СЕРИЯ УНИВЕРСИТЕТСКИХ МОДУЛЕЙ

Киберпреступность **1**

ВВЕДЕНИЕ В КИБЕРПРЕСТУПНОСТЬ

UNODC

Дохинская декларация:
ПООЩРЕНИЕ КУЛЬТУРЫ
СОБЛЮДЕНИЯ ЗАКОННОСТИ

образование для правосудия

Управление Организации Объединенных Наций по наркотикам и преступности

ОБРАЗОВАНИЕ ВО ИМЯ ПРАВОСУДИЯ
СЕРИЯ УНИВЕРСИТЕТСКИХ МОДУЛЕЙ

КИБЕРПРЕСТУПНОСТЬ

Модуль 1

ВВЕДЕНИЕ В КИБЕРПРЕСТУПНОСТЬ

Организация Объединенных Наций
Вéна, 2019

Этот модуль является ресурсом для преподавателей.

Этот модуль, разработанный в рамках инициативы «Образование для Правосудия»(E4J), являющейся компонентом Глобальной программы по осуществлению Дохинской декларации, Управления Организации Объединенных Наций по наркотикам и преступности (УНП ООН) и является частью серии учебных модулей «Образование для правосудия» (E4J) по Киберпреступности и сопровождается учебным пособием. Полный спектр материалов «Образование для правосудия» E4J включает в себя университетские модули по вопросам честности и этики, предупреждения преступности и уголовного правосудия, борьбы с коррупцией, организованной преступности, торговли людьми / незаконного ввоза мигрантов, огнестрельного оружия, охраны дикой природы, лесных и рыболовных преступлений, борьбы с терроризмом, а также киберпреступность.

Все модули в серии модулей университета «Образование для правосудия» E4J содержат предложения для выполнения в классе упражнений, оценки учащихся, слайды и другие учебные пособия, которые преподаватели могут адаптировать к своему контексту и интегрировать в существующую учебную программу. Модуль предоставляет план для трехчасового занятия, но может использоваться для более коротких или более длительных занятий.

Все университетские модули «Образование для правосудия» E4J участвуют в действующих научных исследованиях и дебатах и могут содержать информацию, мнения и заявления из различных источников, включая сообщения прессы и независимых экспертов. Ссылки на внешние ресурсы были проверены на момент публикации. Однако, поскольку сторонние веб-сайты могут измениться, пожалуйста *contact us*, если вы столкнулись с неработающей ссылкой или перенаправлены на неприемлемый контент. Также сообщите нам, если вы заметили, что публикация связана с неофициальной версией или веб-сайтом.

Несмотря на то, что были приложены все усилия для обеспечения точного перевода модуля, обратите внимание, что модуль на английском языке является утвержденной версией. Поэтому в случае сомнений, пожалуйста, обратитесь к первоисточнику в английской версии.

Ознакомиться с условиями использования Модуля можно на *веб-сайте E4J*.

© Организация Объединенных Наций, 2019. Все права защищены.

Используемые обозначения и представление материалов в этой публикации не подразумевают выражения какого-либо мнения со стороны Секретариата Организации Объединенных Наций относительно правового статуса какой-либо страны, территории, города или района или ее органов власти, или относительно разграничения его границ.

Данная публикация не была официально редактирована.

Оглавле́ние

Введение 2

Результаты обучения 2

Основные вопросы 3

Основы компьютерных технологий 3

Глобальные тенденции в области использования технологий и подключения к Интернету 6

Кратко о киберпреступности 9

Тенденции в области киберпреступности 11

Технические проблемы 13

Правовые проблемы 15

Этические проблемы 15

Оперативные проблемы 16

Предупреждение киберпреступности 17

Заключение 18

Список использованной литературы 18

Упражнения 22

Упражнение №.1: Правовые определения компьютера, данных и сети 22

Упражнение №.2: Скорости загрузки веб-страниц 22

Упражнение №.3: Уровни проникновения Интернета 23

Упражнение №.4: Расследования случаев утечки данных 23

Возможная структура занятия 24

Список основной литературы 27

Список дополнительной литературы 28

Оценка учащихся 29

Обзорные вопросы 29

Домашние задания 29

Дополнительные средства обучения 30

Видео 30

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 модуле 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 модуля, содержится обзор ключевых понятий, основных терминов и определений, а также общие сведения о киберпреступности, связанных с ней проблемах и мерах по ее предупреждению.

Результаты обучения

- Определить и описать основные понятия, относящиеся к компьютерным технологиям
- Описать и оценить глобальные тенденции в области использования технологий и подключения к Интернету
- Дать определение киберпреступности и обсудить, почему проблема киберпреступности изучается с научной точки зрения
- Обсудить и проанализировать тенденции в области киберпреступности
- Определить, изучить, и проанализировать проблемы технического, правового, этического и оперативного характера, связанные с расследованием киберпреступлений и предупреждением киберпреступности

Основные вопросы

Данный модуль, являющийся первым модулем в Серии университетских модулей по киберпреступности, начинается с краткой вводной информации о киберпреступности. Вначале обсуждаются ключевые понятия, относящиеся к компьютерным технологиям. Затем рассматриваются вопросы, связанные с глобальным использованием технологий и подключением к Интернету, а также определением понятия киберпреступности и исследованием тенденций в области киберпреступности. Кроме того, в Модуле кратко представлены некоторые теории, которые используются для объяснения конкретных форм киберпреступности, а также некоторые технические, правовые, этические и оперативные проблемы, связанные с киберпреступностью. Наконец, в модуле рассматриваются вопросы предупреждения киберпреступности.

