательства в отношении этих принципов (ITU, 2017, p. 13). Результаты исследования Глобального индекса кибербезопасности 2017 года показали, что половина стран-респондентов не имеют национальной стратегии кибербезопасности (ITU, 2017). Результаты исследования Глобального индекса кибербезопасности 2017 года также выявили значительные различия между государствами внутри и за пределами их регионов с точки зрения принятых обязательств в отношении обеспечения кибербезопасности. Результаты также показали, что степень обязательств стран в отношении обеспечения кибербезопасности варьирует в зависимости от конкретного показателя т.е. страны получили высокие оценки по одному показателю, но средние и низкие оценки по другим показателям (для получения подробной информации о результатах см. ITU, 2017). Однако, для того чтобы усилия были эффективными, обязательства в области обеспечения кибербезопасности должны быть выполнены по всем показателям.

Глобальный центр создания потенциала в области кибербезопасности (GCSCC) при Оксфордском университете разработал модель зрелости потенциала в области кибербезопасности (Cybersecurity Capacity Maturity Model) (CMM) для оценки состояния дел стран в сфере кибербезопасности (т.е. зрелости возможностей обеспечения кибербезопасности) путем изучения усилий стран в таких областях, как «нормативное регулирование и стратегия в области кибербезопасности», «киберкультура и общество», «образование, обучение и навыки в области кибербезопасности», «нормативно-правовая база», а также «стандарты, организации и технологии» (Global Cyber Security Capacity Centre, 2016, pp. 10-13). Эта оценка позволяет странам получить информацию об уровне зрелости их потенциала: *начальный* (т.е. кибербезопасность отсутствует или только начинает развиваться); *формирующийся* (т.е. существует некоторая кибербезопасность); *установленный* (т.е. кибербезопасность существует; уделяется минимальное внимание вопросу выделения ресурсов); *стратегический* (т.е. осознанный и взвешенный выбор в отношении кибербезопасности); и *динамичный* (т.е. меры обеспечения кибербезопасности адаптируются к изменениям условий и потребностей) (Global Cyber Security Capacity Centre, 2016, p. 7). Модель CMM использовалась для оценки многих стран по всему миру по отдельности или в

рамках регионального исследования (Global Cyber Security Capacity Centre, 2018). В дополнение к модели CMM, Глобальный центр создания потенциала в области кибербезопасности разработал портал Cybersecurity Capacity Portal, который содержит материалы по созданию потенциала в области кибербезопасности, информацию о передовой практике и облегчает обмен информацией, чтобы помочь странам улучшить состояние дел в области кибербезопасности.

Вопросы для обсуждения:

1. Включены ли эти принципы в национальную стратегию кибербезопасности? 2. Если да, то какие?

3. Если нет, то какие принципы не включены и почему?

4. Существуют ли какие-либо другие принципы, которые включены в национальную стратегию кибербезопасности?

5. Если да, то какие, и по какой причине они могли быть включены?

Тема 9. Кибербезопасность и предупреждение киберпреступности: практические методы и меры.

1. Активы, уязвимости и угрозы.

Меры обеспечения кибербезопасности реализуются с целью защиты активов, которые определяются как «нечто важное или ценное, включая людей, имущество, информацию, системы и оборудование» (Maras, 2014b, p. 21), таких как, работники организации, цифровые устройства, компьютерное программное обеспечение и данные (ITU, 2008). Активы восприимчивы (т.е. уязвимы) к различным видам ущерба. В частности, активы имеют внутренние или встроенные и внешние или привнесенные *уязвимости*. Например, применительно к информационно-коммуникационным технологиям (ИКТ), внутренние уязвимости могут присутствовать в конструкции системы, конфигурациях системы безопасности, аппаратном и программном обеспечении и в других компонентах (ENISA, 2017). Примером может служить программная ошибка. В 2018 году была обнаружена программная ошибка в кошельке криптовалюты Monero, которая позволяла отдельным лицам использовать эту уязвимость для незаконного удвоения сумм перевода криптовалюты (Barth, 2018). Напротив, внешние уязвимости не присутствуют внутри самих активов, таких как устройства ИКТ. Примером такой уязвимости является пользователь ИКТ. Пользователь может выполнять действия, которые делают устройство восприимчивым к заражению вредоносными программами (например, открывать вложения в электронных письмах от неизвестных отправителей). Встроенные и привнесенные свойства делают активы уязвимыми для *угроз* (т.е. ко всему, что может вызвать неблагоприятные последствия). Эти угрозы могут причинить непреднамеренный и преднамеренный ущерб. Например, аппаратное обеспечение цифрового устройства может работать со сбоями или может быть преднамеренно повреждено в результате эксплуатации уязвимостей

встроенного программного обеспечения (ENISA, 2017).

2. Риск.

Решения о защите активов принимаются в условиях неопределенности; то есть они принимаются при отсутствии полной информации о потенциальных угрозах, уязвимостях и эксплуатации этих уязвимостей. Первоначально *риск* имел узкое определение как вероятность (или возможность) угрозы и ее воздействия (или последствий) в случае ее материализации (Dali and Lajtha, 2012). Эта концепция риска изображается следующей формулой:

Р иск = В ероятность х П оследствия

Формулы, подобные приведенной выше, используются для количественной оценки рисков.

Процесс оценки рисков предполагает выявление уязвимостей активов, определение внутренних и внешних угроз и получение информации о них от средств массовой информации, государственно-частных партнерств и других лиц из государственного и частного секторов, а также определение последствий и вероятностей угроз (NIST, 2018). Целью оценки рисков «является выявление угроз; ущерба т.е. неблагоприятного воздействия), который может быть причинен, учитывая возможность эксплуатации уязвимостей; и вероятность того, что ущерб будет причинен» (NIST, 2012).

После завершения оценки рисков определяются меры реагирования на риски, т.е. меры по *обработке рисков*, приоритетность которых устанавливается на основе имеющихся ресурсов (например, финансовых) и потребностей. На этом этапе реализуются меры по устранению, уменьшению или смягчению рисков.

3. Раскрытие информации об уязвимостях.

Термины «информационная безопасность» и «кибербезопасность» используются взаимозаменяемо, хотя это не вполне правильно. Несмотря на отсутствие согласованного определения понятия информационной безопасности, широко используется определение, включенное в стандарт ISO/IEC 27002. В стандарте ISO/IEC 27002 информационная безопасность определяется как «сохранение конфиденциальности, целостности и доступности информации». Как и в случае информационной безопасности, не существует универсального определения понятия кибербезопасности. Согласно Международному союзу электросвязи (МСЭ), «кибербезопасность состоит в стремлении обеспечить достижение и сохранение свойств безопасности у ресурсов организации или пользователя, направленных против соответствующих угроз безопасности в киберсреде». Таким образом, кибербезопасность подразумевает защиту не только киберпространства, «но и тех, кто функционирует в киберпространстве, и любые их ресурсы, которые могут быть доступны через киберпространство».

Стандарт ISO/IEC 27002 включает в себя 14 областей контроля информационной безопасности, а также руководство по реализации мер контроля информационной безопасности и требования для каждой из этих мер контроля. Этими областями являются: политика информационной

безопасности; организация информационной безопасности; безопасность персонала; управление активами; контроль доступа; криптография; физическая безопасность и защита от природных угроз; безопасность производственной деятельности; безопасность обмена информацией; приобретение, разработка и обслуживание систем; отношения с поставщиками; управление инцидентами информационной безопасности; аспекты информационной безопасности в менеджменте непрерывности бизнеса; и соответствие.

Информационная безопасность и кибербезопасность зависят от раскрытия информации об уязвимостях. Когда уязвимости обнаруживаются исследователями и специалистами в данной области, раскрытие информации о таких уязвимостях может быть либо полным, либо ответственным. *Полное раскрытие* предполагает обнародование информации об уязвимостях программного или аппаратного обеспечения в Интернете (например, на веб-сайте) до того, как эти уязвимости будут устранены. Напротив, *ответственное раскрытие* подразумевает нераскрытие информации об уязвимости до тех пор, пока организация, ответственная за аппаратное или программное обеспечение, не устранит уязвимость. При ответственном раскрытии исследователь или специалист связывается с затронутой организацией и ждет, пока организация не выпустит исправление для выявленной уязвимости. После выпуска исправления исследователь или специалист может официально раскрыть информацию об уязвимости и получить признание и вознаграждение за нахождение уязвимости. При использовании такого метода раскрытия информации исследователь или специалист может просить о предоставлении ему так называемого идентификатора общеизвестных уязвимостей информационной безопасности (CVE). CVE, который представляет собой «список общих идентифицирующих элементов общеизвестных уязвимостей кибербезопасности» (CVE, n.d.), используется для отслеживания уязвимостей в основных элементах программного обеспечения, а также лиц, обнаруживающих такие уязвимости. В дополнение к методам полного и ответственного раскрытия информации, исследователь или специалист может выбрать принцип нераскрытия уязвимости. Еще одним методом раскрытия информации является *координированное раскрытие уязвимостей*, которое означает «процесс сбора информации от лиц, обнаруживших уязвимости, координации обмена этой информацией между соответствующими заинтересованными сторонами и раскрытие информации о наличии уязвимостей программного обеспечения и смягчении негативных последствий различным заинтересованным сторонам, включая общественность».

4. Меры обеспечения кибербезопасности и удобство использования.

В идеале меры реагирования на риски должны преследовать цель защиты конфиденциальности, целостности и доступности систем, сетей, услуг и данных при одновременном обеспечении удобства использования этих мер (NIST, 2018). *Удобство использования* цифровых устройств (т.е. легкость, с

которой они могут использоваться) зачастую имеет преимущество перед безопасностью этих устройств и их содержимого. Однако безопасность и удобство использования не обязательно являются взаимоисключающими. Меры кибербезопасности могут обеспечивать как безопасность, так и удобство использования.

К мерам кибербезопасности относятся меры, направленные на установление личности пользователя, чтобы предотвратить несанкционированный доступ к системам, услугам и данным. Эти меры *аутентификации* включают в себя проверку того, «что вы знаете» (например, пароли, парольные фразы и PIN-коды), «что вы имеете» (например, смарт-карты и токены) и «кем вы являетесь» (например, биометрические данные, такие как отпечатки пальцев). Многофакторная аутентификация (МФА) предполагает использование двух или более таких методов аутентификации для установления личности пользователя.

Еще одним типом мер кибербезопасности является контроль доступа. *Средства контроля доступа*, которые устанавливают привилегии, определяют санкционированный доступ и предотвращают несанкционированный доступ, включают в себя меры аутентификации и другие меры, предназначенные для защиты имен и паролей для входа в систему, приложения, веб-сайты, социальные сети и другие онлайн-платформы и цифровые устройства. В качестве примера можно привести ограничение количества попыток ввода пароля на смартфоне. На смартфонах есть опция, которая позволяет пользователям стирать все данные на устройстве после определенного количества неудачных попыток ввода пароля. Эта функция была создана с тем, чтобы обеспечить пользователям возможность защиты данных на своих устройствах в случае кражи цифрового устройства и получения к ним доступа без авторизации пользователя.

Другие примеры средств контроля доступа включают в себя добавление времени ожидания при каждом неверном вводе пароля и/или ограничение количества неудачных попыток ввода пароля, которые могут быть допустимыми в течение дня, и блокирование учетных записей пользователей на некоторое время. Эти средства управления, контролирующие попытки входа в систему, предназначены для защиты от попыток получить несанкционированный доступ к учетным записям пользователей. В частности, такие временные задержки служат для защиты от атак методом «грубой силы».

Атака методом «грубой силы» - это использование *скрипта* (т.е. компьютерной программы) или *робота* для угадывания (методом проб и ошибок) учетных данных пользователя т.е. имени пользователя и/или пароля/кода доступа. При атаках «грубой силой» используются, среди прочего, общие пароли или взломанные учетные данные для входа в систему. В 2018 году было обнаружено, что функцию мастер-пароля, которая позволяла пользователям шифровать пароли, хранящиеся в браузере Mozilla Firefox (веб-браузер), можно легко взломать с использованием атаки методом «грубой силы».

Пароли либо генерируются системой, либо создаются пользователем. *Пароли, генерируемые системой* (т.е. пароли, созданные программой), являются трудноугадываемыми и могут выдержать атаки парольных взломщиков, хотя это зависит от длины паролей. Проблема, связанная с паролями, генерируемыми системой, заключается в сложности их запоминания. Это приводит к тому, что пользователи записывают пароль, например, на бумагу или сохраняют его в браузере, приложении или цифровом устройстве. Поэтому *пароли, создаваемые пользователем*, являются более предпочтительными. Однако такие пароли, генерируемые пользователем, также могут быть трудными для запоминания. Системы, приложения и онлайн-платформы зачастую устанавливают сложные правила создания паролей, которым должны следовать пользователи, требуя, чтобы пароли соответствовали минимальной установленной длине и включали комбинации букв верхнего и нижнего регистра, цифр и символов. Таким образом, как и пароли, генерируемые системой, большинство паролей, создаваемых пользователями, являются трудно запоминаемыми.

Пользователям также рекомендуется иметь разные пароли для каждой учетной записи. Цель этой рекомендации заключается в минимизации ущерба, причиняемого пользователям, в случае взлома данных для доступа к одной из их учетных записей. В 2017 году одна исследовательская компания обнаружила в Интернете файл с 1,4 миллиардами имен пользователей и паролей для различных социальных сетей, игр, сайтов трансляции телепередач и фильмов и других сайтов сети Интернет. Если кто-либо из этих лиц повторно использует пароли, такие действия в системе защиты ставят под угрозу безопасность других учетных записей в Интернете (где используются те же имя пользователя и пароль). Хотя использование разных и сложных паролей для каждой учетной записи может обеспечить определенный уровень безопасности для отдельных пользователей, это в конечном итоге отрицательно влияет на удобство их использования.

5. Ситуационное предупреждение преступности.

Ситуационное предупреждение преступности (СПП) сосредоточено на способах предотвращения преступлений и сокращения возможностей для их совершения. СПП считается важной частью Руководства Экономического и Социального Совета ООН (ЭКОСОС) по предупреждению преступности.

Хотя концепция СПП применяется к предупреждению преступности в реальном мире, она также может использоваться в качестве меры предотвращения киберпреступности в контексте практики обеспечения кибербезопасности. Применительно к киберпреступности меры СПП направлены на сокращение или предотвращение возможностей для совершения правонарушений и подрыв способностей киберпреступников совершать преступления. Технические меры предупреждения киберпреступности представляют собой одну из форм ситуационного предупреждения преступности. Примеры таких технических мер включают в себя программы обнаружения вредоносных программ, *брандмауэры*, которые предотвращают несанкционированный доступ путем проверки и

блокирования трафика, и *системы обнаружения вторжений*, которые позволяют обнаруживать кибератаки, несанкционированный доступ и несанкционированное использование систем, сетей, данных, услуг и соответствующих ресурсов.

Корниш и Кларк (Cornish and Clarke, 2003) предложили стратегии и методы предотвращения и сокращения преступности. Пять предлагаемых стратегий предупреждения или сокращения преступности включают в себя: увеличение затрачиваемых усилий (со стороны преступника) для совершения преступления; увеличение рисков обнаружения и задержания; сокращение ожидаемой награды за совершение преступления; снижение числа провокаций, ведущих к совершению преступления; и устранение оправданий для совершения преступления. Не все стратегии и методы, перечисленные в рамках этих стратегий, применимы ко всем видам преступлений (Clarke, 2004). Более того, методы и стратегии могут частично совпадать, а некоторые методы могут использоваться сразу в нескольких стратегиях.

Меры СПП могут применяться, применялись ранее и применяются в настоящее время для предупреждения и сокращения киберпреступности (Maras, 2016). Например, один из методов, перечисленных в предложенной Корнишем и Кларком (Cornish and Clarke, 2003) стратегии СПП, - увеличение рисков обнаружения и задержания - заключается в «использовании управляющих на местах». Применительно к киберпреступности, управляющими на местах, которые контролируют поведение в обозначенном месте, могут быть поставщики Интернет-услуг или администраторы и модераторы онлайн-платформ. Управляющие на местах используются для борьбы с киберпреступностью в социальных сетях. Например, Facebook увеличил количество модераторов и усилил мониторинг контента, пропагандирующего насилие и жестокость, после того, как Стивен Стивенс (Steven Stephens) убил человека и транслировал это убийство через FacebookLive. Некоторые из этих методов СПП, применяемые для борьбы с киберпреступностью, могут нарушать права человека (например, при блокировании или удалении контента).

Вытеснение преступности происходит в случае, когда преступление, которое было нацелено на один объект, совершается в отношении другого объекта из-за действующих мер безопасности. Вопреки широко распространенному мнению, исследования в первую очередь показывают, что ситуационное предупреждение преступности необязательно ведет к вытеснению преступности. Исследование использования сутенерами Интернет-сайтов частных объявлений Backpage и Craigslist показало, что усилия правоохранительных органов, связанные с этими Интернет-сайтами, не вытеснили сутенеров с этих сайтов, которые продолжили использовать их для рекламы сексуальных услуг.

Меры СПП сосредоточены на возможности материализации угроз кибербезопасности в определенный момент времени. Таким образом, эти меры применяются на основании предположения о том, что угрозы *будут* материализованы, и поэтому необходимо предпринять

соответствующие действия. В то время как меры СПП преимущественно (но не исключительно) направлены на препятствование совершению преступлений, реальность такова, что даже после принятия этих мер преступление, вероятней всего, будет совершено. В связи с существованием такой вероятности реализуются меры, направленные на обнаружение инцидентов в области кибербезопасности, реагирование на них и восстановление после них.

Вопросы для обсуждения:

1. Что является целью оценки рисков?
2. Какие области к контроля информационной безопасности включает в себя Стандарт ISO/IEC 27002?
3. Охарактеризуйте меры обеспечения кибербезопасности и в чём удобство их использования?

Тема 10. Конфиденциальность и защита данных.

1. Неприкосновенность частной жизни: понятие и важность.

Неприкосновенность частной жизни является одним из основных прав человека. Право на неприкосновенность частной жизни является абсолютным императивом для отдельных лиц и закреплено в международных договорах в области прав человека, например, в статье 8 Европейской конвенции по правам человека 1950 года, статье 11 Американской конвенции о правах человека 1969 года, статье 12 Всеобщей декларации прав человека 1948 года и статье 17 Международного пакта о гражданских и политических правах 1966 года. Это право также признается в статье 16 Конвенции о правах ребенка 1989 года, статье 14 Международной конвенции и защите прав всех трудящихся-мигрантов и членов их семей 1990 года, статье 7 Хартии основных прав Европейского союза 2000 года и статье 22 Конвенции о правах инвалидов 2006 года. Существуют разные концепции неприкосновенности частной жизни, которые включают в себя: право на свободу от наблюдения; право быть оставленным в уединении; возможность хранить в тайне свои мысли, убеждения, личность и поведение; и право выбирать и контролировать, когда, какая, почему, где, как и кому раскрывается личная информация, и в какой степени она раскрывается. Последняя из перечисленных концепций неприкосновенности частной жизни, т.е. право выбирать и контролировать личную информацию, увязывает конфиденциальность с защитой информации или данных.

Право на неприкосновенность частной жизни обеспечивает возможность для осуществления других прав человека и тесно связано с этими правами. Неприкосновенность частной жизни является необходимым условием для осуществления прав на свободу выражения мнений, свободу мысли, вероисповедания, собраний и объединений. Право на неприкосновенность частной жизни также связано с правом на самоопределение. Статья 20(1) Африканской хартии прав человека 1981 года

гласит: «Все народы имеют право на существование. Им принадлежит несомненное и неотъемлемое право на самоопределение. Они свободно определяют свой политический статус и следуют в своем экономическом и социальном развитии политике, которую они свободно избирают». Важнейшим аспектом права на самоопределение является способность делать выбор и действовать по своему собственному выбору без принуждения (*личная автономия*). Этот выбор распространяется не только на физические действия, но и на действия в сети Интернет. Неотъемлемым аспектом частной жизни человека является личная автономия и право на самоопределение. Это право на самоопределение позволяет людям вести самобытную жизнь, иметь свободу выбора, а также выбирать и контролировать, какую информацию о себе сделать доступной для просмотра, раскрытия и обмена.