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 (Maras, 2015; для получения дополнительной информации об Интернете вещей см. Модуль 10 серии модулей по киберпреступности: «Конфиденциальность и защита данных»), 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».

> *Примечание*
>
> Здесь мы пытаемся определить *основы компьютерных технологий*. Цель состоит в том, чтобы ваши учащиеся имели общее представление об инженерной стороне компьютерных технологий (как работают компьютеры), а также о том, какие определения компьютерных систем используются в различных правовых системах.

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

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). (Maras, 2014, с. 385). *Система доменных имен* (DNS) обеспечивает доступ к Интернету путем преобразования доменных имен в IP-адрес.

> *Хотите знать больше?*
>
> Азиатско-Тихоокеанский сетевой информационный центр (APNIC) предлагает бесплатный технический курс обучения по DNS: https://training.apnic.net/courses/wdns01-dns-concepts/

Как только мы получим общее представление о компьютерной системе, компьютерных данных, поставщиках услуг, данных о трафике и прочих понятиях, относящихся к компьютерным технологиям, мы сможем понять, как их можно использовать для торговли, общения и совершения преступлений.

Глобальные тенденции в области использования технологий и подключения к Интернету

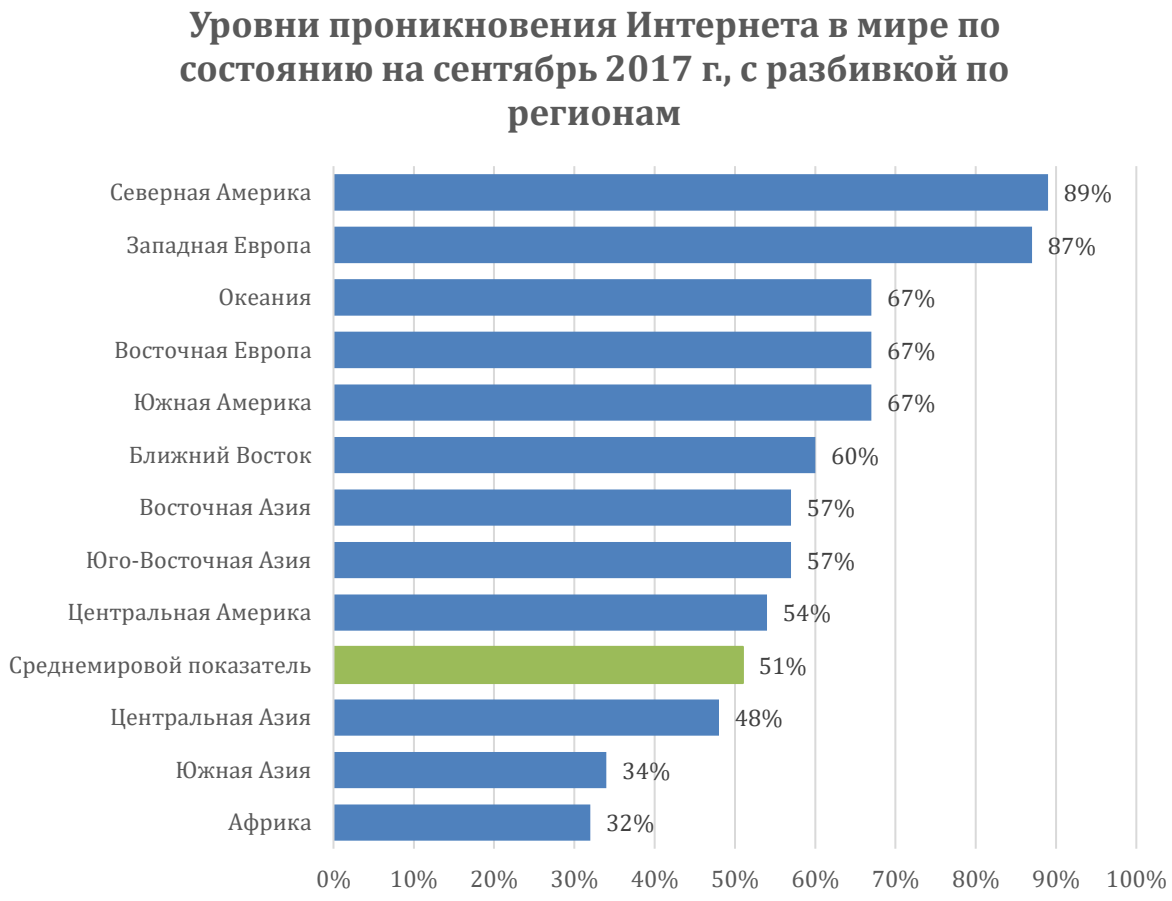
На Земле существует очень мало мест, где вы не сможете получить доступ к Интернету. В большинстве стран есть, как минимум, один поставщик Интернет-услуг, который предоставляет сетевую инфраструктуру (аппаратное обеспечение, такое как оборудование, кабели и беспроводной доступ) для крупных городов. Даже 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 (Statista, 2018). Благодаря доступности Интернет-услуг через

мобильные устройства, использование Интернета неуклонно растет (Statista, 2018). 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% (Statista, 2018). 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).

Рисунок 1



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/.

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» (p. 7). 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.). 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.

Кратко о 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 (e.g., Goodman, and Brenner, 2002; Wall, 2007; Wilson, 2008; 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; для получения информации о различных видах киберпреступности см. Модуль 2 Серии модулей по киберпреступности: «Основные виды киберпреступности»).

Европол (2018) 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 М.О.; 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. Эти категории киберпреступности и виды киберпреступлений, которые подпадают под эти категории, более подробно рассматриваются в Модуле 2 Серии модулей по киберпреступности: «Основные виды киберпреступности».

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 (Wall, 2007). 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 (Jaishankar, 2011; Chapter 11, Holt, Bossler, and Seigfried-Spellar, 2018; см. также: Chapters 5-9, Maras, 2016 для ознакомления с обзором исследований киберпреступности с точки зрения различных дисциплин). 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; см. также Модуль 6 Серии модулей по организованной преступности: «Причины и движущие факторы организованной преступности» для получения информации о некоторых из этих теорий). В других работах изучалась роль «пространства» в киберпреступности, в частности, роль онлайн-пространств и онлайн-сообществ в культурной трансмиссии преступных и/или криминальных ценностей (Evans, 2001; см. также Chapter 6, Maras, 2016). 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).

Примечание

Серия университетских модулей по киберпреступности, разработанная в рамках инициативы «Образование во имя правосудия» (E4J), охватывает применение некоторых из этих теорий киберпреступности и вопросы, связанные с киберпреступностью, в Модуле 5 «Расследование киберпреступлений», в Модуле 8 «Кибербезопасность и предупреждение киберпреступности: стратегии, политика и программы», Модуле 9 «Кибербезопасность и предупреждение киберпреступности: практические методы и меры», Модуле 11 «Преступления в сфере интеллектуальной собственности, совершаемые посредством кибертехнологий», и Модуле 12 «Киберпреступления против личности». Существует слишком много теорий, чтобы можно было их охватить в обзорах тем, предусмотренных в Серии модулей по киберпреступности. Однако исследования, проведенные специалистами различных дисциплин, включены в списки основной и дополнительной литературы, подобранные для Серии модулей по киберпреступности, и доступны для ознакомления, а материалы этих исследований могут быть включены в лекционный материал, разработанный на основе этих модулей.

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.

Знаете ли вы?

Африканский союз, Соединенные Штаты и Symantec являются участниками Инициативы «Глобальный форум по киберэкспертизе» (GFCE), который опубликовал свой первый отчет о тенденциях в области киберпреступности и кибербезопасности в 2017 году.

Хотите знать больше?

https://www.thegfce.com/initiatives/c/cybersecurity-and-cybercrime-trends-in-africa

Отчеты о тенденциях в области киберпреступности и кибербезопасности публикуют и другие организации; например, см. Europol. Trends and Routes. https://www.europol.europa.eu/crime-areas-and-trends/trends-and-routes#fndtn-tabs-0-bottom-2.

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 (TrendMicro, 2018). 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 WannaCry 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.

> *Примечание*
>
> Достоверность данных, используемых для определения тенденций, также варьирует в зависимости от конкретного агентства и организации. При составлении отчетов о тенденциях может возникать конфликт интересов, если компании продают средства обеспечения кибербезопасности, которые могут использоваться людьми для защиты от киберпреступлений, определенных в качестве тенденций.

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.

Технические проблемы

Существует несколько технических причин, которые затрудняют борьбу с киберпреступностью. Первая причина – *атрибуция* (для получения дополнительной информации см. Модуль 5 Серии модулей по киберпреступности: «Расследование киберпреступлений»). Любой компьютер, подключенный к Интернету, может взаимодействовать с любым другим компьютером, подключенным к Интернету. Обычно мы видим общедоступный *IP-адрес* компьютера (Cisco, 2016), 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 (для получения дополнительной информации об этих инструментах и Даркнете см. Модуль 5 Серии модулей по киберпреступности: «Расследование киберпреступлений»).

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* (Securelist, 2018). 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»; для получения дополнительной информации см. Zetter, 2014). 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» (p. 1). 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 (Timberg, et al., 2017). 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 (эти трудности рассматриваются в Модуле 9 Серии модулей по киберпреступности: «Кибербезопасность и предупреждение киберпреступности: практические методы и меры»).