2. Конфиденциальность и безопасность.

Контроль и выбор в отношении раскрытия информации связаны с правом лица на свободу идентификации своей личности и своих действий по своему усмотрению и выбору и по собственному желанию. Следовательно, право на неприкосновенность частной жизни связано с правом не раскрывать свою личность. *Анонимность* позволяет пользователям заниматься деятельностью, не раскрывая себя или своих действий другим лицам (Maras, 2016). Благодаря анонимности в Интернете «у отдельных пользователей и групп в онлайновой среде появляется конфиденциальное пространство, в условиях которого они могут придерживаться тех или иных мнений и пользоваться свободой их выражения, не опасаясь произвольного и незаконного вмешательства или посягательств». Таким образом, конфиденциальность предоставляет пользователям информационно-коммуникационных технологий пространство, в котором они могут не опасаться запугивания, мести и других форм принуждения или санкций за выражение мыслей, мнений, взглядов и идей без необходимости идентифицировать свою личность. Соответственно, «технические средства обеспечения безопасности и защиты конфиденциальности электронных сообщений, в том числе меры по обеспечению анонимности, могут иметь важное значение для обеспечения осуществления прав человека, в частности прав на неприкосновенность частной жизни, свободное выражение мнений и свободу мирных собраний и ассоциации». В этой связи «государства не должны препятствовать использованию таких технических решений и должны обеспечивать, чтобы любые ограничения в отношении них соответствовали обязательствам государств по международному праву в области прав человека».

Существует мнение, что это право не раскрывать свою личность придает некоторым людям смелости адресовать другим людям грубые, дискриминационные, расистские, ненавистнические и оскорбительные высказывания, которые они бы никогда не позволили себе, если бы их личности были известны. Хотя это мнение справедливо в отношении некоторых лиц, встречаются и другие люди, которым раскрытие своей личности придает смелости, когда они распространяют такие высказывания.

Они раскрывают свою личность для того, чтобы быть узнанными единомышленниками и подтолкнуть своих сторонников к действиям. Майло Яннопулос, бывший главный редактор правового издания, специализирующегося на публикации сенсационных новостей (Breitbart), известен своими расистскими, женоненавистническими, анти иммигрантскими и антимусульманскими речами, а также тем, что распространял другие ненавистнические высказывания, чтобы завоевать популярность среди членов альтернативных правых и ультраправых движений со сходными взглядами или сторонников этих движений, и подталкивал других людей к подобным действиям в отношении лиц, являвшихся объектом его ненавистнических высказываний.

Задача установления личности человека и его местонахождения может оказаться трудновыполнимой из-за анонимности и использования технологий повышения конфиденциальности, таких как Tor. Еще одним примером *технологии повышения конфиденциальности* является шифрование. *Шифрование* блокирует доступ третьих лиц к информации и сообщениям пользователей. Правительства многих стран мира высказывались о необходимости обеспечения доступа к зашифрованным сообщениям и информации для борьбы с такими серьезными видами преступности, как терроризм, организованная преступность и сексуальная эксплуатация детей. Именно поэтому в некоторых странах службы обмена шифрованными сообщениями считаются незаконными.

Telegram, приложение для зашифрованных сообщений, которым пользуются более 200 миллионов человек, было заблокировано в судебном порядке в некоторых странах, потому что компания отказалась предоставить правительствам этих стран ключи дешифрования для отслеживания сообщений пользователей, отправляемых через это приложение. В некоторых странах было установлено обязательное требование о создании бэкдоров и предоставлении ключей для дешифровки, в то время как в других странах власти обратились к компаниям с просьбами о создании бэкдоров и предоставлении ключей для дешифровки для борьбы с серьезными преступлениями, такими как терроризм. Однако создание таких бэкдоров и предоставление ключей дешифрования могут привести к случаям злоупотребления доступом к данным (например, данные могут использоваться правительствами для непредвиденных целей, выходящих за рамки первоначального разрешения по какому-либо делу), а также случаям использования этих бэкдоров и ключей преступниками для получения доступа к информации с целью ее просмотра, копирования, удаления и изменения.

3. Киберпреступления, нарушающие конфиденциальность.

Киберпреступления нарушают право на неприкосновенность частной жизни людей и безопасность их персональных данных; к таким киберпреступлениям относятся, в частности, хакерские атаки, вредоносные программы, хищение персональных данных, финансовое мошенничество, медицинское мошенничество и некоторые преступления в отношении лиц, которые связаны с раскрытием личной информации, сообщений, изображений

и видео- и аудиозаписей без согласия или разрешения этих лиц.

Данные рассматриваются в качестве товара в сети Интернет и вне сети - как законно действующими, так и незаконно действующими субъектами (Maras, 2016). Именно поэтому данные являются основной целью киберпреступников. Данные также играют неотъемлемую роль в совершении многих киберпреступлений, прежде всего потому, что они не защищены должным образом и могут быть доступны для незаконного получения. Случаи утечки данных происходят в результате утери или кражи зашифрованных флеш-накопителей и других устройств хранения данных (в основном ноутбуков и смартфонов), низкого уровня безопасности систем и данных, несанкционированного доступа к базе данных или превышения санкционированного доступа к базе данных, а также случайного раскрытия, разглашения или публикации данных. Ниже приведены некоторые известные случаи утечки данных.

Национальная централизованная база персональных данных правительства Индии (Aadhaar), в которой хранятся биометрические данные (например, отпечатки пальцев и фотоснимки радужной оболочки) и идентификационные данные 1,2 миллиарда граждан Индии, и которая используется для проверки личности граждан при оказании финансовых, государственных, коммунальных и прочих услуг, в 2018 году столкнулась с проблемой утечки данных, в результате которой были скомпрометированы личные данные, такие как имена доступа, двенадцатизначный идентификационный номер, номера телефонов, адреса электронной почты и почтовые индексы, но не биометрические данные.

В 2017 году в сеть просочились данные приблизительно 30 миллионов жителей Южной Африки, включая сведения об их именах, половой принадлежности, доходе, истории трудоустройства, идентификационных номерах, номерах телефонов и домашних адресах, в результате утечки данных в одной из ведущих риэлторских компаний страны Jigsaw Holdings.

В 2013 году были скомпрометированы персональные данные более трех миллиардов пользователей Yahoo, включая их имена, адреса электронной почты, пароли (с шифрованием, которое можно было легко обойти) и даты рождения.

Deloitte, глобальная консалтинговая фирма, подверглась атаке хакеров, которые получили доступ через незащищенную учетную запись к данным об именах пользователей и паролях около 350 клиентов.

Персональные данные (т.е. национальный идентификатор, имя, пол, имена родителей, домашний адрес, дата рождения и город рождения) более 49 миллионов граждан Турции в 2016 году были выложены в сеть и стали доступными через базу данных с возможностью поиска.

В 2016 году на Филиппинах были скомпрометированы персональные и биометрические данные более 55 миллионов избирателей, после того как хакеры в «черной шляпе» получили несанкционированный доступ к веб-сайту избирательной комиссии (COMELEC).

Бремя обеспечения безопасности данных зачастую ложится на лиц,

данные которых похищаются. Эти люди информируются о необходимости минимизации своих «цифровых следов» путем обновления настроек системы безопасности приложений, веб-сайтов, социальных сетей и других онлайн-платформ, а также удаления и уменьшения объема личных данных, которыми они делятся с другими лицами (Maras, 2016). Такой подход, ориентированный на интересы потерпевшего, перекладывает ответственность за защиту данных на жертв киберпреступлений, а не на преступников и компании, чьи системы безопасности были повреждены. Реальность такова, что жертвы не могут защитить свои личные данные, когда они «хранятся в базах данных третьих лиц и похищаются из этих баз данных, которые находятся далеко за пределами их контроля» (Maras, 2016, p. 289). Кроме того, сегодня задача минимизации «цифровых следов» становится все более сложной. Практически не остается никаких альтернативных вариантов для людей, которые не желают, чтобы их данные собирались, анализировались или использовались. Например, лицо, пользующееся социальными сетями, выбирает один из двух возможных вариантов: либо предоставить минимальный объем требуемой личной информации для получения права на пользование платформой социальных сетей по сути, это «плата» за пользование услугой, либо отказаться от предоставления такой информации и не пользоваться платформой. Никаких других альтернативных вариантов не предлагается. Устройства, относящиеся к Интернету вещей, также требуют предоставления личной информации, чтобы получить возможность пользоваться ими. Все чаще можно наблюдать, что появляющиеся на рынке новые устройства, - даже те, которые никогда ранее не подключались к Интернету, такие как бытовая техника, ювелирные изделия, одежда и игрушки, - теперь имеют выход в Интернет, что оставляет потребителям все меньше вариантов, если они делают выбор в пользу приобретения устройства, не имеющего таких функциональных возможностей.

4. Законодательство о защите данных.

Защита персональных данных осуществляется в соответствии с правом на неприкосновенность частной жизни, предусмотренном в международных договорах в области прав человека. Например, Европейский суд по правам человека постановил, что данные, относящиеся к использованию телефона, электронной почты и Интернета (*Copland v. United Kingdom*, 2007 §§ 41-42), и данные, хранящиеся на компьютерных серверах (*Wieser and Bicos Beteiligungen GmbH v. Austria*, § 45), подпадают под сферу действия статьи 8(1) Европейской конвенции по правам человека. Само по себе хранение личных данных может рассматриваться как нарушение права пользователя на неприкосновенность частной жизни. Факт наличия нарушения зависит от контекста, в котором данные были получены, метода их сбора, обработки и использования, а также результатов, которые могут быть при этом получены. Базы данных, содержащие персональные данные, доступны для запросов, поиска, редактирования, обновления и просмотра местными и зарубежными государственными и частными организациями. Процедуры управления сбором, хранением, использованием информации и

обменом ею частными и государственными организациями варьируют в зависимости от конкретной страны. Пользователи имеют право на получение информации об обработке данных; право на доступ к обработанным данным; право на исправление обработанных данных; право на удаление данных («право на забвение»; субъект данных имеет право требовать удаления своих данных из журналов контролеров данных, а также не допускать дальнейшего использования и передачи персональных данных субъекта данных третьими лицами); право на возражение против обработки данных; право на ограничение обработки данных; право на переносимость данных (т.е. субъект данных имеет право получить свои персональные данные, которые он предоставил контролеру, и передать эти данные другому контролеру); и право на возражение против автоматизированного процесса принятия решения (например, формирование профиля).

В Руководстве по защите неприкосновенности частной жизни и трансграничной передаче персональных данных 2013 года изложены следующие принципы защиты данных и неприкосновенности частной жизни:

Принцип ограничения объема собираемых данных. Объем собираемых персональных данных должен иметь определенные пределы; все эти данные должны быть получены законным и честным образом - если возможно, то с ведома или согласия субъекта данных.

Принцип качества данных. Персональные данные должны соответствовать целям, в которых они будут использоваться; в той мере, в которой это необходимо в соответствии с упомянутыми целями, персональные данные должны быть точными, полными и регулярно обновляемыми;

Принцип конкретизации целей. Цели, в которых собираются персональные данные, должны быть конкретизированы не позднее момента сбора указанных данных, а их последующее использование должно ограничиваться достижением упомянутых либо сходных (совместимых) целей, которые должны указываться каждый раз, когда эти цели пересматриваются.

Принцип ограничения использования данных. Персональные данные не должны разглашаться, предоставляться в пользование или иным образом использоваться в иных целях, чем те, что перечислены в пункте 9, за исключением случаев, когда:

a) субъект данных дает на то свое согласие; либо

b) это разрешено законом.

Принцип защиты данных. Персональные данные должны быть обеспечены должными механизмами защиты от рисков, связанных с потерей, несанкционированным доступом, уничтожением, использованием, изменением или разглашением данных.

Принцип открытости. Должна существовать общая политика открытости в области практики и политик в отношении персональных данных. В постоянной готовности должны быть средства для установления факта наличия и характера персональных данных, основных целей их использования, а также личности и обычного местонахождения распорядителя

данных.

Принцип персонального участия. Каждый субъект данных (индивид) должен обладать следующими правами:

- получать от распорядителя данных, либо иным образом, подтверждения того, имеются ли у этого распорядителя данных персональные данные, относящиеся к упомянутому субъекту данных;

- получать относящиеся к нему/ней персональные данные в разумные сроки; в случае взимания платы - по тарифу, не являющемуся чрезмерным; в рамках разумной и необременительной процедуры; и в удобной для понимания форме;

- в случае отказа от удовлетворения заявки на предоставление информации, поданной в соответствии с пунктами (a) и (b), получать разъяснения о мотивах отказа и опротестовывать такой отказ; а также опротестовывать относящиеся к нему данные; в случае удовлетворения протеста требовать того, чтобы таковые данные были уничтожены, исправлены или дополнены.

Принцип подотчетности. Распорядитель данных должен нести ответственность за принятие мер, обеспечивающих соблюдение вышеперечисленных принципов.

Данные играют неотъемлемую роль в совершении многих киберпреступлений и возникновении факторов уязвимости к киберпреступности. Несмотря на то, что данные предоставляют пользователям (физическим лицам, частным компаниям, организациям и правительствам) бесчисленное множество возможностей, эти преимущества могут использоваться (и уже используются) некоторыми лицами в преступных целях. В частности, процессы сбора, хранения, анализа данных и обмена данными создают возможности как для совершения многих киберпреступлений, так и для сбора, хранения, использования и распространения огромного объема данных без информированного согласия и осознанного выбора пользователей, а также без необходимых средств правовой защиты и безопасности. Более того, агрегирование, анализ и передача данных происходят в масштабах, к которым правительства и организации не готовы, что создает большое количество рисков кибербезопасности. Понятия конфиденциальности, защиты данных и безопасности систем, сетей и данных являются взаимозависимыми. В связи с этим для обеспечения защиты от киберпреступности необходимы меры безопасности, предназначенные для защиты данных и конфиденциальности пользователей.

Задание для обсуждения:

На основе исследовании законодательств о защите данных определённых заранее стран выявите следующее:

1. Национальный закон (или законы) о защите данных.
2. Национальный орган по защите данных.
3. Учреждение или орган, ответственные за обеспечение соблюдения

национальных законов о защите данных.

4. Принципы сбора и обработки данных.

5. Правила, регулирующие передачу данных и уведомления об утечке данных.

6. Требования по обеспечению безопасности данных.

Тема 11. Преступления в сфере интеллектуальной собственности, совершаемые посредством кибертехнологий.

1. Интеллектуальная собственность.

Всемирная организация интеллектуальной собственности (ВОИС) дает следующее определение *интеллектуальной собственности:* «результат творения человеческого разума. К объектам ИС относятся изобретения, литературные и художественные произведения, символика, названия и изображения, используемые в коммерческих целях». Права на инновации, творения, оригинальное выражение идей и секретные методы и процессы ведения бизнеса охраняются национальным и международным законодательством об интеллектуальной собственности. В соответствии со статьей 2(8) Конвенции, учреждающей Всемирную организацию интеллектуальной собственности 1967 года (изменена в 1979 году), эти права относятся к литературным, художественным и научным произведениям, исполнительской деятельности артистов, звукозаписи, радио и телевизионным передачам, изобретениям во всех областях человеческой деятельности; научным открытиям; промышленным образцам; товарным знакам, знакам обслуживания, фирменным наименованиям и коммерческим обозначениям; защите против недобросовестной конкуренции, а также всем другим правам, относящимся к интеллектуальной деятельности в производственной, научной, литературной и художественной областях.

Доступ к интеллектуальной собственности, ее распространение и использование без предварительного разрешения или после истечения срока действия такого разрешения и в нарушение прав владельца или владельцев интеллектуальной собственности считается преступлением в сфере интеллектуальной собственности (также именуется *кражей интеллектуальной собственности*). Поскольку права интеллектуальной собственности признаются в качестве личных имущественных прав, преступления в сфере интеллектуальной собственности рассматривается как форма кражи личного имущества, даже если она не соответствует общепринятому представлению о краже, т.е. лишение владения. Например, если у человека похищены ювелирные изделия, он лишается своего (материального) имущества, поскольку он больше не имеет доступа к этим ювелирным изделиям. Однако в случае интеллектуальной собственности, даже если имущество «похищено», т.е. используется и потребляется без разрешения, владельца интеллектуальной собственности *не* лишают его собственности, поскольку она все еще находится в его владении. Все, чего он лишается - это контроль, управление и экономическая выгода, которая могла быть получена от последующего использования его интеллектуальной собственности. Лишение вознаграждения за труд т.е. за создание

интеллектуальной собственности служит отрицательным стимулом для создания объектов интеллектуальной собственности, которые имеют важнейшее значение для роста национальной экономики (ВОИС, 2009). В этой связи ВОИС «с помощью сбалансированной и эффективной системы интеллектуальной собственности способствует инновационной и творческой деятельности в интересах социально-экономического и культурного развития всех стран».

В целях защиты прав интеллектуальной собственности были введены в действие несколько международных конвенций, соглашений и договоров (далее - договоры). Примером может служить Бернская конвенция по охране литературных и художественных произведений 1886 года (с поправками, внесенными в 1979 году), в которой устанавливается обязательство государств по защите интеллектуальной собственности и определяются минимальные стандарты защиты интеллектуальной собственности. В связи с обеспокоенностью по поводу обеспечения соблюдения Бернской конвенции, Всемирная торговая организация (ВТО) приняла Соглашение по торговым аспектам прав интеллектуальной собственности (ТРИПС) 1994 года (которое вступило в силу в 1995 году). Соглашение ТРИПС требует, чтобы страны-члены ВТО выполняли свои обязательства, принятые в рамках Бернской конвенции и других договоров. Всемирная торговая организация осуществляет надзор за исполнением Соглашения ТРИПС и, среди прочего, устанавливает стандарты для политики, законов, положений, касающихся интеллектуальной собственности, а также механизмов контроля за выполнением обязательств по защите прав интеллектуальной собственности.

2. Виды интеллектуальной собственности.

Интеллектуальная собственность включает в себя авторские права, товарные знаки, патенты и промышленные секреты.

Авторские права. *Авторские права* включают в себя права на «литературные и художественные произведения», которые определяются в статье 2(1) *Бернской конвенции* по охране литературных и художественных произведений 1886 года следующим образом:

Термин «литературные и художественные произведения» охватывает все произведения в области литературы, науки и искусства, каким бы способом и в какой бы форме они ни были выражены, как-то: книги, брошюры и другие письменные произведения; лекции, обращения, проповеди и другие подобного рода произведения; драматические и музыкально-драматические произведения; хореографические произведения и пантомимы; музыкальные сочинения с текстом или без текста; кинематографические произведения, к которым приравниваются произведения, выраженные способом, аналогичным кинематографии; рисунки, произведения живописи, архитектуры, скульптуры, графики и литографии; фотографические произведения, к которым приравниваются произведения, выраженные способом, аналогичным фотографии; произведения прикладного искусства; иллюстрации, географические карты, планы, эскизы и пластические произведения, относящиеся к географии, топографии, архитектуре или наукам. Нарушение

авторских прав в Интернете именуется *цифровым пиратством*, которое предполагает выкладывание, передачу, загрузку произведений, охраняемых авторским правом, и обмен ими (например, книг, музыки и фильмов) без получения предусмотренного законом разрешения на доступ, использование и распространение. В качестве примера можно привести Napster, онлайн-платформу, которая обеспечила возможность для незаконного распространения музыки через систему обмена файлами одноранговых сетей. *Товарные знаки* - это идентификаторы, которые позволяют отличать товары или услуги одних источников от других (Maras, 2016). Таким источником может быть предприятие, физическое лицо либо географическое местоположение. Товарные знаки могут включать в себя, в числе прочего, логотипы, символы, рисунки, названия и слоганы, которые являются составной частью товаров, услуг и брендов и дают возможность отличать их между собой. Идентификаторы, из которых состоят товарные знаки, приобретают ценность благодаря труду, деньгам, знаниям и навыкам владельцев товарных знаков. Такая приобретенная ценность основана на характеристиках, качестве или надежности товара или услуги. Товарные знаки защищают их владельцев от практики недобросовестной конкуренции, цель которой заключается в попытке получить выгоду от инвестиций владельца товарного знака в разработку или распространение товара или услуги. Товарные знаки также защищают потребителей, помогая им распознавать источник товара или услуги.

Географические указания (или *наименования мест происхождения*) также являются охраняемой формой интеллектуальной собственности. Географические указания, которые «обычно используются в отношении сельскохозяйственной продукции, продуктов питания, вин и крепких спиртных напитков, ремесленных и промышленных изделий», нельзя использовать, кроме случаев, когда продукт был разработан в этом регионе в соответствии с общепринятой стандартной практикой.

Подделка товарных знаков (когда товар или услуга маркирован(а) товарным знаком его законного владельца, но не является настоящим товаром или услугой законного владельца товарного знака) является общемировой глобальной проблемой, и высказываются опасения по поводу того, что такая форма контрафакции финансирует организованную преступность. Товары с поддельными товарными знаками включают в себя ювелирные изделия, аксессуары, одежду, обувь, электронику, игрушки, бытовую технику, производственные детали, продукты питания и напитки (алкогольные и безалкогольные), косметику и средства личной гигиены, лекарственные препараты и т.д. Эти контрафактные товары вызывают серьезные проблемы для здоровья, безопасности, охраны труда и окружающей среды (UNODC, 2014). Продукция с поддельными товарными знаками покупается и продается в личном порядке и через Интернет (Maras, 2016). Даже логотипы, упаковку и другие идентифицирующие промышленные образцы контрафактных товаров можно приобрести в Интернете и вне сети.

Патент - это право на новые и уникальные творения, новаторские

разработки и изобретения, зарегистрированные в органе исполнительной власти, которое может обеспечить их охрану на национальном и/или международном уровне. Патенты позволяют запрещать использование и эксплуатацию новшеств без разрешения (т.е. явно выраженного согласия или одобрения) владельца патента. Патенты на образцы (или *промышленные образцы*) также являются охраняемой формой интеллектуальной собственности. Промышленные образцы считаются одной из форм интеллектуальной собственности, поскольку эти образцы создаются с конкретной целью быть эстетически привлекательными для потребителей и влияют на выбор потребителей между товарами. Следовательно, промышленные образцы влияют на конкурентоспособность и коммерческую ценность товара.

Промышленные секреты представляют собой ценную информацию о бизнес-процессах и деловой практике, которые являются секретными и защищают конкурентные преимущества компании (Maras, 2016). Промышленные секреты могут включать в себя секретные стратегии, методы, процессы и формулы, которые позволяют предприятиям сохранять конкурентное преимущество, такие как любые типы финансовой, деловой, - научной, технической, экономической и инженерной информации, включая информацию об устройстве, планах, наборе данных, программных устройствах, формулах, дизайнах, прототипах, методах, технологиях, - процессах, процедурах, программах или кодах - как осязаемую, так и неосязаемую - независимо от того, как они хранятся, систематизированы ли они или сохранены ли они физически, в электронном виде, графически, на фотографии или письменно (см. параграф 1839(3) титула 18 Свода законов США). В отличие от других форм интеллектуальной собственности, «промышленные секреты охраняются без регистрации» (т.е. «без какой-либо формальной процедуры») и, таким образом, могут «охраняться неограниченный период времени».

3. Причины, основания и предполагаемые мотивы правонарушений, касающихся авторских прав и товарных знаков, совершаемых посредством кибертехнологий.

В качестве возможных объяснений преступлений в сфере интеллектуальной собственности, совершаемых посредством кибертехнологий, предлагаются различные криминологические, социологические, психологические и экономические теории (для получения информации о применении этих и других теорий к преступлениям в сфере интеллектуальной собственности, совершаемым посредством кибертехнологий, см. Maras, 2016). Одни исследования показывают, что на показатели преступности, связанной с цифровым пиратством, влияют социокультурные нормы, групповое поведение и групповая динамика. Результаты других исследований свидетельствуют о том, что цифровое пиратство является поведением, перенятым от других.

Считается, что личностные качества, такие как самообладание, «влияют на вероятность того, что человек будет вовлечен в незаконную деятельность,

а также на частоту и масштабы занятия им такой незаконной деятельностью» (Maras, 2016, p. 160). Исследования показали, что низкий уровень самообладания (в частности, потребность в получении сиюминутного удовольствия), а также стрессы, с которыми сталкиваются люди (например, неспособность заплатить деньги за произведения, охраняемые авторским правом, или получить к ним доступ). Однако результаты исследований связей между стрессом, самообладанием и цифровым пиратством неоднозначны. В других исследованиях были обнаружены лишь слабые или незначительные подтверждения связи между стрессом и цифровым пиратством и между самообладанием и цифровым пиратством. Было также установлено, что исполнители преступлений в сфере интеллектуальной собственности, совершаемых посредством кибертехнологий, используют определенные методы (*технику нейтрализации*), чтобы «преодолеть чувства угрызения совести или вины за поведение, противоречащее общепринятым нормам, ценностям и убеждениям общества», и «временно освободить себя от общепринятых ограничений путем оправдания или обоснования своего незаконного поведения» (Maras, 2016, p. 152).

Используемые виды техники нейтрализации (*отрицание ответственности*; *отрицание жертвы*; *отрицание вреда*; *осуждение осуждающих;* и *обращение к высшим ценностям*) в сфере цифрового пиратства бывают разными. Еще одно исследование показало, что цифровая асимметрия (например, отсутствие непосредственного контроля за действиями в Интернете) может способствовать постепенному отклонению людей в цифровое девиантное поведение и получению ими доступа к информации/ресурсам, которые поддерживают или стандартизируют противозаконные действия, такие как пиратство.

4. Усилия по защите и профилактике.

Предлагаемые решения проблемы преступлений в сфере интеллектуальной собственности, совершаемых посредством кибертехнологий, включают в себя меры уголовно-правового характера, технические решения по ограничению несанкционированного доступа к объектам интеллектуальной собственности и просветительские кампании. Меры профилактики, принимаемые в области уголовного правосудия, включают в себя: мониторинг Интернет-сайтов, на которых публикуются произведения, охраняемые авторским правом; тайные расследования в отношении лиц, вовлеченных в различные формы преступлений в сфере интеллектуальной собственности, совершаемых посредством кибертехнологий (например, *Операция Fastlink*, в которой участвовали многочисленные агентства США, проводившие несколько тайных операций одновременно для идентификации и, в конечном итоге, ареста лиц, ответственных за незаконное распространение в Интернете охраняемых авторским правом произведений, таких как игры, программное обеспечение, музыка, фильмы; Department of Justice, 2004); закрытие сайтов, которые заведомо распространяют объекты интеллектуальной собственности (например, Megaupload); и судебное преследование лиц, вовлеченных в

преступления в сфере интеллектуальной собственности, совершаемые посредством кибертехнологий (например, участников и администраторов онлайн-платформ, на которых размещаются произведения, охраняемые авторским правом). Более того, такие компании, как Canada Goose и Chanel, которые стали жертвами преступлений в сфере интеллектуальной собственности, совершаемых посредством кибертехнологий, подали в суд на торговые площадки в Интернете в связи с нарушением прав на товарные знаки за продажу контрафактных версий своих товаров.

Меры уголовного наказания также активно применяются как способ демонстрации того, что нарушения прав интеллектуальной собственности являются серьезными и караются в соответствии с действующим законодательством. Наказания за преступления в сфере интеллектуальной собственности, совершаемые посредством кибертехнологий, назначаются в целях сдерживания. Для того чтобы такое средство *сдерживания* было эффективным, меры наказания должны быть: *суровыми* (т.е. вред от наказания должен перевешивать выгоды от преступления); *определенными* (т.е. лицо, которое совершает преступление, должно наказываться за совершение этого преступления); и *безотлагательными* (т.е. лицо наказывается вскоре после совершения преступления) (Maras, 2016). Меры уголовного наказания за нарушение прав интеллектуальной собственности ориентированы на *конкретное сдерживание* (т.е. лицо, понесшее наказание, прекращает дальнейшие противоправные действия, если полученное наказание перевешивает выгоды от совершения преступления), и *общее сдерживание* (т.е. посылают сигнал всем остальным, что схожее поведение повлечет за собой схожее суровое наказание). Однако сегодняшний характер Интернета серьезно ограничивает практическую осуществимость сдерживания, поскольку масштаб и частота случаев пиратства значительно превосходят возможности принятия каких-либо ответных мер противодействия.

Используя Интернет и другие цифровые технологии, любой человек может получить доступ к охраняемому контенту, мгновенно переиздать и повторно распространить его по всему миру. В качестве решений проблемы преступлений в сфере интеллектуальной собственности, совершаемых посредством кибертехнологий, предлагаются меры в области уголовного правосудия, технологические решения по ограничению несанкционированного доступа к интеллектуальной собственности и информационно-просветительские кампании. Несмотря на принимаемые на национальном, региональном и международном уровнях меры нормативно-правового характера, простота, легкость и дешевизна тиражирования, хранения, распространения и/или иного способа обеспечения доступности объектов интеллектуальной собственности делают усилия по расследованию этих киберпреступлений, их предотвращению и преследованию лиц, виновных в их совершении, весьма затруднительными для соответствующих органов и учреждений во всем мире.

Вопросы для обсуждения:

1. Что является интеллектуальной собственностью**?**

2. Какие виды деятельности и услуги входят в систему интеллектуальной собственности?

3. Что является причиной, основанием и предполагаемым мотивом правонарушений, касающихся авторских прав и товарных знаков, совершаемых посредством кибертехнологий**?**

Тема 12. Киберпреступления против личности.

1. Сексуальная эксплуатация детей и сексуальное насилие над детьми в Интернете

Сексуальная эксплуатация детей и сексуальное насилие над детьми в Интернете предполагают использование информационно-коммуникационных технологий в качестве *средства* для сексуального насилия над детьми и/или сексуальной эксплуатации детей. Экономическая и социальная комиссия Организации Объединенных Наций для Азии и Тихого океана (ЭСКАТО ООН) определяет сексуальное насилие над ребенком «как контакты или взаимодействия между ребенком и более старшим по возрасту или более осведомленным ребенком или взрослым (незнакомцем, братом, сестрой, родителем или опекуном), при которых ребенок используется как предмет удовлетворения сексуальных потребностей более старшего по возрасту ребенка или взрослого. Такие действия в отношении ребенка производятся с использованием силы, хитрости, взяток, угроз или давления». *Сексуальная эксплуатация детей* подразумевает сексуальное насилие над детьми или другие сексуализированные действия с использованием детей, которые предполагают обмен на удовлетворение каких-либо потребностей (например, в заботе, еде, наркотиках, убежище). Лица, совершающие такое преступление, злоупотребляют или покушаются на злоупотребление «уязвимым положением, властью или доверием в сексуальных целях» для приобретения денежной или иной выгоды (например, сексуального удовлетворения). На самом деле, зачастую трудно провести различие между сексуальным насилием над детьми и сексуальной эксплуатацией детей, потому что «у них имеется очень много общего». В статье 1 Конвенции о правах ребенка 1989 года ребенок определяется как «каждое человеческое существо до достижения 18-летнего возраста, если по закону, применимому к данному ребенку, он не достигает совершеннолетия ранее». Минимальные возрастные пороги варьируют в зависимости от конкретного государства. Эти различия могут препятствовать осуществлению трансграничного сотрудничества при расследовании случаев сексуальной эксплуатации детей и сексуального насилия над детьми.

Виды сексуальной эксплуатации детей и сексуального насилия над детьми в Интернете.

В то время как сексуальная эксплуатация детей и сексуальное насилие над детьми в Интернете запрещены национальным, региональным и

международным законодательством и представляют собой серьезную форму насилия в отношении детей, в разных правовых инструментах предусмотрены разные виды преступлений, которые считаются сексуальной эксплуатацией детей и сексуальным насилием над детьми. Примерами преступлений, запрещенных законодательством (в той или иной степени), являются груминг в Интернете, размещение материалов с изображением сексуального насилия над детьми/материалов с изображением сексуальной эксплуатации детей и прямая трансляция сексуального насилия над детьми.

Груминг с участием детей также известный как соблазнение детей или домогательство в отношении детей с сексуальными целями можно описать как практику, при помощи которой взрослый знакомится с ребенком (зачастую в Интернете, однако груминг вне сети Интернета также существует, и не должен оставаться без внимания) с намерением совершить над ним/ней сексуальное насилие. Исследования и имеющиеся данные показывают, что преступления в форме груминга преимущественно совершают мужчины; в меньших масштабах домогательство в отношении детей с сексуальными целями и груминг совершают женщины.

В типичных случаях процесс груминга происходит поэтапно, начиная с этапа выбора жертвы. В Интернете дети являются участниками различных социальных сетей и коммуникационных приложений, которые преступники могут использовать для получения доступа к учетным записям детей. Преступники выбирают жертву на основании «привлекательности/притягательности» жертвы определяется желаниями преступников, «легкости доступа» (например, в зависимости от того, отключены ли настройки конфиденциальности на веб-сайтах, платформах и в приложениях, используемых детьми, или установлены ли они ненадлежащим образом) и «уязвимостей» (например, дети размещают сообщение о своем одиночестве или чувстве непонимания). После выбора жертвы преступник связывается с жертвой, чтобы получить к ней доступ. Затем преступник пытается завязать с жертвой дружбу. Преступник может по крупицам собирать информацию о жертве из источников в сети и использовать эту информацию, чтобы обмануть жертву, например, притворяясь, что он имеет с ней общие интересы и увлечения, находится в схожей ситуации в семье и обществе, чтобы сойтись с жертвой, достичь взаимопонимания и вызвать у нее доверие. Цель преступника заключается в дальнейшем развитии дружеских отношений. Прежде чем перейти к сексуальной эксплуатации или насилию преступник оценивает риск быть обнаруженным (например, спрашивает жертву, контролируют ли родители или другие лица учетные записи и/или цифровые устройства ребенка), сообщает об исключительности их отношений и необходимости держать эти отношения в тайне и изолирует ребенка. Однако преступники вполне могут использовать иные подходы.

Под *детской порнографией* понимается «изображение, какими бы то ни было средствами, ребенка, совершающего реальные или смоделированные откровенно сексуальные действия, или любое изображение половых органов ребенка главным образом в сексуальных целях».

Прямая трансляция сексуального насилия над детьми предполагает трансляцию сцен сексуального насилия над детьми в режиме реального времени удаленным пользователям. Хотя прямая трансляция сексуального насилия над детьми зачастую предполагает передачу видеосигнала за пределы национальных границ через Интернет, важно отметить, что некоторые страны сообщают о случаях прямой трансляции сцен сексуального насилия над детьми зрителям внутри страны.

Прямая трансляция сексуального насилия над детьми осуществляется в Интернет-чатах, социальных сетях и коммуникационных приложениях (с функциями видеочата). Зрители прямой трансляции сексуального насилия над ребенком могут быть пассивными (т.е. оплачивать просмотр) или активными, общаясь с ребенком, сексуальным насильником и/или организатором сексуального насилия над ребенком и требуя совершения конкретных физических действий (например, удушения) и/или половых актов с ребенком и/или в отношении ребенка. Активное участие со стороны зрителя называется *сексуальным насилием над детьми на заказ*, причем заказ может делаться до или во время прямой трансляции сексуального насилия над детьми. Иан Уоткинс, скандально известный вокалист группы Lostprophets, был признан виновным в совершении преступления, связанного с сексуальным насилием над детьми, в том числе за то, что во время общения по Skype он побуждал женщину к сексуальному насилию над ее ребенком. Этот случай наглядно демонстрирует, что прямая трансляция сексуального насилия над детьми осуществляется не только за плату, но и для ублажения любовников или сексуальных партнеров и/или для удовлетворения желаний сексуальных насильников и зрителей, и/или в контексте иных насильственных отношений (например, когда насильник может реагировать на указания человека, со стороны которого он также подвергается насилию).

2. Киберпреследование и кибердомогательство.

Киберпреследование предполагает использование информационно-коммуникационных технологий (ИКТ) для совершения неоднократных действий с целью домогательства, беспокойства, нападок, угроз, запугивания и/или словесного оскорбления отдельных лиц на систематической основе (UNODC, 2015; Maras, 2016). Преступники могут осуществлять киберпреследование напрямую посредством электронной почты, мгновенных сообщений, звонков, текстовых сообщений или иных форм электронной коммуникации для передачи непристойных, вульгарных и/или оскорбляющих достоинство высказываний и/или угроз жертве и/или семье, партнерам и друзьям жертвы, и использовать технологии для мониторинга, наблюдения и отслеживания передвижений жертвы (например, путем тайной установки устройств GPS-слежения в автомобили, сумки и даже детские игрушки). Преступники могут также осуществлять киберпреследование косвенным образом посредством причинения ущерба цифровому устройству жертвы (например, путем заражения компьютера жертвы вредоносной программой и использования этой программы для тайного мониторинга за жертвой или кражи информации о жертве) или размещения ложной, порочащей или

оскорбительной информации о жертве в Интернете, или создания поддельной учетной записи на имя жертвы для размещения материалов в Интернете (социальных сетях, чатах, дискуссионных форумах, веб-сайтах и т. д.).

Киберпреследование подразумевает серию поступков и действий в течение некоторого периода времени, цель которых заключается в том, чтобы запугать, встревожить, устрашить или домогаться жертвы и/или семьи, партнера и друзей жертвы. Такие поступки и действия включают в себя (среди прочего): заполнение почтового ящика пользователя электронными письмами; частое размещение сообщений на сайтах, страницах и учетных записях пользователя в социальных сетях; многократные звонки или отправка текстовых сообщений жертве; оставление голосовых сообщений и отправка запросов на подписку и добавление в друзья; присоединение ко всем группам и сообществам в сети, участником которых является жертва, или подписка на публикации жертвы через учетные записи знакомых, коллег, одноклассников, членов семьи или друзей в социальных сетях; и непрерывный просмотр страницы жертвы, некоторые веб-сайты регистрируют эту информацию и сообщают пользователю, когда его страница просматривается. Преступники могут непрерывно приглядывать, наблюдать за жертвами и следить за ними с их ведома или без их ведома в Интернет пространстве или в пространстве вне сети Интернет. Поступки и действия киберпреследователей заставляют жертв опасаться за свою безопасность и благополучие, и, в зависимости от действий киберпреследователя, такой страх может распространяться на безопасность и благополучие семей, партнеров и друзей жертв.

Кибердомогательство предполагает использование ИКТ для преднамеренных действий с целью унижения, раздражения, нападок, угроз, запугивания, нанесения обиды или оскорбления (Maras, 2016). Для признания факта совершения киберпреступления достаточно одного лишь инцидента; однако такое киберпреступление может включать в себя несколько инцидентов. Кибердомогательство может также предполагать целенаправленное домогательство, когда один или несколько человек объединяют усилия для многократного домогательства к своей жертве в Интернете в течение ограниченного периода времени (зачастую короткого периода времени), чтобы причинить жертве страдания, унизить ее и/или заставить ее замолчать. Кибердомогательство может также предполагать размещение или распространение иным способом ложной информации или слухов о человеке, чтобы причинить ущерб его социальному положению, межличностным отношениям или репутации, это одна из форм *киберклеветы*. Такая ложная информация размещается на веб-сайтах, в чатах, дискуссионных форумах, социальных сетях и прочих Интернет-сайтах, чтобы опорочить репутацию людей и компаний. Преступники могут также выдавать себя за жертв путем создания учетных записей со схожими именами, размещая на них существующие фотографии жертв, и использовать эти учетные записи для отправки запросов на добавление в друзья или подписку друзьям и членам семьи жертв, чтобы обманным путем вынудить их принять эти запросы, это одна из форм *персонации в сети*. Принятие этих запросов обеспечивает

преступникам доступ к учетным записям друзей и членов семей жертв и, соответственно, доступ к реальным учетным записям жертв.