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 (правовые проблемы, связанные с облачными данными, более подробно рассматриваются в Модуле 7 Серии модулей по киберпреступности: «Международное сотрудничество в борьбе с киберпреступностью»).

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. Эти правовые проблемы более подробно рассматриваются в Модуле 3 Серии модулей по киберпреступности: «Правовая база и права человека» и Модуле 10 Серии модулей по киберпреступности: «Конфиденциальность и защита данных».

Этические проблемы

Правоохранительные органы (рассматриваются в Модуле 5 Серии модулей по киберпреступности: «Расследование киберпреступлений») должны соблюдать правовые и этические нормы при расследовании преступлений (и киберпреступлений), обработке, анализе и толковании доказательств (см. Модуль 6 Серии модулей по киберпреступности: «Практические аспекты расследования киберпреступлений и цифровой криминалистики»). 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 (для получения дополнительной информации о важности честности, неподкупности и этики см. также Серию университетских модулей по честности, неподкупности и этике, разработанную в рамках инициативы «Образование во имя правосудия» (E4J)). 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 (AMA, 2018).

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 (для получения информации о различиях и связи между этикой и правом просьба ознакомиться с Модулем 12 Серии университетских модулей по честности, неподкупности и этике: «Честность и неподкупность, этика и право»).

Оперативные проблемы

Одна из ключевых оперативных проблем при расследовании киберпреступлений связана с сотрудничеством с другими странами. Международное сотрудничество в расследовании киберпреступлений требует унификации законодательства в сотрудничающих странах (для получения дополнительной информации см. Модуль 11 Серии университетских модулей по организованной преступности, разработанной в рамках инициативы E4J). Такие инструменты, как *договоры о взаимной правовой помощи* (т.е. соглашения, в рамках которых стороны соглашаются сотрудничать в расследовании и судебном преследовании правонарушений, уголовно наказуемых в соответствии с их

национальными законодательствами; Garcia & Doyle 2010; Maras, 2016), могут использоваться для направления официальных запросов об оказании помощи из одной страны в другую. Однако запросы об оказании правовой помощи могут занимать много времени и могут не привести к достижению приемлемых результатов, таких как предупреждение преступления или предоставление доказательств для использования в суде. Оперативные проблемы более подробно рассматриваются в Модуле 7 Серии модулей по киберпреступности: «Международное сотрудничество в борьбе с киберпреступностью». Оперативные проблемы также возникают из-за нехватки национального потенциала (особенно в развивающихся странах), необходимого для борьбы с киберпреступностью (см. Модуль 5 Серии модулей по киберпреступности: «Расследование киберпреступлений», Модуль 7 Серии модулей по киберпреступности: «Международное сотрудничество в борьбе с киберпреступностью» и Модуль 8 Серии модулей по киберпреступности: «Кибербезопасность и предупреждение киберпреступности: стратегии, политика и программы»).

Предупреждение киберпреступности

Киберпреступники зачастую используют как технические, так и социальные подходы к совершению преступлений. Некоторые виды киберпреступности трудно предотвратить, однако пользователи технологий могут предпринимать определенные действия, чтобы защитить себя (в какой-то степени) от киберпреступности.

Европол (2018) размещает многочисленные руководства по информированию общественности и профилактике преступности на своем веб-сайте. Тем не менее, даже маленькие действия способны привнести большие перемены. Ниже приведены некоторые советы, которые следует учитывать при подключении к Интернету.

- Регулярно обновляйте операционную систему и установленное программное обеспечение
- Регулярно удаляйте программное обеспечение, которое вы больше не используете
- Используйте антивирусную программу, разработанную компанией с хорошей репутацией
- Не загружайте программное обеспечение, фильмы или музыку с сайтов общего доступа – они часто имеют вредоносную программу
- Не загружайте вложения и не нажимайте на ссылки от неопознанных отправителей
- Не вводите личную информацию на неизвестных веб-сайтах
- Подтвердите правильность адреса веб-сайта при вводе финансовой информации

Вопросы предупреждения киберпреступности более подробно рассматривается в Модуле 9 Серии модулей по киберпреступности: «Кибербезопасность и предупреждение киберпреступности: практические методы и меры».

Заключение

В данном модуле была представлена вводная информация о киберпреступности, связанных с ней концепциях и проблемах, возникающих при расследовании киберпреступлений и предупреждении киберпреступности. Кроме того, были представлены некоторые понятия, темы и проблемы, которые более подробно рассматриваются в других модулях Серии модулей по киберпреступности. Тенденции, рассмотренные в данном модуле, дают лишь краткий обзор угроз киберпреступности, с которыми сталкиваются страны сегодня. Новые технологии и меры безопасности и профилактики влияют на будущие тенденции в области киберпреступности. Модуль 2 серии модулей по киберпреступности: «Основные виды киберпреступности» охватывает категории киберпреступности и виды киберпреступлений, которые подпадают под эти категории.