3. Кибертравля. Дети, которые занимаются кибертравлей, используют текстовые сообщения, электронные письма, веб-сайты, блоги, опросы, сообщения в социальных сетях, мгновенные сообщения, игровые сайты и сайты виртуальной реальности с целью унижения, очернения, домогательства, оскорбления, распространения ложной информации, сплетен и слухов, угрозы и/или изолирования, вытеснения и маргинализации других детей. Как и в случае киберпреследования и кибердомогательства, существует два типа кибертравли: прямая кибертравля (т.е. лицо, осуществляющее кибертравлю, совершает прямые нападки на жертву) и кибертравля чужими руками (т.е. другие лица осознанно или неосознанно оказывают содействие в кибертравле жертвы) (Maras, 2014). Лица, осуществляющие кибертравлю, или другие лица, оказывающие им содействие, могут опубликовать персональную информацию о жертве, такую как домашний адрес и номер телефона, в открытом доступе (это одна из форм доксинга). Эта информация может использоваться для дальнейшей виктимизации объекта кибертравли. Опубликование адреса жертвы также может привести к домогательствам, травле и преследованию в реальной жизни и может повлечь за собой причинение жертве физического вреда. В открытом доступе могут также размещаться имя пользователя, пароль и другие учетные данные жертвы. Размещение учетных данных жертвы в сети может повлечь за собой кражу личной информации жертвы, ее фотографий, видео, документов и прочих предметов, содержащихся в ее учетной записи, другими лицами. Эти учетные данные могут также использоваться для того, чтобы выдать себя за жертву и совершать действия (например, размещать непристойные и оскорбительные комментарии в адрес других лиц или публиковать какие-либо материалы, которые могут унизить жертву, такие как обнаженные фото жертвы или видео с изображением неуклюже танцующей жертвы), которые спровоцируют негативную реакцию других лиц (например, оскорбительные комментарии и высмеивание жертвы).

Сторонние наблюдатели играют важную роль в кибертравле; они преднамеренно или непреднамеренно помогают лицу, осуществляющему кибертравлю, путем нажатия на кнопку «мне нравится», вторичной публикации его сообщений или иным образом поддерживая кибертравлю, защищая жертву или не предпринимая никаких действий. Сторонние наблюдатели могут проявлять нежелание вмешиваться из-за *социальной дилеммы*, когда решения основываются скорее на личном интересе, а не на интересе группы или коллектива, даже когда практическая польза от действий в коллективных интересах выше, чем польза от преследования личного интереса. Исследование показало, что такое бездействие на благо коллектива вызвано недоверием и неуверенностью в том, что другие люди также предпримут действия в интересах коллектива и присоединятся к человеку в этих усилиях.

Масштаб использования ИКТ детьми во всем мире неуклонно растет, причем дети все более младшего возраста получают доступ к различным

видам цифровых технологий и Интернету и используют их (UNODC, 2015). В то время как ИКТ предоставляют детям возможность общаться с другими людьми, получать доступ к информации, делиться информацией, а также строить отношения, такие технологии также ставят под угрозу безопасность детей и делают их уязвимыми к киберпреступлениям, таким как кибертравля. *Кибертравля* предполагает использование детьми ИКТ «для досаждения, унижения, запугивания, оскорбления или иных нападок» в отношении других детей (Maras, 2016, p. 254). Таким образом, в отличие от киберпреследования и кибердомогательства, дети являются как исполнителями, так и жертвами этого киберпреступления.

Зачастую законы о кибертравле принимаются в качестве ответных действий, т.е. они внедряются после совершения самоубийства ребенка в результате кибертравли. Это можно наблюдать на примере Италии, где закон №71 от 29 мая 2017 года был принят после самоубийства жертвы, которая выпрыгнула из окна третьего этажа здания в результате непрекращающейся и масштабной кибертравли со стороны нескольких злоумышленников (Reuters, 2017). Однако страны обязаны защищать детей, и эта обязанность, наряду с обязательствами в отношении защиты прав детей, закреплена в Конвенции о правах ребенка. Статья 37(a) данной конвенции гласит, что ни один ребенок не должен подвергаться «пыткам или другим жестоким, бесчеловечным или унижающим достоинство видам обращения или наказания». Следовательно, кибертравля является явным нарушением Конвенции о правах ребенка. Кроме того, кибертравля нарушает и другие права ребенка, такие как право детей на свободу от дискриминации (статья 2), свободу выражать свое мнение (статья 13), неприкосновенность личной жизни (статья 16) и другие. В то время как в некоторых странах действуют национальные законы о кибертравле (например, Закон Японии о поощрении мер предотвращения издевательств 2013 года и Закон Италии №71 от 29 мая 2017 года), ответственными за принятие мер по защите благополучия учащихся считаются в первую очередь образовательные учреждения, которые должны защищать детей от издевательств (в том числе от кибертравли) и реагировать на инциденты, которые угрожают безопасности и благополучию детей. Национальные законы, такие как Закон Швеции «Об образовании» 2010 года (Закон 2010 года «Об образовании 800») и Закон Соединенного Королевства Великобритании и Северной Ирландии «О детях» 1989 года, определяют границы таких обязанностей. В Соединенном Королевстве Великобритании и Северной Ирландии школы обязаны иметь четкую политику, в которой первоочередное внимание уделяется обеспечению безопасности и благополучия детей и принятию мер по защите детей от угроз безопасности и здоровью (таких как кибертравля), предотвращению таких угроз и реагированию на них.

4. Профилактика киберпреступлений против личности.

Для борьбы с киберпреступлениями против личности предлагается использовать стратегии профилактики, ориентированные на потерпевших. Теория рутинной деятельности, предложенная Лоренсом Коэном (Lawrence Cohen) и Марком Фелсоном (Mark Felson) в 1979 году, гласит, что

преступление совершается в том случае, когда присутствуют два элемента - *мотивированный преступник* и *подходящая цель*, и когда отсутствует один элемент - *дееспособный защитник* (т.е. что-то или кто-то, способные сорвать попытки преступника совершить преступление).

Согласно теории рутинной деятельности, для предотвращения преступления необходимо изменить хотя бы один из основных элементов - отсутствие дееспособного защитника, мотивированный преступник или подходящая цель. Следовательно, для того чтобы сделать преступление менее привлекательным для преступников, предлагаются дееспособные защитники, в роли которых могут выступать люди (например, родители, братья и сестры, друзья, партнеры и другие) или решения по обеспечению безопасности (например, настройки конфиденциальности, родительский контроль, программное обеспечение для фильтрации или блокировки и т.п.). Теория утверждает, что меры самозащиты могут служить в качестве дееспособных защитников и подорвать попытки преступников приблизиться к жертве, связаться с ней или иным образом преследовать жертву.

Такие стратегии профилактики, ориентированные на потерпевших, позволяют жертвам предпринимать незамедлительные действия для предотвращения киберпреступлений против личности (по крайней мере, тем из них, кто обладает знаниями, навыками и способностями для этого) или, как минимум, для подрыва планов лиц, покушающихся на совершение таких киберпреступлений. Основная критика таких подходов состоит том, что они возлагают бремя профилактики киберпреступлений против личности на жертву, а не на учреждения, которые должны уберегать людей от неприятностей (Maras, 2016; Henry, Flynn and Powell, 2018).

Одно из наиболее серьезных препятствий для предотвращения насилия и надругательств связано со взглядами, убеждениями и ценностями. К сожалению, многие люди продолжают придерживаться взглядов, которые возлагают вину на жертв киберпреступлений против личности и преуменьшают ущерб, причиняемый этими киберпреступлениями. Например, в 2017 году в ходе австралийского исследования проблемы сексуального надругательства с использованием изображений выяснилось, что 70% респондентов согласны с тем, что «люди должны понимать, что в принципе нельзя фотографировать самих себя в голом виде, даже если они никому не отправляют эти фото», а 62% согласны с тем, что «если человек отправляет свою фотографию интимного или сексуального характера кому-то еще, он несет, как минимум, частичную ответственность, если эта фотография оказывается в сети» (Henry, Flynn and Powell, 2018). В целом, каждый второй мужчина (или 50%) и каждая третья женщина (или 30%) в исследовании Генри, Флинна и Пауэлла (Henry, Flynn and Powell, 2018) придерживались взглядов, которые либо преуменьшали ущерб, либо возлагали вину на жертв. Такие взгляды, возлагающие вину на жертв, являются спорными и преобладают не только среди преступников или потенциальных преступников, но и более того, когда лица, ставшие жертвами сексуального надругательства с использованием изображений, винят самих себя, они с

меньшей вероятностью сообщают о таких случаях или обращаются за помощью (Henry, Flynn and Powell, 2018). Если члены общества придерживаются таких взглядов, они могут нанести дополнительный вред лицам, раскрывающим информацию о том, что они стали жертвами этого преступления.

Проблемы киберпреступлений против личности с участием детей решаются во многих странах посредством родительского контроля и образовательных инициатив. Исследования показали, что родительский мониторинг доступа детей в Интернет, использования Интернета, а также количества времени, проводимого в сети, защищает детей от кибертравли. Однако родители могут не иметь возможности отслеживать действия детей в Интернете и/или принимать необходимые технологические решения (например, инструменты фильтрации для блокировки доступа к определенным сайтам) для контроля доступа в Интернет и активности в сети без помощи других лиц (например, школ, органов власти, служб защиты детей и родственников) (UNODC, 2015). Образовательные инициативы учат детей и родителей безопасному использованию Интернета и информируют их о кибертравле. Поскольку кибертравля совершается с участием обидчиков, жертв и сторонних наблюдателей, усилия по профилактике должны включать каждого из этих участников.

Задание для обсуждения:

Даниэль Сон Вунг Ли - южнокорейский музыкант, известный как Табло, который был женат на южнокорейской актрисе и имел многочисленных поклонников. До своей музыкальной карьеры Ли получил степень бакалавра и одну степень магистра в Стэнфордском университете. После скандалов с поддельными дипломами в Южной Корее (когда было установлено, что многие высокопоставленные частные и государственные деятели имеют поддельные дипломы об образования), анонимные граждане сформировали онлайн группы, чтобы поставить под сомнение дипломы Ли. Интернет-форум «Мы требуем правды от Табло» (TaJinYo) был крупнейшим из этих групп. Члены этой группы и другие пользователи Интернета осуществляли анонимные нападки на Ли в сети и подвергали его оскорблениям. Доказательства, которые подтверждали диплом Ли (даже из Стэнфордского университета), отклонялись как ложные доказательства, и представление таких доказательств считалось выгораживанием со стороны людей, которым платили за то, что они лгут от его имени. Любой, кто пытался его защищать, также назывался лжецом и сталкивался с рисками для своей репутации. По этой причине мало кто был готов публично поддержать Ли. Даже средства массовой информации в Южной Корее сообщали о претензиях, предъявляемых его хулителями в сети, без проверки фактов. Это еще больше усугубило проблему. Южнокорейские жители подвергали его словесным оскорблениям и открытым угрозам, ему угрожали физической расправой, к нему приставали на улице и даже отвергали и подвергали остракизму. Люди, осуществлявшие на него нападки, нацеливались даже на членов его семьи,

позоря их, подвергая сомнению их чистоплотность и угрожая их жизням. Киберпреступления, совершаемые против него, в значительной степени (но не полностью) прекратились после того, как он поехал в Калифорнию со съемочной группой и известным южнокорейским журналистом, чтобы снять видеоматериал о своей учебе в Стэнфордском университете, и чтобы его в*ыписка* из *зачетно-экзаменационной ведомости была подтверждена на камеру представителями* Стэнфордского университета.

Вопросы:

1. Какие киберпреступления были совершены против Табло? Почему вы так считаете?

2. Изменились ли бы ваши ответы на вышеуказанные вопросы, если бы вы были в другой стране? Ообоснуйте свой ответ.

Тема 13. Организованная киберпреступность.

Организованная киберпреступность: что это такое?

Многие преступления и киберпреступления совершаются при определенном уровне организации, то есть эти преступления и киберпреступления являются «запланированными и представляют собой рациональные действия, которые отражают усилия групп лиц».

Киберпространство и организация преступных групп.

Многие организованные преступные группы используют Интернет-технологии просто для того, чтобы общаться друг с другом и вести свои дела. Такие «дела» могут привести к созданию «эфемерных» форм организаций, в которых Интернет используется для объединения преступников с целью совершения преступлений офлайн, после чего они рассеиваются, чтобы сформировать новые альянсы. В качестве альтернативы, организованные преступные группы могут использовать сетевые технологии для создания более «устойчивых» форм организаций, которые просуществуют в течение длительного времени и обеспечат защиту преступникам, действующим под ее крылом, от других преступников, осуществляющих деятельность в той же области, а также от правоохранительных органов (Varese, 2010, p. 14). Между этими двумя крайними полюсами спектра существуют также «гибридные» формы организаций, в которых более широко признанная преступная цель активно распространяется небольшой основной группой «виртуально», но ее физическое воплощение осуществляется отдельными волками-одиночками или местными ячейками - как это происходит в случае некоторых хакерских групп или в ситуациях офлайн, когда устанавливается связь между преступностью и терроризмом. Важно отметить, что, хотя «сферы деятельности террористов и организованных преступных групп могут пересекаться», «они обычно преследуют разные цели». Большинство организованных преступных групп, как правило, существуют в спектре между эфемерными и устойчивыми формами организации с гибридной формой посередине и в той или иной степени используют Интернет-технологии для

самоорганизации.

Киберпространство и организация киберпреступлений.

Хотя почти все организованные преступные группы используют какую-либо сетевую технологию для самоорганизации и организации своих преступлений, некоторые из них используют эти технологии также и для совершения киберпреступлений. Фактический характер организации киберпреступлений варьируется в зависимости от уровня задействованных цифровых и сетевых технологий, образа действий и намеченных жертв, что также помогает определить различия между ними.

Уровень использования цифровых и сетевых технологий или трансформации преступного поведения.

Более традиционные организованные преступные группы, как правило, не участвуют в совершении киберзависимых преступлений, то есть преступлений, совершение которых невозможно в отсутствие Интернета. Однако они все чаще используют сетевые технологии для общения друг с другом с целью организации преступлений или поиска предполагаемых жертв, например, для продажи наркотиков через Интернет или даркнет. Эти виды киберпреступлений относятся либо к преступлениям, совершаемым с использованием кибертехнологий (обычно с использованием коммуникационных технологий), потому что без Интернета правонарушение все равно было бы совершено, но с помощью других средств коммуникации, либо к преступлениям, совершаемым посредством кибертехнологий, когда давно существующие (обычно локализованные) виды правонарушений, такие как незаконные азартные игры, мошенничество и вымогательство, приобретают глобальный охват благодаря цифровым и сетевым технологиям. Если убрать Интернет, то правонарушение потеряет глобальный масштаб и вновь приобретет локальную форму. Они резко контрастируют с «киберзависимыми» преступлениями, такими как хакерские атаки, распределенная атака типа «отказ в обслуживании» и атаки с использованием программ-вымогателей, а также спам, которые, как указано выше, исчезают при удалении Интернета из уравнения.

Киберпреступления также варьируют в зависимости от *modus operandi,* т.е. способа совершения правонарушения, который связан с мотивами и профилем преступников. Организация «киберпреступлений против машины», таких как, например, неправомерное использование компьютеров хакерами, весьма отличается от организации «киберпреступлений с использованием машины», таких как аферы, мошенничество и вымогательство. Эти два вида преступлений также весьма значительно отличаются от «киберпреступлений в машине», таких как распространение материалов с изображением сексуального надругательства над детьми, пропаганда ненависти, террористические материалы. Последним фактором, который необходимо учитывать при исследовании киберпреступности и ее организации, являются группы жертв, на которых нацелены преступники. Некоторые преступные группы преднамеренно нацеливаются на отдельных пользователей, например, путем массовой

рассылки вводящих в заблуждение электронных писем с целью мошенничества или обмана. Другие группы преднамеренно нацеливаются на коммерческие или правительственные организации с целью совершения мошенничества в более крупном масштабе, овладения коммерческой тайной или подрыва деловой активности (в целях вымогательства или по просьбе конкурента). Наконец, третьи группы, к которым обычно относятся государственные субъекты, преднамеренно нацеливаются на объекты инфраструктуры других государств, чтобы создать атмосферу недоверия или недовольства и/или причинить ущерб. Поэтому вопрос заключается не только в том, что способ организации преступников, использующих сетевые технологии, сильно отличается от того, как преступники организуют преступления в Интернете, но и в том, что характер организации преступлений в Интернете зависит от уровня используемых технологий, конкретных преступных действий, совершаемых преступниками, а также от намеченных жертв.

Результаты различных исследований показывают, что организованные преступные группы, действующие в офлайн-среде, являются полной противоположностью организованным преступным группам, осуществляющим свою деятельность в сети Интернет, и отличаются от них возрастом своих членов, мотивами, организацией и половым составом. Эти группы могут отличаться друг от друга не только своими участниками; их организация может быть децентрализованной - если не сказать беспорядочной - по сравнению с организованными преступными группами в среде офлайн.

2. Концептуализация организованной преступности и определение ее участников.

Вопрос о том, считаются ли те или иные киберпреступления разновидностью организованной преступности, или связаны ли они с организованной преступностью, зависит от рабочих определений, используемых для термина «организованная преступность» (УНП ООН, 2013, pp. 49-50). Конвенция Организации Объединенных Наций против транснациональной организованной преступности не содержит определения организованной преступности. Это связано не столько с отсутствием договоренности между государствами, сколько с сознательным выбором, сделанным участниками переговоров по Конвенции. Любое определение, скорее всего, включало бы в себя список осуществляемых организованными преступными группами незаконных действий, которые постоянно меняются и адаптируются к условиям нашего динамично развивающегося мира; поэтому любое такое определение быстро бы устаревало. Вместо того чтобы дать определение преступлению, Конвенция против организованной преступности определяет субъекта, участвующего в ее совершении: «организованную преступную группу». В частности, в соответствии со статьей 2 (a) Конвенции, «организованная преступная группа» означает «структурно оформленную группу в составе трех или более лиц, существующую в течение определенного периода времени и действующую согласованно с целью совершения одного или нескольких серьезных преступлений или преступлений, признанных

таковыми в соответствии с настоящей Конвенцией, с тем чтобы получить, прямо или косвенно, финансовую или иную материальную выгоду». Здесь в структурно оформленной группе «не обязательно формально определены роли ее членов или оговорен непрерывный характер членства». Это определение является широким и охватывает группы, которые не имеют между собой тесных связей, каких-либо формально определенных ролей или развитой структуры.

Хотя общепризнанного определения организованной преступности не существует ее можно определить, как «постоянно действующее преступное предприятие, рационально работающее для получения прибыли путем незаконной деятельности в сферах тех служб, на которые есть большой общественный спрос. Продолжительное существование организованной преступности поддерживается при помощи подкупа публичных должностных лиц, запугивания, угроз и применения силы с целью защиты преступной деятельности». Соответственно, термин *организованная киберпреступность* используется для описания организованной преступной деятельности в киберпространстве. Как и в случае организованной преступности, не существует единого мнения в отношении определения киберпреступности или организованной киберпреступности (УНП ООН, 2013; Broadhurst et al., 2014; and Maras, 2016).

Исследования в области организованной киберпреступности показывают, что некоторые традиционные характерные черты организованной преступности трудно интерпретировать в контексте киберпространства. Примером такой характерной черты является «контроль над территорией» (УНП ООН, 2013, стр. 50). Варезе (Varese) утверждает, что организованная преступная группа «прилагает усилия для незаконного регулирования и контроля производства и распространения определенных товаров и услуг» (Varese, 2010, p. 14). Такое регулирование возможно на темных рынках (например, на прекративших существование рынках DarkMarket и CardersMarket), где администраторы и модераторы следят за сайтом и контентом и обеспечивают соблюдение правил использования платформ. В случае несоблюдения правил, лица, нарушившие правила, исключаются из числа участников сайта. Хотя «производство и распространение определенных товаров или услуг» могут контролироваться в пределах этих сайтов, такой контроль не распространяется на другие онлайн-форумы (что ограничивает права и полномочия сетей). Поэтому, в отличие от традиционной организованной преступности, их «контроль над производством и определенными товарами или услугами в преступном подполье» является ограниченным (Leukfeldt, Lavorgna, and Kleemans, 2017, p. 296).

На темных рынках структура, организация, регулирование и контроль над незаконными товарами и услугами привязаны к сайтам сети Интернет, а не к людям, которые управляют ими и/или модерируют их. В результате, когда эти сайты темных рынков отключаются от Интернета (например, в связи с расследованием, проводимым правоохранительными органами, или

конфискацией сайта), сеть, связанная с этим сайтом, во многих случаях перестает существовать. Однако существуют исключения, когда участники или другие лица, подключенные к сайту (которые не втянуты в полицейское расследование и процессы судебного преследования), создают другой сайт, который с точностью воспроизводит отключенный сайт. Две другие характерные черты, присущие деятельности традиционных организованных преступных сетей и связанные с коррупцией и угрозой или применением силы (Arsovska, 2011), не находят своего воплощения в контексте организованной киберпреступности (Leukfeldt, Lavorgna, and Kleemans, 2017). Однако это зависит от типа организованной киберпреступной деятельности. Что касается первой характерной черты, то исследования показали, что политическая коррупция влияет на решения об участии в организованной преступной деятельности. В одной стране Интернет-мошенничество, в числе прочих финансовых преступлений, было признано неотъемлемой частью процесса функционирования государства. В отношении второй характерной черты имеется мало свидетельств того, что насилие или угроза применения насилия используется для достижений целей организованной киберпреступной деятельности (УНП ООН, 2013; Leukfeldt, Lavorgna, and Kleemans, 2017), за исключением некоторых случаев, когда, например, *денежные мулы* (т.е. «физические лица, которые получают… и переводят… деньги незаконно по просьбе и за вознаграждение от других лиц»; Maras, 2016) были вовлечены в организованную киберпреступную деятельность и информировали власти о том, что они участвовали или продолжают участвовать в незаконной деятельности, поскольку им угрожают преступники (Leukfeldt, Lavorgna, and Kleemans, 2017, p. 294). В качестве альтернативы физическому насилию организованные киберпреступники совершают кибератаки либо угрожают совершением кибератак или иных киберпреступлений в качестве средства принуждения лиц к выполнению своих требований (Maras, 2016). В качестве примера можно привести использование организованными киберпреступниками *криптовымогателя* («вредоносной программы, которая заражает цифровое устройство пользователя, шифрует документы пользователя и угрожает удалить файлы и данные, если жертва не заплатит выкуп) и/или *шифровальщика-вымогателя*.

3. Преступные группы, вовлеченные в организованную киберпреступность

Организованная киберпреступность может включать в себя деятельность организованных преступных групп, вовлеченных в киберпреступность, а также киберпреступников или иных групп, которые не соответствуют критериям, установленным Конвенцией против организованной преступности, и которые вовлечены в деятельность, обычно связанную с организованной преступностью. Что касается первого типа организованной киберпреступности, то существуют свидетельства того, что в киберпреступления вовлечены традиционные организованные преступные группы (УНП ООН, 2013). Исследования также показывают, что организованные преступные группы используют возможности, которые им

предоставляют информационно-коммуникационные технологии, для совершения киберпреступлений. В частности, как показали результаты одного исследования, организованные преступные группы применяют информационно-коммуникационные технологии для использования новых криминальных онлайн-рынков (например, рынков азартных игр в Интернете). Например, в 2016 году члены преступных групп Каморра и Ндрангета были арестованы за организацию азартных игр в Интернете (OCCRP, 2016). Более того, организованные преступные группы вовлекаются в киберпреступления также и для того, чтобы содействовать организованной преступной деятельности офлайн. Например, организованная преступная группа, занимающаяся незаконным оборотом наркотиков, наняла хакеров для получения доступа к информационным системам порта Антверпен в Бельгии, в которых хранились данные о контейнерах.

Организованные преступные группы, вовлеченные в организованную киберпреступность, могут действовать исключительно в киберпространстве или использовать киберпространство лишь частично. Более того, исследователи расширили понятие организованной преступности, включив в нее действия, продиктованные желанием получить некоторую прямую или косвенную выгоду, которые совершаются полностью или частично в сети Интернет. Таким образом, эти группы могут действовать частично, преимущественно или исключительно в онлайн-среде. Хотя встречаются случаи, когда сети формируются и/или эксплуатируются исключительно и/или преимущественно в сети исследования проблемы создания и развития организованных киберпреступных сетей показывают, что географическая близость и контакты офлайн играют большую роль в формировании и расширении (через вербовку) этих сетей (Broadhurst et al., 2014; Leukfeldt, Lavorgna, and Kleemans, 2017, pp. 292-293). Например, злачные места и хабы организованных киберпреступных сетей были выявлены в Восточной Европе. Кроме того, Европол установил, что «мошенничество методом социальной инженерии, нацеленное на граждан ЕС, осуществляется западноафриканскими организованными преступными группами» (Europol, 2018, p. 13).

До сих пор практически ничего не известно о степени организованности организованной киберпреступной деятельности. Эмпирическая доказательная база данных о структуре организованной киберпреступности, группах, вовлеченных в киберпреступность такого типа, и типах совершаемых киберпреступлений является ограниченной (УНП ООН, 2013, стр. 50). Тем не менее, с учетом имеющихся данных о связях между организованной преступностью и киберпреступностью были предложены типологии, основанные на «степени вовлеченности групп в деятельность в сети Интернет (в отличие от деятельности офлайн) и структуре связей внутри группы» (BAE Systems Detica and London Metropolitan University, 2012, процитировано в УНП ООН, 2013, стр. 51). В частности, были определены три основных типа групп: группы, которые преимущественно действуют в сети Интернет и совершают киберпреступления (тип I); группы, которые действуют офлайн и онлайн и

вовлечены в преступность и киберпреступность (тип II) (см. рисунок 2); и группы, которые используют информационно-коммуникационные технологии только для совершения преступлений офлайн (тип III; не показан на рисунке 2).

Рисунок 2: Типы преступных групп, вовлеченных в организованную киберпреступность

Источник: BAE Detica/LMU

Дополнительно проводится различие между группами каждого типа (BAE Systems Detica и London Metropolitan University, 2012; УНП ООН, 2013; Broadhurst et al., 2014):

Группы типа I могут быть далее разделены на *«рои»* (т.е. менее структурно оформленные группы, которые действуют в основном в сети) и *«хабы»* (т.е. более структурно оформленные группы, которые преимущественно действуют в сети). «Рои» - это кратковременные объединения, которые формируются для достижения конкретной цели и ликвидируются после выполнения своих задач (BAE Systems Detica and London Metropolitan University, 2012).

Группы типа II могут быть далее разделены на *кластерные гибриды* (т.е. группы небольшого размера, которые объединяются по признаку определенных преступлений и киберпреступлений, методов работы и тактики или местоположения) и *расширенные гибриды* (т.е. менее четко определенные, весьма сложные группы, действующие офлайн и онлайн).

Группы типа III могут представлять собой *иерархии* (т.е. традиционные организованные преступные группы, которые используют других лиц для облегчения своей деятельности офлайн с использованием информационно-коммуникационных технологий) и *агрегации* (т.е. кратковременные, слабо организованные группы, которые используют ИКТ по ограниченным, конкретным причинам для способствования деятельности офлайн).

Члены этих групп выполняют различные роли и имеют разные степени значимости для своих групп. Некоторые из них имеют существенно важное

значение для группы и ее деятельности, в то время как другие считаются второстепенными членами или, возможно, даже членами для выполнения разовых задач. К первой категории относятся лидер и некоторые основные члены, имеющие жизненно важное значение для успеха деятельности группы в зависимости от совершаемого киберпреступления (или киберпреступлений) (например, программисты, специалисты по вторжению в системы, технические эксперты, добытчики данных, специалисты по денежным операциям и т.д.). Ко второй категории относятся, например, денежные мулы. Эти лица (сознательно или неосознанно) вербуются преступниками, работают на них, передают товары между третьими лицами и используются для отмывания денег (Maras, 2016).

В 2018 году преступная группа, которая была вовлечена в организованную киберпреступность, осуществила атаку типа *«компрометация деловой переписки»*, которая обманным путем вынудила своих жертв перевести деньги исполнителям этого киберпреступления, выдававшим себя за законных лиц, с которыми работали компании. В этом инциденте денежные мулы в США получали предложение о работе, заключавшейся в осуществлении телеграфных денежных переводов, и/или вербовались с целью создания фиктивных компаний и открытия банковских счетов для фиктивных компаний для получения доходов от онлайн-мошенничества. После того как деньги переводились на банковские счета, контролируемые денежным мулом, денежный мул оставлял себе часть вырученных средств (по согласованию с вербовщиком и/или членами группы) и переводил остальные деньги в банк в Польше или Китае. Денежные мулы и другие неосновные члены киберпреступных групп, вовлеченных в организованную преступную деятельность, являются временными членами группы и участвуют в ее деятельности только по мере необходимости или до тех пор, пока не выполнят свою задачу.

4. Организованная киберпреступная деятельность.

Организованные киберпреступники участвуют в совершении различных киберпреступлений, включая мошенничество, хакерские атаки, создание и распространение вредоносных программ, DDoS-атаки, шантаж и преступления в сфере интеллектуальной собственности такие как продажа контрафактных или фальсифицированных товаров с фирменным знаком (например, одежды, аксессуаров, обуви, электроники, лекарственных препаратов, автомобильных деталей и т.д.), а также этикеток, упаковок и любых других идентифицирующих знаков для этих товаров. Преступные группы, которые вовлечены в организованную киберпреступность, также предоставляют услуги, способствующие совершению преступлений и киберпреступлений («преступление как услуга»), такие как предоставление данных и документов, удостоверяющих личность (например, финансовых и медицинских данных, паспортов, идентификационных данных зарегистрированных избирателей); предоставление вредоносных программ (созданных на заказ или известных программ, таких как, например, Zeus, банковской троянской программы, предназначенной для тайного получения

банковских данных пользователей и прочей информации, необходимой для входа в учетные записи в Интернете); проведение распределенных атак типа «отказ в обслуживании» (DDoS-атаки) и услуги бот-сетей; предоставление клавиатурных шпионов; инструментов фишинга/целевого фишинга; учебников по хакерству; и информации об уязвимостях и эксплойтах, а также инструкций о способах их эксплуатации в целях извлечения выгоды (Broadhurst et al., 2018; Maras, 2016). Например, Shadowcrew, «международная организация, насчитывающая около 4000 членов, … способствовала и содействовала осуществлению обширной и разнообразной преступной деятельности (в сети Интернет), включая, среди прочего, электронную кражу личной идентификационной информации, мошенничество с кредитными и дебетовыми картами, а также изготовление и продажа поддельных документов, удостоверяющих личность» (*United States v. Mantovani et al*., criminal indictment, 2014).

Организованные преступные группы также получают прибыль и/или извлекают иную выгоду от продажи незаконных продуктов и услуг в сети Интернет. Например, создатель вредоносной программы Butterfly Bot рекламировал эту программу в Интернете как способную получить контроль над компьютерами Windows и Linux (BBC News, 2013). Создатель Butterfly Bot также продавал плагины, которые модифицировали функции вредоносной программы, а также предлагал услуги по созданию заказных версий программы для платежеспособных клиентов. Различные онлайновые преступные сети использовали Botfly Bot, и крупнейшее по своим масштабам применение этой вредоносной программы привело к созданию бот-сети Mariposa, которая заразила 12,7 миллионов компьютеров по всему миру (BBC News, 2013).

Организованные киберпреступники также предоставляют услуги *«пуленепробиваемого» хостинга*, которые позволяют преступникам использовать серверы для совершения киберпреступлений и не удаляют преступный контент с этих серверов (National Cyber Security Centre, 2017, p. 8). Из-за низкого уровня доверия к преступным транзакциям в Интернете и существования мошенников, услуги условного депонирования, предоставляемые организованными киберпреступными группами, пользуются большим спросом. Такие услуги позволяют отправлять денежные средства, которые преступные клиенты платят за незаконные товары и услуги, только после того как они подтвердят, что оплаченные ими товары или услуги были получены в целости и сохранности (National Cyber Security Center, 2017, p. 8).

Незаконные товары и услуги в основном приобретаются за *криптовалюту* (т.е. «цифровую валюту, которая использует криптографию в целях безопасности»; Maras, 2016, p. 337). На рынке существует множество криптовалют (например, биткойн, Litecoin, Dogecoin, Ethereum, Monero и т.д.). Хотя на большинстве рынков даркнета торговля ведется в основном за биткойны, используются и другие криптовалюты (например, Ethereum и Monero), а в некоторых случаях им отдается предпочтение перед биткойном (US Department of Justice, 2017; Broadhurst et al., 2018; Europol, 2018).

Некоторые сайты даркнета используют так называемый «тумблер», который отправляет «все платежи через сложную, полупроизвольную серию фиктивных транзакций, что практически исключает возможность связать… платеж с какой-либо криптовалютой, покидающей сайт» (*United States v. Ross William Ulbricht,* Criminal Complaint, 2013, p. 14).

Кроме того, организованные киберпреступники также предоставляют услуги по *отмыванию денег,* т.е. «сокрытию и легализации незаконных средств преступников» (Maras, 2016). Отмываются также и доходы от услуг, предоставляемых организованными киберпреступниками. Процесс отмывания денег включает в себя три этапа: введение незаконных доходов в финансовую систему (*размещение*), сокрытие источника происхождения незаконных средств (*расслоение*) и возвращение средств в экономику без указания источника происхождения. Деньги отмываются с использованием *цифровой валюты* (т.е. нерегулируемой валюты, существующей лишь виртуально); предоплаченных кредитных и дебетовых карт (даже биткойновых карт); подарочных карт; банковских счетов денежных мулов; банковских счетов, открытых на вымышленные имена/фиктивные компании; счетов PayPal; игорных сайтов в Интернете (через виртуальную игровую валюту); и незаконных сайтов азартных игр. Кроме того, организованные киберпреступники используют информационно-коммуникационные технологии (ИКТ) для содействия в осуществлении различных видов традиционной организованной преступной деятельности вне сети, таких как незаконный ввоз мигрантов и торговля людьми, незаконная торговля объектами живой природы, наркотиками, огнестрельным оружием и сигаретами. Например, незаконный ввоз мигрантов, который в соответствии со статьей 3 (a) Протокола против незаконного ввоза мигрантов по суше, морю и воздуху 2000 года, дополняющего Конвенцию Организации Объединенных Наций против транснациональной организованной преступности, определяется как «обеспечение, с целью получения, прямо или косвенно, какой-либо финансовой или иной материальной выгоды, незаконного въезда в какое-либо Государство-участник любого лица, которое не является его гражданином или не проживает постоянно на его территории», осуществляется при содействии контрабандистов, использующих ИКТ для рекламы своих услуг, вербовки мигрантов, коммуникации с ними и, в конечном итоге, продажи им своих услуг.

Вопросы для обсуждения:

1. Какая криптовалюта в основном используется гражданами вашей страны? Почему она используется?
2. Используются ли какие-либо другие криптовалюты? Если да, определите и обсудите их.
3. Как криптовалюты используются организованными киберпреступниками?

Тема 14. Хактивизм, терроризм, шпионаж, дезинформационные кампании и войны в киберпространстве.

1. Хактивизм.

Информационно-коммуникационные технологии используются в кампаниях за социальные или политические перемены (т.е., для онлайн-активизма). Кампании такого типа предполагают сбор подписей под онлайн-петициями, хэштег-кампании, создание веб-сайта кампании, набор добровольцев, получение средств от участников и сторонников, а также организацию и планирование офлайн-протестов (Maras, 2016). Однако существуют отдельные лица и группы людей, которые считают такие методы недостаточными для привлечения внимания к своим идеям, и вместо этого, в качестве средства политического протеста, прибегают к стратегиям, которые непосредственно влияют на функционирование или доступность веб-сайтов и онлайн-сервисов (т.е. *хактивисты*) (Maras, 2016).

Хотя общепризнанного определения термина *хактивизм* не существует, эти действия описываются как преднамеренный доступ к системам, веб-сайтам или данным без авторизации либо с превышением авторизованного доступа, и/или преднамеренное вмешательство в функционирование и/или доступность систем, веб-сайтов и данных без авторизации либо с превышением авторизованного доступа в целях продвижения социальных или политических преобразований (Maras, 2016). Мнения в отношении законности хактивизма как формы законного политического протеста различаются. Например, виртуальные сидячие забастовки, предназначенные для имитирования распределенных атак типа «отказ в обслуживании», но не предполагающие использования зараженных вредоносными программами цифровых устройств (т.е. бот-сетей), нацеленных на веб-сайт, описываются некоторыми исследователями как форма политического протеста. Виртуальные сидячие забастовки (или блокады) подразумевают совершение коллективных действий, во время которых «тысячи активистов одновременно посещают веб-сайт и пытаются сгенерировать такой объем трафика на сайте, чтобы другие пользователи не могли получить к нему доступ». Например, когда группы людей одновременно и непрерывно нажимают на кнопку обновления при посещении сайта. Такие виртуальные сидячие забастовки описываются как действия при наличии авторизованного доступа к веб-сайту, связанные с неоднократным и частым осуществлением доступа на этот веб-сайт; такой неоднократный и частый доступ осуществляется в масштабе, который препятствует доступу к этому веб-сайту другим пользователям. Существует множество групп хактивистов, преследующих различные социальные и политические цели. Киберпреступления, совершаемые хактивистами, включают в себя порчу веб-сайтов, перенаправление пользователей на другой веб-сайт, атаки типа «отказ в обслуживании» (DoS-атаки) или распределенные атаки типа «отказ в обслуживании» (DDoS-атаки), распространение вредоносных программ, кражу и раскрытие данных, а также саботаж (Maras, 2016). Все эти методы подразумевают несанкционированный доступ к системам, веб-сайтам и/или данным, являющимся объектами атаки.

Например, в Уганде веб-сайты официальной резиденции президента страны и Управления по инвестициям Уганды были искажены хактивистами, которые разместили на сайте резиденции президента нацистскую свастику и фото Адольфа Гитлера, а на сайте Управления по инвестициям заменили часть текста изображением страшного клоуна.

2. Кибершпионаж.

Несмотря на отсутствие единого универсального определения термина шпионаж, его определяют как метод сбора разведывательных данных: в частности, как «процесс получения информации, которая обычно не является общедоступной, с использованием человеческих источников (агентов) или технических средств (например, путем взлома компьютерных систем)» (UK MI5 Security Service, n.d.). Тем не менее, даже термин «сбор разведывательных данных» не имеет «признанного на международном уровне и пригодного для использования определения». Более того, складывается впечатление, что существует почти столько же определений термина «разведывательные данные», сколько экспертов, которых просят дать определение этому термину. Как утверждает Уорнер (Warner), толкователи термина «шпионские операции» обычно относят себя к одному из двух лагерей оппонентов: «В первом лагере толкователи придерживаются американской военной терминологии двадцатого века и считают, что разведданные - это информация для лиц, принимающих решения; это любая информация из любого источника, которая может помочь руководителю принять решение о том, как поступить с противником. Во втором лагере сбор разведданных определяется как война более тихими средствами». Любин предлагает более детальное определение шпионских операций. Он утверждает, что все такие операции включают в себя следующие четыре элемента: «1) операция предполагает сбор, анализ, проверку и распространение сведений, которые имеют значение для принятия решений государством или государствами либо служат определенным государственным интересам в иных отношениях; 2) операция инициируется агентами государства или государств либо лицами, тесно связанными с соответствующим государством или государствами; 3) операция нацелена на иностранное государство или иностранные государства, их субъектов, ассоциации, корпорации или агентов и осуществляется без ведома или согласия этого государства или этих государств; и 4) операция предполагает определенную степень секретности и конфиденциальности в отношении потребностей, обусловливающих ее проведение, или используемых методов сбора и анализа, с тем чтобы обеспечить ее эффективность».