Список использованной литературы

- American Marketing Association. The Murky Ethics of Data Gathering in a Post-Cambridge Analytica World. *The Medium*, 31 May 2018. https://medium.com/ama-marketing-news/the-murky-ethics-of-data-gathering-in-a-post-cambridge-analytica-world-33848084bc4a
- Asia-Pacific Network Information Center (APNIC). (2018) WDNS01: DNS Concepts. Workshop. https://training.apnic.net/courses/wdns01-dns-concepts/
- Bilge, Leyla and Tudor Dumitras. (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. https://users.ece.cmu.edu/~tdumitra/public_documents/bilge12_zero_day.pdf.
- China Internet Network Information Center. The 41st Statistical Report on Internet Development in China (January 2018). https://cnnic.com.cn/IDR/ReportDownloads/201807/P020180711391069195909.pdf.
- Cisco. (2016) IP Addressing and Subnetting for New Users. Cisco. https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html

- Council of Europe. (2001) Convention on Cybercrime. Budapest. http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf.
- Cybercrime Convention Committee (2012). T-CY Guidance Note # 1. On the notion of computer system. Article 1(a) Budapest Conception on Cybercrime. Adopted by the T-CY at its 8th Plenary (December 2012). https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e79e6.
- Directorate General For Internal Policies Policy Department C: Citizens' Rights and Constitutional Affairs (2015). The Law Enforcement Challenges of Cybercrime: Are we really catching up? http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536471/IPOL_STU(2015)536471_EN.pdf
- Europol. (2017). Internet Organised Crime Threat Assessment 2017. https://www.europol.europa.eu/iocta/2017/index.html.
- Europol. (2018). Internet Organised Crime Threat Assessment 2018. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018.
- Europol. (2018). Public Awareness and Prevention Guides. https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/online-sex
- Fisher, Tim. (2018) Free and Public DNS Servers. Lifewire. https://www.lifewire.com/free-and-public-dns-servers-2626062
- Garcia, Michael John and Doyle, Charles. (2010). Extradition to and from the United States: Overview of the Law and Recent Treaties. *Congressional Research Service* 7-5700. https://fas.org/sgp/crs/misc/98-958.pdf.
- Goodman, Marc D. and Brenner, Susan W. (2002). The Emerging Consensus on Criminal Conduct in Cyberspace. *International Journal of Law and Information Technology*, Vol. 10, No. 2, 139-223.
- Hern, Alex. (2017). WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017. *The Guardian*, 30 December 2017. https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware.
- Holt, Thomas, J., Adam M. Bossler, and Kathryn C. Seigfried-Spellar. (2018). *Cybercrime and Digital Forensics*, 2nd edition. Routledge.
- IGI Global. (n.d.) What is the penetration rate. https://www.igi-global.com/dictionary/internet-penetration-rate/15439.
- International Telecommunication Union (ITU). (2012). Understanding cybercrime: Phenomena, challenges and legal response. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf.

- Jaishankar, K. (Ed.). *Cyber criminology: Exploring Internet crimes and criminal behavior*. CRC Press.
- Kessel, J. M. and Mozur, P. (2016) How China Is Changing Your Internet. *New York Times*. https://www.nytimes.com/video/technology/100000004574648/china-internet-wechat.html.
- Krocker, Rachel. (2013) An Internet Connection does not equal Internet access. ICT Works. https://www.ictworks.org/an-internet-connection-does-not-equal-internet-access/
- Lee, Seung-ho. (2013) Cybercrime sleuths have highly intricate challenges. http://koreajoongangdaily.joins.com/news/article/article.aspx?aid=2969778
- Maras, Marie-Helen. (2014). *Computer Forensics: Cybercriminals, Laws and Evidence*, second edition. Jones and Bartlett.
- Maras, Marie-Helen. (2016). *Cybercriminology*. Oxford University Press.
- Maras Marie-Helen. (2015). The Internet of Things: Security and Privacy Implications. *International Data Privacy Law*, Vol. 5(2), 99–104.
- McGuire, Mike and Dowling, Samantha. (2013). Cyber crime: A review of the evidence Research Report 75, Chapter 1: Cyber-dependent crimes. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246751/horr75-chap1.pdf.
- OECD. (2018). Data: Internet access. https://data.oecd.org/ict/internet-access.htm.
- Reuters. (2017). Cyber attack hits 200,000 in at least 150 countries: Europol. Reuters, 14 May 2017. https://www.reuters.com/article/us-cyber-attack-europol/cyber-attack-hits-200000-in-at-least-150-countries-europol-idUSKCN18A0FX
- Rouse, Margaret. (2014) Confidentiality, integrity and availability (CIA Triad). TechTarget. https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA
- Securelist. (2018) Software vulnerabilities. Kaspersky Lab. https://securelist.com/threats/software-vulnerabilities/
- Statcounter. (2016) Mobile and tablet internet usage exceeds desktop for first time worldwide, GlobalStats. http://gs.statcounter.com/press/mobile-and-tablet-internet-usage-exceeds-desktop-for-first-time-worldwide.
- Statista. (2018) Global internet penetration rate as of September 2017, by region, Statista. https://www.statista.com/statistics/269329/penetration-rate-of-the-internet-by-region/.
- The Hague, the Netherlands, (2011). Cybercrime Presents a Major Challenge for Law Enforcements. https://www.europol.europa.eu/newsroom/news/cybercrime-presents-major-challenge-for-law-enforcement.
- Timberg, Craig, Elizabeth Dowskin, Brian Fung. (2017) Data of 143 million Americans exposed in hack of credit reporting agency Equifax. *The Washington Post*.