Кибершпионаж предполагает использование информационно-коммуникационных технологий (ИКТ) отдельными лицами, группами лиц или компаниями для извлечения определенной экономической или личной выгоды. Кибершпионаж может также осуществляться правительственными структурами, группами, финансируемыми или контролируемыми государством либо прочими лицами, действующими от имени правительства, для получения несанкционированного доступа к системам и данным и сбора разведданных об интересующих их объектах, чтобы повысить уровень

национальной безопасности, экономической конкурентоспособности и/или военной мощи своей страны (Maras, 2016). Хотя шпионаж и не является новым явлением, возникновение ИКТ обеспечило возможности для осуществления действий по незаконному сбору разведданных, предпринимаемых и/или организуемых другими странами, с беспрецедентной скоростью, частотой, интенсивностью и в невиданных ранее масштабах, а также для снижения рисков, связанных с осуществлением шпионажа (например, рисков быть пойманным страной, на которую направлены усилия по сбору данных). Осуществление кибершпионажа стало возможным благодаря многочисленным хакерским инструментам, которые широко доступны в Интернете. Эти инструменты включают в себя эксплойты (например, *уязвимость нулевого дня,* т.е. ранее неизвестные уязвимости, эксплуатируемые после их обнаружения, либо вредоносные программы, которые могут проникать в системы и обходить брандмауэры) и *импланты* (например, *бэкдор*, секретный портал, используемый для получения несанкционированного доступа к системам, или инструмент удаленного доступа RAT). Начиная с 2016 года, группа, известная как Shadow Brokers, выпускает хакерские инструменты (Newman, 2018). Один из таких инструментов предназначен для эксплуатации уязвимости Windows (эксплойт EternalBlue); он был частью программы-вымогателя WannaCry, которая атаковала системы здравоохранения, транспорта и другие системы по всему миру с целью причинения им ущерба.

3. Кибертерроризм.

Информационно-коммуникационные технологии (ИКТ) могут использоваться для способствования совершению преступлений, связанных с терроризмом (разновидность терроризма, совершаемого посредством кибертехнологий), или могут быть целью террористов (форма киберзависимого терроризма). Например, ИКТ могут использоваться для поощрения, поддержки террористических актов, содействия в их совершении или участия в них. В частности, Интернет может использоваться для таких целей террористической деятельности, как распространение «пропаганды (включая вербовку, радикализацию и подстрекательство к терроризму); финансирование терроризма; подготовка террористов; планирование террористических атак (в том числе с использованием засекреченных каналов связи и информации из открытых источников); исполнение террористических актов; и кибератаки» (UNODC, 2012, p. 3). Термин кибертерроризм используется некоторыми исследователями для описания действий, связанных с использованием Интернета в террористических целях.

Точно так же, как нет единого мнения в отношении определения термина «киберпреступность», не существует общепринятых определений ни терроризма ни кибертерроризма. Понятия кибертерроризма варьируют от «более широких концепций, включающих в себя любую форму террористической деятельности в Интернете до более узкого понимания этого понятия». Некоторые исследователи толкуют кибертерроризм в узком его понимании как «чистый кибертерроризм». В рамках такого узкого

определения кибертерроризм рассматривается как киберзависимое преступление, совершаемое в политических целях, чтобы вызвать страх, запугать правительство или население, являющееся объектом атаки, или оказать на него давление, а также причинить ущерб или выступить с угрозой причинения ущерба (например, саботаж). Примеры такого узкого понятия кибертерроризма включают в себя «атаки, которые приводят к смерти или телесным повреждениям, взрывам, авиакатастрофам, загрязнению воды или серьезным экономическим потерям. Серьезные атаки на критически важные объекты инфраструктуры могут представлять собой акты кибертерроризма в зависимости от их последствий. Атаки, которые нарушают работу второстепенных служб либо вызывают в основном неприятности, сопряженные с издержками, не являются кибертерроризмом».

4. Кибервойна.

Средства массовой информации, политики, ученые и практикующие специалисты относят многочисленные инциденты, связанные с киберпреступностью, к категории «кибернетических войн» или «кибервойн» (Maras, 2014; Maras, 2016). Как и в случае других терминов, рассмотренных выше, не существует единого универсального определения кибервойны. Термин *кибервойна* используется для описания действий в киберпространстве, которые ставят под угрозу и разрушают критически важные системы инфраструктуры и могут приравниваться к вооруженному нападению (Maras, 2016). *Вооруженное нападение* - это преднамеренное действие, влекущее за собой разрушительные последствия (т.е. смерть или телесное повреждение живых существ или уничтожение имущества) (Maras, 2016). Только правительства, государственные органы либо отдельные лица или группы лиц, управляемые или финансируемые государством, могут участвовать в кибервойне.

Существующие правовые нормы и правила, касающиеся приемов ведения войны, распространяются на кибервойны. Прежде чем начать кибервойну, необходимо установить *jus ad bellum* (т.е. право применить силу). При этом причины применения силы любой формы должны быть законными и разрешены законодательством. Одной из таких обоснованных причин является самооборона. Страны могут применять силу в целях самообороны в соответствии со статьей 51 Устава ООН 1945 года, которая гласит:

Настоящий Устав ни в коей мере не затрагивает неотъемлемого права на индивидуальную или коллективную самооборону, если произойдет вооруженное нападение на Члена Организации, до тех пор, пока Совет Безопасности не примет мер, необходимых для поддержания международного мира и безопасности. Меры, принятые Членами Организации при осуществлении этого права на самооборону, должны быть немедленно сообщены Совету Безопасности и никоим образом не должны затрагивать полномочий и ответственности Совета Безопасности, в соответствии с настоящим Уставом, в отношении предпринятия в любое время таких действий, какие он сочтет необходимыми для поддержания или восстановления международного мира и безопасности.

Право на самооборону служит одним из исключений из общего запрета на применение силы против других государств, предусмотренного в статье 2(4) Устава ООН («все Члены Организации Объединенных Наций воздерживаются в их международных отношениях от угрозы силой или ее применения как против территориальной неприкосновенности или политической независимости любого государства, так и каким-либо другим образом, несовместимым с Целями Объединенных Наций»).

При участии в кибервойне необходимо соблюдать *jus in bello* (т.е. правила ведения войны). При этом действия в киберпространстве, которые равносильны применению силы, должны: быть соразмерными (как угрозе, которая явилась основанием для ответных действий, так и с учетом потенциального сопутствующего ущерба); быть направлены на минимизацию потерь путем принятия определенных мер предосторожности; распознавать цели (т.е. только реальная цель должна подвергаться кибератакам); и использоваться только в качестве крайней меры после того, как менее агрессивные средства были исчерпаны или исключены как неосуществимые (Maras, 2016).

5. Информационная война, дезинформация и мошенничество на выборах.

Термин *информационная война* используется для описания процесса сбора, распространения, изменения, разрушения, порчи, повреждения и ухудшения качества информации с целью получения определенного преимущества перед противником. Цель этого процесса заключается в том, чтобы использовать и сообщать эту информацию таким образом, чтобы изменить восприятие объекта в отношении какой-либо проблемы или какого-либо события для достижения определенного желаемого результата. В информационной войне используются два метода: *дезинформация* (т.е. преднамеренное распространение ложной информации) и *фальшивые новости* (т.е. пропаганда и дезинформация, распространяемые под видом реальных новостей). Важно отметить, что последний из перечисленных терминов не имеет четкого определения и может использоваться неправильно (см. ниже вставку о Совместной декларации о свободе выражения мнения, а также «фейковых» новостях, дезинформации и пропаганде).

Снижение уровня доверия способствовало быстрому распространению и потреблению *фальшивых новостей* общественностью (Morgan, 2018, p. 39). Дезинформация и фальшивые новости распространяются на платформах социальных сетей, а также через ведущие и второстепенные средства массовой информации. Платформы социальных сетей позволяют распространять дезинформацию быстрее и охватить более широкую аудиторию по сравнению с другими онлайн-платформами; на некоторых платформах она может распространяться в режиме реального времени (например, в Twitter). Автоматические учетные записи ботов облегчают эти усилия, помогая распространять информацию быстрее и с более высокой частотой, чем это могут делать отдельные пользователи. Например, ИГИЛ разработало приложение «The Dawn of Glad Tidings» («Рассвет благих вестей»), которое

его участники и сторонники могли загружать на свои мобильные устройства; это приложение, помимо прочего, было разработано для получения доступа к учетным записям пользователей Twitter и публикации сообщений от их имени. Сторонники кампании по дезинформации и боты также способствуют более широкому распространению дезинформации и фальшивых новостей в Интернете. Избирательное, повторяющееся и частое воздействие дезинформации и фальшивых новостей помогает сформировать, подкрепить и усилить уверенность о том, что передаваемое сообщение является правдой. Считается, что дезинформация и фальшивые новости влияют на поведение избирателей и, в конечном итоге, на результаты выборов.

Мошенничество на выборах «можно определить как любое целенаправленное действие, предпринимаемое для манипулирования выборными процессами и материалами, связанными с выборами, с целью оказания влияния на результаты выборов, которое может препятствовать свободе выбора избирателей или исказить их волеизъявление». Одним из примеров мошенничества на выборах является получение несанкционированного доступа к устройствам для голосования и изменение результатов голосования. Важно отметить, что общепринятого определения мошенничества на выборах не существует, поскольку понятие мошенничества зависит от контекста: действие, воспринимаемое как мошенническое манипулирование избирательным процессом, толкуется по-разному с течением времени в зависимости от конкретной страны. Даже в научных кругах теоретические определения мошенничества до сих пор еще не унифицированы в областях международного и внутреннего права, сравнительной и американской политологии и проведения выборов в развитых и развивающихся странах (Alvarez, Hall, and Hyde, 2008, pp. 1-2).

В некоторых странах действуют законы, предусматривающие уголовную ответственность за распространение ложной информации, которая может повлиять на поведение избирателей и результаты выборов, а также за другие формы мошенничества на выборах (например, во Франции, Великобритании и различных штатах США). Другие страны, в которых действуют законы, предусматривающие уголовную ответственность за распространение ложной информации и фальшивых новостей, используют эти законы для преследования журналистов и других лиц, которые критикуют правительство или иным образом бросают ему вызов (Reuters, 2018).

Задание для обсуждения:

Меры реагирования на кибератаки. Сотрудники компьютерной компании, базирующейся в стране А, обвиняются в проведении многочисленных распределенных атаках типа «отказ в обслуживании» на сектор финансовых услуг и получении доступа к автоматизированной системе управления плотиной в стране Б. Представители сектора финансовых услуг сообщили о значительном экономическом ущербе; однако представители плотины сообщили лишь о краже информации. Хотя злоумышленники получили доступ к автоматизированной системе управления (АСУ) плотиной,

которая позволила бы модифицировать систему и управлять плотиной удаленно, та часть АСУ, которая могла бы позволить это сделать, находилась в автономном режиме и проходила техническое обслуживание во время инцидента. Считается, что сотрудники этой компании финансировались страной А.

Вопросы:

1. Какой тип киберинцидента описывается в этом сценарии? Почему вы так считаете?
2. Что бы потребовалось для того, чтобы доказать, что ответственность за инцидент несет страна А?
3. С какими препятствиями вы можете столкнуться при доказывании ответственности страны А?
4. Какие действия можно предпринять в ответ на это кибервмешательство? Почему вы так считаете?
5. Можно ли легко распознать фальшивые новости? Поясните свой ответ.
6. Какие действия могут предпринять люди, чтобы распознать фальшивые новости?

Глоссарий

Адрес Интернет-протокола. Уникальный идентификатор, присваиваемый подключенному к Интернету цифровому устройству поставщиком услуг Интернета для подключения к сети. Также известен под названием *IP -адрес.*

Актив. Нечто, считающееся важным или ценным.

Активный цифровой отпечаток. Создается данными, предоставляемыми пользователем.

Анализ временных рамок. Анализ, выполняемый с целью создания временной шкалы или временной последовательности действий с использованием меток времени (даты и времени), которые привели к событию, или установления времени и даты, когда пользователь совершил определенное действие.

Анализ метода сокрытия данных. Тип анализа, при помощи которого осуществляется поиск скрытых данных в системе.

Анализ приложений и файлов. Тип анализа, который выполняется для исследования приложений и файлов в компьютерной системе, чтобы установить заведомость, умысел и возможности преступника в отношении совершения киберпреступления.

Анализ собственности и владения. Тип анализа, используемый для установления лица, которое создало файлы в компьютерной системе, получило к ним доступ и/или изменило их.

Анонимайзеры. Эти прокси-серверы позволяют пользователям скрывать свои идентифицирующие данные, маскируя их IP-адреса и заменяя их другими IP-адресами. Также известны под названием *анонимные прокси-серверы*.

Анонимность. Сокрытие человеком своей личности, что позволяет ему заниматься какой-либо деятельностью, не раскрывая информации о себе и/или своих действиях другим лицам.

Анонимные прокси-серверы. Эти прокси-серверы позволяют пользователям скрывать свои идентифицирующие данные, маскируя их IP-адреса и заменяя их другими IP-адресами. Также известны под названием *анонимайзеры*.

Антикриминалистика. Инструменты и методы, используемые для того, чтобы запутать расследование киберпреступлений и затрудняет усилия по проведению цифровой судебной экспертизы. Также известна под названием *цифровая антикриминалистика.*

Атака «грубой силой». Использование скрипта или робота для угадывания учетных данных пользователя.

Атака на водопое. Размещение вредоносных программ на веб-сайтах, наиболее часто посещаемых жертвами, чтобы в конечном итоге заразить их системы и получить несанкционированный доступ к ним.

Атака типа «отказ в обслуживании». Киберпреступление, которое создает помехи системам, перегружая серверы запросами, чтобы препятствовать доступу законного трафика к сайту и/или использованию системы. Также известна под названием *DoS -атака.*

Атрибуция. Определение того, кто и/или что является ответственным за совершение киберпреступления.

Блокировщик записи. Предназначен для предотвращения изменения данных в процессе копирования.

Большие данные. Структурированные и неструктурированные данные больших объемов, которые можно объединить и проанализировать для выявления ассоциаций, закономерностей и тенденций.

Бот-код. Тип вредоносного программного обеспечения, который позволяет удаленно управлять этими устройствами и использовать их для совершения киберпреступлений, кражи информации и/или участия в кибератаках.

Бот-сеть. Сеть компьютеров, зараженных бот-кодом.

Бэкдор. Секретный портал, используемый для получения несанкционированного доступа к системам.

Видимая паутина. Индексированные сайты, которые доступны и готовы к использованию для широкой публики, и которые можно найти с использованием традиционных поисковых систем. Также известна под названием *видимая сеть* или *видимый Интернет.*

Видимая сеть. Индексированные сайты, которые доступны и готовы к использованию для широкой публики, и которые можно найти с использованием традиционных поисковых систем. Также известна под названием *видимый Интернет* или *видимая паутина*.

Видимый Интернет. Индексированные сайты, которые доступны и готовы к использованию для широкой публики, и которые можно найти с использованием традиционных поисковых систем. Также известна под названием *видимая сеть* или *видимая паутина.*

Вирус. Вредоносная программа, для распространения которой требуется участие пользователя.

Вирус-вымогатель. Вредоносная программа, предназначенная для взятия систем, файлов и/или данных пользователей в заложники и возвращения контроля пользователям только после выплаты выкупа.

Вишинг. Фишинг с использованием телефонных коммуникаций.

Восстановление. Определение, разработка и окончательная реализация мер по усилению устойчивости и восстановление систем, сетей, услуг и данных, которые были недоступны, нарушены, повреждены и/или скомпрометированы во время инцидента.

Вредоносная программа. Вредоносное программное обеспечение.

Временной анализ. Установление времени и последовательности событий.

Вытеснение преступности. Когда преступление, которое было нацелено на один объект, совершается в отношении другого объекта из-за действующих мер безопасности.

Вычленение однородных массивов данных. Поиск на основе

идентификаторов контента.

Географические указания. Символ качества изделия и репутация места его создания, которые нельзя использовать, кроме случаев, когда продукт был разработан в этом регионе в соответствии с общепринятой стандартной практикой. Также известны как *наименования мест происхождения.*

Глубокая сеть. Часть Всемирной паутины, сайты которой не индексируются поисковыми системами и не являются легкодоступными и/или готовыми к использованию для широкой публики.

Груминг детей. Соблазнение детей или домогательство в отношении детей с сексуальными целями.

Группа реагирования на инциденты в сфере компьютерной безопасности. Группа, которая предоставляет поддержку в случае инцидентов, связанных с компьютерной безопасностью. Также известна под названием *Группа реагирования на нарушение компьютерной защиты.*

Группа реагирования на нарушение компьютерной защиты. Группа, которая предоставляет поддержку в случае инцидентов, связанных с компьютерной безопасностью. Также известна под названием *Группа реагирования на инциденты в сфере компьютерной безопасности.*

Данные. Любое представление информации, которая обрабатывается в системе цифрового устройства. Также известны под названием *компьютерные данные* или *компьютерная информация*.

Данные, не относящиеся к контенту. Данные о содержании. Также известны под названием *метаданные.*

Данные, относящиеся к контенту. Слова в письменных сообщениях или произнесенные слова.

Данные о трафике. Данные, которые передаются по компьютерной сети.

Даркнет. Часть Всемирной паутины, известная своими веб-сайтами с затрудненным доступом и скрытыми веб-сайтами, на которых осуществляются незаконные действия и реализуются незаконные товары и услуги, и доступ к которым возможен только с помощью специализированного программного обеспечения. Также известна под названием Темная паутина.

Дезинформация. Умышленное распространение ложной информации.

Денежные мулы. Лица, которые сознательно или неосознанно совершают преступления и/или киберпреступления путем получения и перевозки незаконных товаров, участия в оказании незаконных услуг и/или незаконного получения или перевода денег другим лицам за вознаграждение.

Диссоциативная анонимность. Выпадение поведения людей в Интернете из контекста обычного поведения в реальной жизни из-за анонимности, которая обеспечивается им при использовании Интернета и цифровых технологий.

Диссоциативное воображение. Восприятие киберпространства как форума, в рамках которого не применяются правила повседневного взаимодействия, кодексы поведения, социальные нормы и/или законы, запрещающие человеку действовать вопреки правилам повседневного взаимодействия, кодексам поведения, социальным нормам и/или законам, действующим в реальном

мире.

Доксинг. Публикация личной информации в Интернете с целью причинения какого-либо вреда.

Доменное имя. Представление IP-адреса в Интернет-браузере (или веб-браузере).

Договор о взаимной правовой помощи. Соглашение между странами о сотрудничестве в расследованиях и судебном преследовании в отношении некоторых и/или всех преступлений, считающихся таковыми в соответствии с национальным законодательством обеих сторон.

Догпайлинг. Тактика, при помощи которой пользователи в рамках одного пространства в Интернете заваливают жертв непристойными, оскорбительными и угрожающими сообщениями, чтобы заставить их замолчать, вынудить их забрать свои слова обратно и/или извиниться или заставить их покинуть платформу.

Доступность. Когда данные, услуги и системы доступны по первому требованию.

Жесткий диск. Внутренняя постоянная память компьютера.

Защита данных. Защита личной информации и регулирование процессов ее сбора, хранения, анализа, использования и обмена.

Защита данных на основе продуманных действий. Меры по обеспечению конфиденциальности, встроенные в конструкцию систем и технологий. Также известна под названием *конфиденциальность на основе подуманных действий.*

Значимость с точки зрения криминалистики. Значимость данных для судебной экспертизы определяется тем, могут ли цифровые доказательства: установить или исключить связь между преступником и мишенью и/или местом преступления; подтвердить или опровергнуть показания преступника, потерпевшего и/или свидетеля; установить личность исполнителя (исполнителей) киберпреступления; позволить выдвинуть следственные версии; обеспечить получение информации о способе действий, использованном преступником; и показать, что преступление действительно имело место.

Интеллектуальная собственность. Продукты творчества, такие как произведения, инновации, творения, оригинальное выражение идей и секретные методы, процессы ведения бизнеса, на которые люди имеют права в соответствии с законом.

Интернет вещей. Сеть взаимосвязанных и взаимодействующих друг с другом устройств с выходом в Интернет, которые позволяют отслеживать объекты, людей, животных и растения, а также осуществлять сбор, анализ, хранение и распространение информации о них.

Интернет тролли. Люди, которые намеренно публикуют грубые, агрессивные и оскорбительные высказывания в Интернете, направленные на создание раздоров и недовольства в Интернете.

Информационная война. Процесс сбора, распространения, изменения, разрушения, порчи, повреждения и ухудшения качества информации с целью

получения определенного преимущества над противником.

Кибербезопасность. Набор стратегий, механизмов и мер, которые предназначены для выявления угроз и уязвимостей систем, сетей, услуг и данных к этим угрозам; предотвращения эксплуатации уязвимостей; смягчения вреда, причиняемого материализованными угрозами; и защиты людей, имущества и информационно-коммуникационных технологий.

Кибервойна. Действия в киберпространстве, которые ставят под угрозу и разрушают критически важные системы инфраструктуры и приравниваются к вооруженному нападению.

Кибердомогательство. Использование информационно-коммуникационных технологий для преднамеренных действий с целью унижения, раздражения, нападок, угроз, запугивания, нанесения обиды и/или оскорбления лица (или лиц).

Киберзависимое преступление. Киберпреступление, которое было бы невозможно без Интернета и цифровых технологий.

Киберклевета. Размещение или распространение иным способом в интернете ложной информации или слухов о взрослом или ребенке, чтобы причинить ущерб его социальному положению, межличностным отношениям и/или репутации.

Киберпреследование. Использование информационно-коммуникационных технологий для совершения неоднократных действий в течение определенного периода времени с целью домогательства, беспокойства, нападок, угроз, запугивания и/или словесного оскорбления лица (или лиц).

Киберпреступления против личности. Киберпреступления, совершаемые отдельными лицами против других лиц, с которыми они взаимодействуют, общаются и/или имеют какие-либо реальные или воображаемые отношения.

Кибер-прокси. Посредники, непосредственно или косвенно способствующие совершению киберзависимого преступления, преднамеренно нацеленного на государство.

Киберпространство. Среда, доступная с помощью цифровых устройств с выходом в Интернет, в которой осуществляется онлайн деятельность.

Кибертерроризм. Киберзависимые преступления, совершаемые против критически важных объектов инфраструктуры, чтобы причинить какой-либо вред и вызвать страх у целевой группы населения.

Кибертравля. Использование информационно-коммуникационных технологий детьми с целью досаждения, унижения, оскорбления, нанесения обиды, домогательства, запугивания, преследования, жестокого обращения или иных нападок в отношении других детей

Кибершпионаж. Использование информационно-коммуникационных технологий правительственными структурами, группами, финансируемыми или контролируемыми государством либо прочими лицами, действующими от имени правительства, для получения несанкционированного доступа к системам и данным и сбора разведданных о своих целях, чтобы повысить уровень национальной безопасности, экономической конкурентоспособности и/или военной мощи своей страны.

Ключевые показатели деятельности. Меры, которые используются для оценки прогресса в деле реализации стратегических задач национальной стратегии кибербезопасности.

Кодекс этики. Руководящие принципы, которые определяют правильное и неправильное поведение в процессе принятия решений.

Коммерческая сексуальная эксплуатация детей. Термин, используемый для описания некоторых видов деятельности и преступлений, связанных с сексуальным насилием над детьми в обмен на какое-либо либо денежное или неденежное вознаграждение.

Компьютерная информация. Любое представление информации, которая обрабатывается в системе цифрового устройства. Также известна под названием *компьютерные данные* или *данные*.

Компьютерная сеть. Два или более компьютеров, которые обмениваются данными, отправляя их друг другу.

Компьютерная система. Автономное или сетевое устройство, которое выполняет обработку данных и другие функции.

Компьютерные данные. Любое представление информации, которая обрабатывается в системе цифрового устройства. Также известны под названием *компьютерная информация* или *данные*.

Конфиденциальность на основе продуманных действий. Меры по обеспечению конфиденциальности, встроенные в конструкцию систем и технологий. Также известная под названием *защита данных на основе продуманных действий.*

Конфиденциальность. Системы, сети и данные защищены, и только авторизованные пользователи могут получить к ним доступ.

Координированное раскрытие уязвимостей. Практика согласованного обмена информацией и раскрытия информации об уязвимостях соответствующим заинтересованным сторонам и смягчение негативных последствий такого раскрытия.

Косвенные доказательства. Доказательство, которое позволяет вывести заключения об истинности факта.

Криптовалюта. Разновидность цифровой валюты, которая защищена с использованием продвинутого стандарта шифрования.

Криптовымогатель. Вредоносная программа, которая заражает цифровое устройство пользователя, шифрует документы пользователя и угрожает удалить файлы и данные, если жертва не заплатит выкуп.

Криптоджекинг. Способ, при помощи которого вычислительная мощность зараженных компьютеров используется для добычи криптовалюты для извлечения финансовой выгоды лицом (лицами), контролирующим зараженные цифровые устройства.

Криптомаркет. Веб-сайт, использующий криптографию для защиты пользователей сайта.

Критически важная инфраструктура. Жизненно важные отрасли, которые считаются основополагающими для надлежащего функционирования общества.

Кэтфишинг. Дача ложных или вводящих в заблуждение обещаний любви и дружбы, чтобы мошенническим путем отнять у них время, деньги и/или прочие предметы.

Лица, принимающие первые ответные меры. Лица, которые первыми реагируют на преступление и отвечают за сохранность доказательств на месте совершения преступления.

Личная автономия. Способность делать выбор и действовать по своему собственному выбору без принуждения.

Логическое извлечение. Поиск и получение доказательств из места, в котором они находятся относительно файловой системы.

Материальное право. Правовые нормы, регулирующие поведение и обязанности лиц, в отношении которых государство осуществляет юрисдикцию.

Материалы с изображением сексуального насилия над детьми. Изображение сексуального насилия над детьми и/или других сексуализированных действий с использованием детей.

Межсетевой экран. Системазащиты, которая ограничивает свободный поток информации, блокируя несанкционированный трафик.

Метаданные. Данные о содержании. Также известны под названием *данные, не относящиеся к контенту.*

Менялы. Полуавтоматические биржи криптовалют.

Микро-отмывание. Форма отмывания денег, при помощи которой преступники отмывают значительные суммы денег посредством осуществления многочисленных мелких транзакций.

Морфинг. Процесс, при котором лицо или голова жертвы накладывается на тела других людей с целью диффамации, создания порнографии и/или сексуального надругательства.

Мошенничество методом социальной инженерии. Склонение жертвы к раскрытию или предоставлению иным образом личной информации и/или средств злоумышленнику.

Мошенничество на выборах. Использование неправомерных методов для оказания влияния на результаты выборов.

Мошенничество с авансовым платежом. Вид компьютерного мошенничества, предполагающий использование писем с просьбой произвести авансовый платеж для завершения операции по переводу денег, депонированию или иной трансакции в обмен на более крупную сумму денег.

Наилучшее доказательство. Подлинное доказательство или точная копия подлинного доказательства.

Наименования мест происхождения. Символ качества изделия и репутация места его создания, которые нельзя использовать, кроме случаев, когда продукт был разработан в этом регионе в соответствии с общепринятой стандартной практикой. Также известны как *географические указания*.

Недостоверная информация. Ложная или неточная информация.

Неприкосновенность частной жизни. Право быть оставленным в покое; право на свободу от наблюдения; способность хранить в тайне свои мысли,

убеждения, личность и поведение; и право выбирать и контролировать, когда, почему, где, как и кому раскрывается личная информация, какая личная информация раскрывается и в каком объеме.

Нераспределенное пространство. Пространство, доступное для использования, потому что информация из него была удалена, или пространство, которое никогда не использовалось.

Обеспечение сохранности данных. Направление просьб поставщикам услуг правоохранительными органами в целях сохранения данных до того, как они будут удалены или каким-либо образом изменены.

Обнаружение инцидентов. Процесс определения угроз путем активного мониторинга активов и выявления аномальной активности.

Обоюдное признание соответствующего деяния преступлением. Пункт в международных договорах, требующий, чтобы действия считались незаконными в сотрудничающих странах.

Обработка рисков. Меры реагирования на риски.

Обратное прослеживание. Процесс прослеживания незаконных действий для установления источника киберпреступления. Также известно как *прослеживание в обратном направлении*.

Организованная киберпреступность. Термин, используемый для описания постоянно действующего преступного предприятия, которое рационально работает для получения прибыли путем незаконной деятельности в сферах тех служб, на которые есть большой спрос в Интернете.

Организованная преступность. Постоянно действующее преступное предприятие, рационально работающее для получения прибыли путем незаконной деятельности в сферах, на которые есть большой общественный спрос.

Организованные киберпреступники. Структурно оформленная группа в составе трех или более лиц, существующая в течение определенного периода времени и действующая согласованно с целью совершения одного или нескольких серьезных преступлений или преступлений, признанных таковыми в соответствии с Конвенцией Организации Объединенных Наций против транснациональной организованной преступности 2000 года, которая действует полностью или частично в сети Интернет, с тем чтобы получить, прямо или косвенно, финансовую или иную материальную выгоду.

Ответственное раскрытие информации об уязвимости. Практика нераскрытия информации об уязвимости до тех пор, пока ответственная организация не устранит уязвимость.

Отмывание денег. Сокрытие незаконных средств путем сочетания законных и незаконных операций.

Оценка риска. Оценка вероятности угрозы, ее последствий и подверженности актива этой угрозе.

Пассивный цифровой отпечаток. Данные, которые получают и непреднамеренно оставляют люди, пользующиеся Интернетом и цифровыми технологиями.

Патент. «Исключительное право, предоставляемое на изобретение

(инновацию или творение), являющееся изделием или процессом, который, как правило, представляет собой новый способ выполнения того или иного действия или предлагает новое техническое решение той или иной задачи».

Патентные тролли. Эти лица ничего не создают и не изобретают; они просто покупают патенты, выдают лицензии другим лицам, а затем судятся с любым лицом, группой или организацией, которые нарушают их приобретенные патентные права.

Патенты на образцы. Форма интеллектуальной собственности, которая включает в себя образцы, создаваемые с конкретной целью быть эстетически привлекательными для потребителей и влияющие на выбор потребителей между товарами. Также известны под названием *промышленные образцы.*

Педофил. Лицо, испытывающее сексуальное влечение к ребенку.

Персонация в сети. Процесс, при котором преступники выдают себя за жертв, создавая учетные записи со схожими именами и используя существующие фотографии жертв.

План действий по урегулированию чрезвычайных ситуаций. План с изложением инструкций, которые необходимо соблюдать, и действий, которые необходимо предпринять в случае возникновения инцидента в области кибербезопасности. Также известен под названием *план непрерывности бизнеса.*

План непрерывности бизнеса. План с изложением инструкций, которые необходимо соблюдать, и действий, которые необходимо предпринять в случае возникновения инцидента в области кибербезопасности. Также известен под названием *план действий по урегулированию чрезвычайных ситуаций.*

Подделка товарных знаков. Преднамеренное несанкционированное использование товарного знака для маркировки товара или услуги, которые не являются товаром или услугой владельца товарного знака.

Поисковая система человеческой плоти. Термин, используемый для описания пользователей Интернета, которые совместными усилиями идентифицируют цель и совершают скоординированное надругательство над ней в Интернете.

Поисковые роботы. Приложения, разработанные для обхода страниц Интернета для достижения конкретных целей.

Поиск по ключевым словам. Поиск на основе терминов, предоставленных следователем.

Показания с чужих слов. Заявления, сделанные вне суда.

Полное раскрытие уязвимостей. Публичное обнародование информации об уязвимостях программного или аппаратного обеспечения на онлайн-форумах или веб-сайтах до того, как эти уязвимости будут устранены.

Поставщики услуг Интернета. Лица, которые предоставляют услуги Интернета компьютерной системе или системе другого цифрового устройства.

Превентивное право. Правовые нормы, сосредоточенные на регулировании и снижении рисков с целью предотвращения преступлений, либо, как минимум, смягчения ущерба, причиняемого в результате совершения

преступлений.

Предвзятость подтверждения. Процесс, во время которого люди ищут и поддерживают результаты, подтверждающее их рабочую гипотезу, и отклоняют результаты, которые противоречат их рабочей гипотезе.

Преступление, совершаемое посредством кибертехнологий. Киберпреступление, которое совершается посредством Интернета и цифровых технологий.

Преступления, связанные с использованием персональных данных. Преступник неправомерно выдает себя другого человека и/или незаконно присваивает себе идентификационные данные жертвы и/или использует эти идентификационные и/или личные данные в незаконных целях.

Прокси-сервер. Промежуточный сервер, который используется для соединения клиента с сервером, с которого клиент запрашивает ресурсы.

Промышленные образцы. Форма интеллектуальной собственности, которая включает в себя образцы, создаваемые с конкретной целью быть эстетически привлекательными для потребителей и влияющие на выбор потребителей между товарами. Также известны под названием *патенты на образцы.*

Промышленные секреты. Ценная информация о бизнес-процессах и деловой практике, которые являются секретными и защищают конкурентные преимущества компании.

Прослеживание в обратном направлении. Процесс прослеживания незаконных действий для установления источника киберпреступления. Также известно как *обратное прослеживание.*

Процессуальное право. Правовые нормы, которые охватывают процессы и процедуры, которые должны соблюдаться при применении норм материального права, правила, позволяющие обеспечить соблюдение норм материального права, а также правила и стандарты в уголовном судопроизводстве.

Процесс цифровой судебной экспертизы. Поиск, извлечение, сохранение и хранение цифровых доказательств; описание, объяснение цифровых доказательств и установление их происхождения и значимости; анализ доказательств и их убедительности, достоверности и относимости к делу; и представление доказательств, имеющих отношение к делу.

Прямая трансляция сексуального насилия над детьми. Трансляция сцен сексуального насилия над детьми в режиме реального времени зрителям, находящимся (зачастую) в отдаленных местах.

Прямое доказательство. Доказательство, которое устанавливает факт.

Псевдонимизация. Процесс, при котором идентифицирующие данные в записи заменяются искусственными идентификаторами.

«Пуленепробиваемый» хостинг. Услуга, которая позволяет преступникам использовать серверы для совершения киберпреступлений, хранить запрещенный контент и защищать запрещенный контент от доступа правоохранительных органов и/или отключения от Интернета.

Пятая сфера. Термин, используемый для описания киберпространства как еще одной сферы ведения боевых действий.

Развитые устойчивые угрозы. Отдельные лица и/или группы лиц, которые постоянно совершают целевые атаки на объект.

Распределенная атака типа «отказ в обслуживании». Использование нескольких компьютеров и других цифровых технологий для проведения скоординированных атак с целью перегрузки серверов для препятствования доступу законным пользователям. Также известна под названием *DDoS-атака.*

Растормаживание. Процесс, при котором человек демонстрирует отсутствие социальных ограничений в отношении поведения в Интернете.

Реконструкция преступления. Процесс, проводимый для того, чтобы установить, *кто* несет ответственность за преступление, *что* произошло, *где* произошло это преступление, *когда* оно произошло, и *как* оно развивалось, путем идентификации, сопоставления и увязывания данных. Также известна пол названием *реконструкция событий.*

Реконструкция событий. Процесс, проводимый для того, чтобы установить, *кто* несет ответственность за событие, *что* произошло, *где* произошло это событие, *когда* оно произошло, и *как* оно развивалось, путем идентификации, сопоставления и увязывания данных. Также известна пол названием *реконструкция преступления.*

Реляционный анализ. Определение участников событий, их действий, а также связей и отношений между ними.

Риск. Воздействие угрозы и вероятность ее возникновения.

Секстинг. Отправка собственных изображений откровенно сексуального характера.

Сексторшн. Форма кибердомогательства, которое совершается, когда преступник угрожает распространить фотографии или видеозаписи жертвы откровенно сексуального характера, если не будут выполнены его требования.

Сексуальная эксплуатация детей в Интернете. Использование информационно-коммуникационных технологий в качестве *средства* для сексуальной эксплуатации детей, когда сексуальное насилие над детьми и/или другие сексуализированные действия с использованием детей предполагают обмен на удовлетворение каких-либо потребностей.

Сексуальное насилие над детьми в Интернете. Использование информационно-коммуникационных технологий в качестве *средства* для сексуального насилия над детьми.

Сексуальное насилие над детьми на заказ. Зрители трансляции сексуального насилия над ребенком могут активно участвовать в насилии, общаясь с ребенком, сексуальным насильником и/или организатором сексуального насилия над ребенком и требуя совершения конкретных физических действий и/или половых актов ребенком и/или в отношении ребенка.

Сексуальное надругательство с использованием изображений. Форма сексуального насилия, при которой преступники намеренно создают,

распространяют или угрожают распространить интимные фото и/или видеозаписи жертв без их согласия. Такое действие может причинить жертве вред и/или каким-то образом принести пользу преступнику (например, денежная выгода, сексуальное удовлетворение, повышение социального статуса и т.д.).

Сетевой нейтралитет. Принцип, требующий одинакового отношения ко всем данным, независимо от источника.

Сдерживание. Препятствование незаконной деятельности через наказание.

Система доменных имен. Обеспечивает доступ к Интернету путем преобразования доменных имен в IP-адрес.

Система обнаружения вторжений. Система обеспечения кибербезопасности, которая позволяет обнаруживать кибератаки, несанкционированный доступ и несанкционированное использование систем, сетей, данных, услуг и соответствующих ресурсов.

Система охраны доказательств. Подробный учет доказательств, их состояния, процессов сбора, хранения, получения доступа и передачи, а также причин получения доступа и передачи, которые имеют важнейшее значение для обеспечения допустимости цифровых доказательств в большинстве судов.

Системы управления технологическими процессами. Системы командования и управления производственными процессами на объектах критически важной инфраструктуры.

Ситуационное предупреждение преступности. Меры, используемые для предотвращения преступлений и сокращения возможностей для их совершения.

Скрипт. Компьютерная программа.

Смишинг. Фишинг с использованием текстовых сообщений. Также известен как *SMS -фишинг*.

Создание неискаженного образа. Создание дубликата содержимого цифрового устройства.

Солипсическая интроекция. Вымышленный образ людей, созданный восприятием пользователей в отношении других людей и их характерных черт в отсутствие реального контакта с ними, включая взаимоотношения, основанные на воображаемой, а не реальной информации.

Состояние дел (потенциал) в области кибербезопасности. Термин, используемый для описания возможностей страны, организации или компании для обеспечения кибербезопасности.

Социальная дилемма. Когда решения основываются скорее на личном интересе, а не на интересе группы или коллектива, даже когда практическая польза от действий в коллективных интересах выше, чем польза от преследования личного интереса.

Социальная инженерия. Тактика, при помощи которой злоумышленник обманом заставляет свою цель раскрыть информацию или совершить иное действие.

Спам. Рассылка незапрашиваемых электронных писем.

Средства контроля доступа. Меры, которые устанавливают привилегии,

определяют санкционированный доступ и предотвращают несанкционированный доступ.

Стандартные оперативные процедуры. Документы, в которых описываются методы и последовательность действий, которые следует соблюдать при расследовании киберпреступления и обращении с цифровыми доказательствами на устройствах информационно-коммуникационных технологий.

Стеганография. Сокрытие секретных данных, когда содержимое сообщения скрывается и делается невидимым.

Суверенитет. Право государства осуществлять полномочия на своей собственной территории.

Судебные поручения. Письменные запросы национальных судов в органы зарубежного государства с просьбой о предоставлении доказательств.