https://www.washingtonpost.com/business/technology/equifax-hack-hits-credit-histories-of-up-to-143-million-americans/2017/09/07/a4ae6f82-941a-11e7-b9bc-b2f7903bab0d_story.html?noredirect=on&utm_term=.be97d83a9fb7

- УНП ООН (2013). Проект доклада УНП ООН «Всестороннее исследование проблемы киберпреступности». https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.
- Wall, David. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Polity.
- Wall, Matthew. (2016) How long will you wait for a shopping website to load? *BBC News*, 19 August 2017. http://www.bbc.com/news/business-37100091
- Wilson, Clay. (2008). Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. https://fas.org/sgp/crs/terror/RL32114.pdf.
- Zetter, Kim. (2014). Hacker Lexicon: What Is A Zero Day? *Wired*, 11 November 2014. https://www.wired.com/2014/11/what-is-a-zero-day/.

Упражнения

Упражнение №.1: Правовые определения компьютера, данных и сети

Попросите учащихся выяснить, как в местном законодательстве определяются понятия *компьютерная система, компьютерные данные, поставщик услуг* и *данные о трафике*. Ответьте на вопрос: в чем разница между определениями, приведенными в Конвенции Совета Европы о компьютерных преступлениях, и определениями, содержащимися в местном законодательстве?

Рекомендации для лектора

Студенты, вероятно, обнаружат, что для правовых определений используются иные формулировки. Они должны попытаться описать, как различия в формулировках могут повлиять на то, как правовая система определяет понятия компьютер, данные или сеть.

Упражнение №.2: Скорости загрузки веб-страниц

Попросите учащихся измерить скорость загрузки веб-страницы. Откройте веб-страницу в Google Chrome. Нажмите на три точки в правом верхнем углу Chrome. Нажмите «Дополнительные инструменты» -> «Инструменты разработчика» -> «Производительность». Нажмите Ctrl+E, чтобы начать запись и обновить веб-страницу. После загрузки веб-страницы остановите запись и выясните, сколько времени потребовалось для загрузки различных частей веб-страницы. Почему разные части веб-страницы загрузились в разное время?

Рекомендации для лектора

Учащиеся должны попытаться объяснить, почему разные части веб-страницы загружаются с разной скоростью. На основании того, что они узнали из лекции, они могут обсудить, как компьютеры общаются друг с другом, или даже как DNS влияет на время загрузки.

Упражнение №.3: Уровни проникновения Интернета

Многие люди переоценивают уровень проникновения Интернета в своей стране. Это может привести к интересным дискуссиям о группах, которые подключены к Интернету, и группах, которые не подключены.

Ответьте на некоторые из следующих вопросов:

- Каков уровень проникновения Интернета в вашей стране?
- Какие группы испытывают наибольшие затруднения при подключении к Интернету и почему?
- Имеют ли все, кто подключен к Интернету, одинаковые возможности?

Рекомендации для лектора

Цель этого упражнения – познакомить учащихся со статистическими методами и методами сбора и проверки данных. Последние два вопроса касаются навыков критического мышления и имеют отношение к социологии. Во всех случаях лектор должен оценить доказательства, которые учащиеся приводят для любого высказанного ими утверждения. Лектор также должен попытаться оценить правдивость и обоснованность утверждения.

Упражнение №.4: Расследования случаев утечки данных

Случаи утечки данных в Интернете довольно часто освещаются в новостях. Некоторые истории, однако, сопровождаются весьма скудными подробностями.

Попросите учащихся исследовать случаи масштабных утечек данных в их стране. Могут ли учащиеся определить тип уязвимости, который привел к утечке данных?

Учащиеся зачастую не могут найти технические подробности об утечке данных. В таком случае попросите учащихся обсудить, что могло произойти, и объяснить, почему они так думают.

Рекомендации для лектора

Лектор должен ответить на следующие вопросы:

- Определили ли учащиеся реальный случай утечки данных из новостей?
- Была ли выявлена уязвимость, ставшая причиной утечки данных?

- Подтверждается ли доказательствами тот факт, что уязвимость, обнаруженная учащимся, стала причиной утечки данных?

Возможная структура занятия

Ниже описана рекомендуемая структура для занятия. Учащиеся должны закончить прочтение обязательной литературы до начала занятия. Лекции призваны закрепить материал, с которым учащиеся ознакомились при прочтении литературы, а упражнения предназначены для практического применения знаний, полученных из прочтенной литературы и лекций. Для трехчасового занятия предлагается следующая структура. Лекторы могут изменить эту структуру, исходя из своих потребностей и расписания занятий.