Темная паутина. Часть Всемирной паутины, известная своими веб-сайтами с затрудненным доступом и скрытыми веб-сайтами, на которых осуществляются незаконные действия и реализуются незаконные товары и услуги, и доступ к которым возможен только с помощью специализированного программного обеспечения. Также известна под названием Даркнет.

Теория ожидаемой полезности. Теория, которая гласит, что люди участвуют в каких-либо действиях, когда ожидаемая полезность от этих действий превосходит ожидаемую полезность участия в других действиях.

Теория «прививки». Эта теория гласит, что способ сделать людей невосприимчивыми к попыткам убеждения, предпринимаемым другими людьми, состоит в том, чтобы подвергнуть их этим попыткам и дать им инструменты, необходимые для противодействия этим попыткам.

Теория рутинной деятельности. Теория, которая гласит, что преступление совершается в том случае, когда присутствуют два элемента - *мотивированный преступник* и *подходящая цель*, и когда отсутствует один элемент - *дееспособный защитник*.

Территориальный суверенитет. Полное и исключительное осуществление государством своих прав и полномочий в отношении своей географической территории.

Техника нейтрализации. Методы, используемые для преодоления или минимизации негативных эмоций, связанных с вовлечением в незаконную деятельность.

Товарные знаки. Идентификаторы, которые позволяют отличать товары или услуги одних источников от других.

Торговля детьми в целях сексуальной эксплуатации. Действие, которое предполагает вербовку детей, ведет к коммерческой сексуальной эксплуатации детей, является ее причиной, поддерживает ее и/или иным образом способствует ей.

Троянский конь. Вредоносная программа, маскирующаяся под легитимное программное обеспечение, чтобы обманом заставить пользователя загрузить программу, которая заражает систему пользователей с целью шпионажа,

кражи и/или причинение вреда.
Угроза. Обстоятельство, которое может причинить вред.
Удобство использования. Легкость, с которой могут использоваться цифровые устройства.
Управление Интернетом. Разработка и применение принципов, правил, процедур работы Интернета различными субъектами для регулирования использования Интернета и его развития.
Управление знаниями. Выявление и оценка потребностей в знаниях и использование ресурсов знаний.
Управление учетными данными. Процесс аутентификации идентификационных данных пользователей, идентификации соответствующих привилегий и предоставления доступа пользователям на основе этих привилегий.
Уровень проникновения Интернета. Доля населения определенного региона, которые используют Интернет.
Устойчивость. Способность выдерживать сбои, адаптироваться к изменяющимся условиям и восстанавливаться после инцидентов с ИКТ, а также защищать конфиденциальность, целостность и доступность систем, сетей, сервисов и данных.
Уэйлинг. Метод, при помощи которого преступники выдают себя за высокопоставленных руководителей компании, юристов, бухгалтеров и других лиц, занимающих руководящие и ответственные должности, чтобы обманом вынудить сотрудников отправить им денежные средства.
Уязвимость. Подверженность вреду.
Уязвимость нулевого дня. Ранее неизвестные уязвимости, которые эксплуатируются после их обнаружения.
Фальшивые новости. Пропаганда и дезинформация, распространяемые под видом реальных новостей.
Фарминг. Создание поддельного, дублирующего веб-сайта, который предназначен для того, чтобы обманом заставить пользователей вводить свои учетные данные для входа.
Физическое извлечение. Поиск и получение доказательств из такого места в цифровом устройстве, в котором хранятся доказательства.
Фишинг. Рассылка электронных писем, содержащих ссылку на веб-сайт, при нажатии на которую пользователи могут либо загрузить вредоносную программу в свои цифровые устройства, либо могут быть перенаправлены на вредоносный веб-сайт, созданный для кражи учетных данных пользователей.
Функциональный анализ. Оценка производительности и возможностей систем и устройств, задействованных во время событий.
Хакерская атака. Несанкционированный доступ к системам, сетям и данным.
«Хозяин» бот-сети. Лицо, контролирующее зараженные цифровые устройства.
Хэш. Сгенерированное значение.
Целевой фишинг. Отправка электронных писем с зараженными вложениями или ссылками, чтобы вынудить получателя открыть приложение или нажать

на ссылку.

Целостность. Данные являются точными и достоверными и не подвергались изменениям.

Цензура. Запрет на распространение информации, визуальных изображений и письменных или устных сообщений, которые запрещены законом, и/или их пресечение со стороны правительства, сообщества или группы, поскольку они являются незаконными и/или рассматриваются как вредные, непопулярные, нежелательные или политически некорректные.

Цифровая антикриминалистика. Инструменты и методы, используемые для того, чтобы запутать расследование киберпреступлений и затрудняет усилия по проведению цифровой судебной экспертизы. Также известна под названием *антикриминалистика*.

Цифровая криминалистика. Отрасль криминалистики, которая применяет вопросы права к информационно-коммуникационным технологиям и цифровым устройствам.

Цифровое пиратство. Незаконная загрузка фильмов с веб-сайта третьей стороны без получения права на распространение произведений, охраняемых авторским правом.

Цифровые доказательства. Данные, полученные из устройств информационно-коммуникационных технологий. Также известны под названием *электронные доказательства*.

Цифровые отпечатки. Данные, оставленные пользователями ИКТ, которые могут раскрыть сведения о них, включая информацию о возрасте, половой, расовой и этнической принадлежности, гражданстве, сексуальной ориентации, мыслях, предпочтениях, привычках, хобби, истории болезни и проблемах здоровья, психологических расстройствах, статусе занятости, принадлежности к какому-либо сообществу, отношениях, геолокации, распорядке дня и прочей активности.

«Червь». Автономная вредоносная программа, которая распространяется без участия пользователя.

Шифрование. Мера, которая блокирует доступ третьих лиц к информации и сообщениям пользователей.

Шпионская программа. Вредоносное программное обеспечение, предназначенное для тайного мониторинга зараженных систем, а также сбора и передачи информации создателю и/или пользователю шпионской программы.

Электронные доказательства. Данные, полученные из устройств информационно-коммуникационных технологий. Также известны под названием *цифровые доказательства*.

Юрисдикция. Право и полномочия государства применять законы и назначать наказание за несоблюдение законов.

Data mining. Извлечение информации из наборов данных.

DDoS-атака. Использование нескольких компьютеров и других цифровых технологий для проведения скоординированных атак с целью перегрузки серверов для препятствования доступу законным пользователям. Также

известна под названием *распределенная атака типа «отказ в обслуживании».*

DoS-атака. Киберпреступление, которое создает помехи системам, перегружая серверы запросами, чтобы препятствовать доступу законного трафика к сайту и/или использованию системы. Также известна под названием *атака типа «отказ в обслуживании».*

Doxware (шифровальщик-вымогатель). Разновидность криптовымогателя, которую злоумышленники используют против жертв, угрожая разглашением данных пользователя, если не будет выплачен выкуп за предоставление кода для расшифровки файлов и данных.

eDiscovery (поиск электронных документов). Процесс поиска, идентификации и сохранения цифровых данных для использования в качестве доказательств в судебном процессе.

IP-адрес. Уникальный идентификатор, присваиваемый подключенному к Интернету цифровому устройству поставщиком услуг Интернета для подключения к сети. Также известен под названием *адрес Интернет-протокола.*

SMS-фишинг. Фишинг с использованием текстовых сообщений. Также известен как *смишинг.*

Stalkerware. Одна из разновидностей шпионского программного обеспечения, которое может запускаться на компьютере, смартфоне или ином цифровом устройстве, подключенном к Интернету, и собирать и передавать данные обо всех действиях пользователя на этих устройствах - начиная с данных об отправленных и полученных электронных и текстовых сообщениях и заканчивая информацией о снятых фотографиях и нажатиях клавиш.

Литература:

1. Масалков А.С. Особенности киберпреступлении в России. Издательство: ДМК-Пресс, 2018. - 226 б. https: //www.labirint.ru/books/626293/
2. Клаверов В.Б. Современная киберпреступность. Изд: LAP Lambert Academic Publishing, 2012. - 92 б.
3. Исмагулова А.Т. Уголовные правонарушения в сфере информатизации и связи в Республике Казахстан: монография / А.Т. Исмагулова, А.М. Галиаскарова; Костанайский филиал ФГБОУ ВПО «Челябинский государственный университет». - Костанай: ТОО «New Line Media», 2016. - 160 б.
4. УНП ООН (2013). Draft Comprehensive Study on Cybercrime.
5. Segal, Mark (2013). How to Train: A Practical Guide for Training and Working with Others.
6. Weiping Chang, Peifang Chung. Knowledge Management in Cybercrime Investigation – A Case Study of Identifying Cybercrime Investigation Knowledge in Taiwan. PAISI 2014: Intelligence and Security Informatics /https://link.springer.com/book/10.1007/978-3-319-06677-6
7. Berliner, Lucy and Jon R. Conte (1990). The process of victimization: A victims' perspective. Child Abuse & Neglect, Vol. 14(1), 29-40. https://www.sciencedirect.com/science/article/abs/pii/0145213490900788
8. O'Connell, Rachel. (2003). A typology of cyber sexploitation and online grooming practices. Cyberspace Research Unit: University of Central Lancashire. http://image.guardian.co.uk/sysfiles/Society/documents/2003/07/17/Groomingreport.pdf
9. Ospina, Maria, Christa Harstall, and Liz Dennet (2010). Sexual exploitation of children and youth over the internet: A rapid review of the scientific literature. Alberta, Canada: Institute of Health Economics. https://era.library.ualberta.ca/items/d45bd9d4-2c28-4172-8f91 c529e8d96df7/view/7b0416bb-843f-4492-a872 2388ed56bec2/sexual_exploitation_of_children_and_youth_over_the_internet_a_rapid_review_of_the_scientific_literature-20(1).pdf
10. UNODC, 2011 (Всемирный доклад о наркотиках, 2011 г.). https://www.unodc.org/unodc/en/data-and-analysis/WDR-2011.html
11. UNODC, 2012 (Всемирный доклад о наркотиках, 2012 г.) https://www.unodc.org/unodc/en/data-and-analysis/WDR-2012.html
12. UNODC, 2014. https://www.unodc.org/documents/AnnualReport 2014/ Annual_Report_2014_WEB.pdf
13. UNODC, 2015./https://www.unodc.org/wdr2015/

14. Maras 2014. 4th International Conference on Mobile, Adaptable and Rapidly Assembled Structures 11-13 June 2014. Ostend, Belgium. https://www.wessex.ac.uk/conferences/2014/maras-2014
15. Maras 2016. 5th International Conference on Mobile, Adaptable and Rapidly Assembled Structures. 21-23 September 2016 Siena, Italy. https://www.wessex.ac.uk/conferences/2016/maras-2016.
16. Susan W. Brenner, Bert-Jaap Koops. Approaches to Cybercrime Jurisdiction. Journal of High Technology Law, Vol. 4, No. 1, 2004. 46 p. Posted: 25 Aug 2005. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=786507
17. Policing image-based sexual abuse: stakeholder perspectives. Nicola Henry, Asher Flynn, Anastasia Powell. Pages 565-581/Published online: 20 Sep 2018. https://www.researchgate.net/publication/327794543_Policing_image based_sexual_abuse_stakeholder_perspectives
18. Maras and Miranda, January 2014. Forensic Science in book: Encyclopedia of Law and Economics, pp.1-6. /https://www.researchgate.net/publication/ 304088810_Forensic_Science
19. Cognitive Bias and Blindness: A Global Survey of Forensic Science Examiners Jeff Kukuckaa, Saul M. Kassinb, Patricia A. Zapfb, Itiel E. Dror. Journal of Applied Research in Memory and Cognition. Volume 6, Issue 4, December 2017. /https://www.sciencedirect.com/science/article/ abs/pii/ S2211368117300323?via%3Dihub.
20. A survey of mutual legal assistance involving digital evidence. Joshua I.James, PavelGladyshev. Digital Investigation. Volume 18, September 2016. /https://dl.acm.org/doi/abs/10.1016/j.diin.2016.06.004
21. International Law Enforcement Access to User Data: A Survival Guide and Call for Action. Kate Westmoreland Gail Kent. Home > JOURNALS > CJLT > Vol. 13 (2015) > No.2./ https://digitalcommons.schulichlaw.dal. ca/cjlt/ vol13/iss2/5/
22. Crime, Security and Information Communication Technologies: The Changing Cybersecurity Threat Landscape and Its Implications for Regulation and Policing. 22 Pages Posted: 25 Jul 2017. David S. Wall./https://papers.ssrn.com/sol3/papers. cfm?abstract_id=3005872
21. International Telecommunication Union, ITU,2012. Understanding cybercrime: phenomena, challenges and legal response /https://www.itu.int/en/ITU D/Statistics/Documents/publications/mis2012 /MIS2012_without_Annex_4.pdf
23. Understanding cybercrime: phenomena, challenges and legal response (pp. 11-33).2014. /https://www.itu.int/en/ITU-D/Cybersecurity/Documents /cybercrime2014.pdf
24. Statcounter, 2016. /http://www.oszone.net/29945/StatCounter_ August_2016_OS_stats
25. Bilge, L. and Dumitras, T. (2012) Before We Knew It: An Empirical Study of Zero-Day Attacks in the Real World. Proceedings of the 2012 ACM Conference on Computer and Communications Security, Raleigh, 16-18 October 2012, 833-844. /https://doi.org/10.1145/2382196.2382284
26. Henry, Flynn and Powell, 2018 https://doi.org/10.1080/15614263.2018.

1507892
27. Broadhurst et al., 2014. /https://www.researchgate.net/publication/288262190_Organizations_and_cyber_crime_An_analysis_of_the_nature_of_groups_engaged_in_cyber_crime
28. Broadhurst et al., 2018./https://link.springer.com/article/10.1007/s11306-018-1367-3
29. ITU 2008. https://www.itu.int/council/C2008/index.html
30. ITU 2012. https://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2012/MIS2012_without_Annex_4.pdf
31. ITU 2017. https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2017.pdf
32. ITU 2018. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf
33. Morgan et al., 2016. /https://bmcpublichealth.biomedcentral.com/articles/10.1186/s12889-016-2882-7
34. UNSCR 1624 /2005. https://digitallibrary.un.org/record/556538?ln=ru 28. UN-CCPCJ, 2017. /https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_26/E_CN15_2017_CRP4_e_V1703636.pdf
35. OCCRP, 2016; Reuters, 2016. /https://www.reuters.com/article/europe-moneylaundering-idUKL3N20T2PD
36. Leukfeldt, Kleemans, and Stol, 2017; Leukfeldt, Lavorgna, және Kleemans, 2017, 292-293 бб. /https://journals.sagepub.com/doi/abs/10.1177/0002764217734267
37. Leukfeldt, Lavorgna and Kleemans, 2017. /https://www.cybercrimeworkingroup.com/rutger-leukfeldt
38. Hern, 2017. /https://www-theguardian-com.translate.goog/technology/2017/aug/01/data-browsing-habits-brokers?_x_tr_sl=en&_x_tr_tl=ru&_x_tr_hl=ru&_x_tr_pto=sc
39. Bilge and Dumitras, 2012. /https://www.scirp.org/(S(i43dyn45teexjx455qlt3d2q))/reference/ReferencesPapers.aspx?ReferenceID=2024179
40. Henry, Flynn and Powell, 2018, 566 p. /https://www.researchgate.net/publication/327794543_Policing_image-based_sexual_abuse_stakeholder_perspectives
41. Morgan et al., 2016 /https://bmcpublichealth.biomedcentral.com/articles/10.1186/s12889-016-2882-7
42. NIST, 2018. /https://www.nist.gov/publications/2018-national-institute-standards-and-technology-environmental-scan
43. NIST, 2012. /https://csrc.nist.gov/News/2012/NIST-Special-Publication-800-30-Revision-1
44. Hubbard and Seiersen, 2016. /https://www.amazon.com/How-Measure-Anything-Cybersecurity-Risk/dp/1536669741
45. Lehtinen, Russell, Gangemi Sr., 2006. /https://books.google.kz/books/about/Computer_ Security_Basics.html?id=DyrLV0kZEd8C&redir_esc=y
46. Cornish and Clarke, 2003. /https://popcenter.asu.edu/sites/default/files/Responses/ crime_prevention/PDFs/Cornish%26Clarke.pdf

47. Clarke, 2004. /http://www.sciepub.com/reference/203861
48. Reuters, 2017. /https://reutersinstitute.politics.ox.ac.uk/sites/default/files/Digital%20News%20Report%202017%20web_0.pdf
49. Reuters, 2018. https://www.digitalnewsreport.org/survey/2018/
50. Henry, Flynn and Powell, 2017. /https://reutersinstitute.politics.ox.ac.uk/sites/default/files/Digital%20News%20Report%202017%20web_0.pdf
51. Henry, Flynn and Powell, 2018. /https://www.tandfonline.com/doi/abs/10.1080/15614263.2018.1507892
52. Varese, 2010 / https://www.routledge.com/Organized-Crime/Varese/p/book/9780415460743
53. United States v. Ross William Ulbricht, Criminal Complaint, 2013. /https://caselaw.findlaw.com/us-2nd-circuit/1862572.html
54. Newman, 2018./https://global.oup.com/academic/product/networks-9780198805090?cc=us&lang=en&#
55. Morgan, 2018. /https://www.jpmorgan.com/solutions/cib/insights/health-care-conference
56. Alvarez, Hall, and Hyde, 2008 /https://www.jstor.org/stable/41403728
57. McGuire and Dowling, 2013. /https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf
58. Europol, 2018./ https://www.europol.europa.eu/activities-services/main-reports/europol-in-brief-2018.
59. Read et al., 2016. /https://agupubs.onlinelibrary.wiley.com /doi/10.1002/2016WR019993
60. Conrad, Dorn, and Craiger, 2010. /https://commons.erau.edu/publication/999/
61. Casey, Ferraro, and Nguyen, 2009. /https://www.researchgate.net/publication/26819089_Investigation_Delayed_Is_Justice_Denied_Proposals_for_Expediting_Forensic_Examinations_of_Digital_Evidence.
62. Tcherni et al., 2016./https://www.researchgate.net/publication/305630752_Reasons_for_Gaps_in_Crime_Reporting_The_Case_of_White-Collar_Criminals_Investigated_by_Private_Fraud_Examiners_in_Norway
63. Smeets, 2018. /https://econpapers.repec.org/paper/zbwwtowps/ersd201803.htm
64. Kallender and Hughes, 2017. /https://www.tandfonline.com/doi/abs/10.1080/01402390.2016.1233493
65. Brenner and Koops, 2004. /https://papers.ssrn.com/sol3/papers.cfm?abstract_id=786507
66. Frischmann, 2003. /https://lawecommons.luc.edu/luclj/vol35/iss1/8/
67. Kerr, 2003, /https://www.unodc.org/e4j/data/university_uni/the_problem_of_perspective_in_internet_law.html?lng=en
68. Report of the Working Group on Internet Governance. Château de Bossey. June 2005. (WGIG, 2005). /https://www.wgig.org/docs/WGIGREPORT.pdf
69. Enisa 2014. https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014
70. Enisa 2017./ https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017

71. NIST 2012./ https://csrc.nist.gov/News/2012/NIST-Special-Publication-800-30-Revision-1
72. NIST 2018. /https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework
73. Leukfeldt et al., 2017. /https://www.researchgate.net/publication/320323730_The_Use_of_Online_Crime_Markets_by_Cybercriminal_Networks_A_View_From_Within
74. Leukfeldt, Lavorgna, and Kleemans, 2017. /https://www.researchgate.net/publication/309960777_Organised_Cybercrime_or_Cybercrime_that_is_Organised_An_Assessment_of_the_Conceptualisation_of_Financial_Cybercrime_as_Organised_Crime
75. Arsovska, 2011./ https://journals.sagepub.com/doi/abs/10.1177/0094306110391764l
76. Whiteman, 2012. /https://www.tandfonline.com/doi/abs/10.1080/14780887.2015.1008913