Представление занятия и результатов обучения

Лекция (10 минут):

- Вкратце представьте занятие и его содержание
- Определите и обсудите конечные результаты занятия

Основы компьютерных технологий

Лекция (20 минут):

- Определите и опишите основные понятия, относящиеся к компьютерным технологиям

Рекомендации для лектора:

- Если вы используете данный Модуль на юридических курсах, мы рекомендуем углубиться в технические аспекты компьютерных технологий. Очень часто на юридических курсах не проводятся необходимые технические занятия по компьютерным технологиям.
- Если вы используете данный Модуль на курсах по информационной безопасности или инженерному делу, подробная техническая информация, вероятно, не потребуется. Вместо этого сосредоточьтесь больше на применении технических знаний учащихся к юридическим понятиям. Соответствуют ли определения понятий компьютера или сети, которые используют учащиеся, правовым определениям этих понятий?

- Технические и юридические материалы для чтения перечислены в разделе «Список дополнительной литературы».

Упражнение (20 минут):
Попросите учащихся выполнить «Упражнение №.1: Правовые определения компьютера, данных и сети» в разделе «Упражнения» данного Модуля до начала занятия и попросите их обсудить результаты во время лекции. Учащиеся могут либо представить резюме своих результатов на 1-3 страницах, либо прийти подготовленными для обсуждения своих результатов на занятии.

Глобальные тенденции в области использования технологий и подключения к Интернету

Лекция (20 минут):

- Обсудите глобальные тенденции в области использования технологий и подключения к Интернету

Рекомендации для лектора: Всем нужен *быстрый* Интернет. Объяснение того, как ускорить доступ в Интернет, – отличный способ увлечь учащихся. Начните обсуждение, сказав: «Знаете ли вы, что вы можете ускорить свой Интернет, изменив DNS-серверы?». Обычно этот вопрос привлекает внимание учащихся. Затем вы можете объяснить, как работает DNS на уровне, соответствующем базовым знаниям учащихся. Наконец, вы можете *показать* учащимся, как можно вручную поменять DNS-серверы на их устройствах.

[Примечание: существует много бесплатных и быстрых DNS-серверов. По состоянию на февраль 2019 года для тестирования доступны CloudFlare (1.1.1.1), Google (8.8.8.8), Cloud9 (9.9.9.9) и OpenDNS (208.67.222.222). Для получения информации о других бесплатных DNS-серверах см. https://www.lifewire.com/free-and-public-dns-servers-2626062].

Обсуждение тематического исследования (20 минут):
В разделе «Упражнения» данного модуля есть тематическое исследование под названием «Упражнение №.2: скорости загрузки веб-страниц».

[*Альтернативный вариант*: попросите учащихся выполнить «Упражнение №.3: Уровни проникновения Интернета» в разделе «Упражнения» данного Модуля до начала занятия и попросите их обсудить результаты во время лекции. Учащиеся могут либо представить резюме своих результатов на 1-3 страницах, либо прийти подготовленными для обсуждения своих результатов на занятии].

Перерыв

Время: 10 минут

Кратко о киберпреступности и тенденции в области киберпреступности

Лекция (20 минут):

- Определите и обсудите киберпреступность
- Обсудите, почему киберпреступность изучается с научной точки зрения
- Оцените тенденции в области киберпреступности

[*Альтернативный вариант*: поручите учащимся выполнить «Домашнее задание №.2: Остались ли какие-либо виды киберпреступлений неохваченными?» в разделе «Оценка учащихся» данного Модуля до начала занятия и попросите их обсудить результаты во время этой лекции и/или любой последующей лекции. Вы можете задать учащимся вопрос из этого упражнения и/или из любого (или всех) из нижеследующих занятий. Учащиеся могут либо представить резюме своих результатов на 1-3 страницах, либо прийти подготовленными для обсуждения своих результатов на занятии].

Технические, правовые, этические и оперативные проблемы

Лекция (30 минут):

- Распознайте и проанализируйте проблемы технического, правового, этического и оперативного характера, связанные с расследованием киберпреступлений и предупреждением киберпреступности

Рекомендации для лектора: обсудите тематическое исследование в разделе «Дополнительные средства обучения» данного Модуля во время лекции.

Упражнение (20 минут):
Поручите учащимся выполнить «Упражнение №.4: Расследования случаев утечки данных» в разделе «Упражнения» данного Модуля до начала занятия и попросите их обсудить результаты во время лекции. Учащиеся могут либо представить резюме своих результатов на 1-3 страницах, либо прийти подготовленными для обсуждения своих результатов на занятии.

Предупреждение киберпреступности

Лекция (10 минут):

- Обсудите вопросы предупреждения киберпреступности.

Список основной литературы

- Bynum, Terrell. (2011). Computer and Information Ethics. In Edward N. Zalta. (ed.). *The Stanford Encyclopedia of Philosophy*. https://plato.stanford.edu/archives/spr2011/entries/ethics-computer/.
- Finklea, Kristin and Catherine A. Theohary. Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement. *Congressional Research Service*, 15 January 2015. https://fas.org/sgp/crs/misc/R42547.pdf.
- International Telecommunication Union (ITU). (2012). Understanding cybercrime: Phenomena, challenges and legal response (pp. 1-12). http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf.
- Introducing Basic Network Concepts. https://www3.nd.edu/~cpoellab/teaching/cse40814_fall14/networks.pdf.
- Jang, Junsik. (2009). Challenges and Best Practices in Cybercrime Investigation. https://www.unafei.or.jp/publications/pdf/RS_No79/No79_09VE_Jang2.pdf.
- Maras, Marie-Helen. (2014). *Computer Forensics: Cybercriminals, Laws, and Evidence*. Jones and Bartlett.
- Maras, Marie-Helen. (2016). *Cybercriminology*. Oxford University Press.
- УНП ООН (2013). Проект доклада УНП ООН «Всестороннее исследование проблемы киберпреступности» (стр. xvii-xxviii). https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.
- Wall, David. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Polity.

Список дополнительной литературы

- Directorate General For Internal Policies Policy Department C: Citizens' Rights and Constitutional Affairs (2015). The Law Enforcement Challenges of Cybercrime: Are we really catching up? http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536471/IPOL_STU(2015)536471_EN.pdf
- Eichensehr, Kristen E. (2015). The Cyber-Law of Nations. *Georgetown Law Journal*, 103, 365-379. https://georgetownlawjournal.org/articles/63/cyber-law-of-nations/pdf.
- Europol. (2018) Cybercrime. https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime.
- FBI. (2018) What we investigate: Cyber Crime. https://www.fbi.gov/investigate/cyber.
- Godwin, James B, Andrey Kulpin, Karl Frederick Rauscher, Valery Yaschenko. (2014) Critical Terminology Foundations 2. EastWest Institute. https://www.eastwest.ngo/idea/critical-terminology-foundations-2.
- INTERPOL. (2018) Cybercrime. https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime.
- Maras, Marie-Helen. *Cyberlaw and Cyberliberties*. Oxford University Press, Forthcoming, 2020.
- Mclaughlin, Eugene and Muncie, John. (2013). *Criminological Perspectives: Essential Readings*. Third Edition. Sage.
- Matwyshyn, Andrea M. (2009). CSR and the Corporate Cyborg: Ethical Corporate Information Security Practices. *Journal of Business Ethics*, Vol. 88(4), 579–594.
- Menon, Sundaresh and Teo Guan Siew. (2012). Key challenges in tackling economic and cyber crimes: Creating a multilateral platform for international co-operation, *Journal of Money Laundering Control*, Vol. 15(3), 243-256.
- Moor, James H. (1985). What is computer ethics? *Metaphilosophy*, Vol. 16(4), 266-275.
- O'Connell, Mary Ellen and Louise Arimtasu. (2012). Cyber Security and International Law. Chatham House: International Law: Meeting Summary. http://www.chathamhouse.org/sites/default/files/public/Research/International%20Law/290512summary.pdf.
- Petzold, Charles. (2000). *Code: The Hidden Language of Computer Hardware and Software*. Microsoft Press.
- Silberschatz, A., Galvin, P. B. and Gagne, G. (2012). *Operating System Concepts*. 9th edn. Wiley.
- Ward, Dan. (2016). Cybersecurity, Simplicity, and Complexity: The Graphic Guide to Making Systems More Secure Without Making Them Worse. *New America*.

https://static.newamerica.org/attachments/12685-the-comic-guide-to-cybersecurity-and-simplicity/Comic%20Vfinal.5e00364a8df04b7e835ad030046dc5da.pdf.
- Zimmer, Michael. (2010). “But the data is already public”: on the ethics of research in Facebook. *Ethics and Information Technology*, Vol. 12(2), 313-325.
- Zwitter, Andrej. (2014). Big Data Ethics. *Big Data & Society*, Vol. 1(2), 1-1.

Оценка учащихся

В дополнение к упражнениям, другими средствами для оценки учащихся, используемыми в данном Модуле, являются обзорные вопросы и домашние задания.

Обзорные вопросы

Эти вопросы могут также использоваться для стимулирования групповых обсуждений во время лекции.

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

Домашние задания

Учащимся могут быть заданы одно или несколько домашних заданий, которые необходимо выполнить до начала занятия, либо в форме письменного домашнего задания (объемом от 1 до 3 страниц) и/или в рамках обсуждения в классе:

Домашнее задание №.1

Следующее задание предлагается выполнить в течение двух недель после завершения данного Модуля:

Найдите местный закон, в котором дается правовое определение понятиям компьютер, данные или сеть. Затем найдите закон другой страны, который также дает определение одному из этих понятий. Опишите своими словами, насколько эти определения схожи друг с другом, и чем они отличаются. Рекомендуемый объем: 1.500 слов.

Домашнее задание №.2

Поручите учащимся исследовать теорию из их учебной дисциплины и отыскать учащихся, которые применили эту теорию к киберпреступности.

Дополнительные средства обучения

Видео

- Kessel, J. M. and Mozur, P. (2016) How China Is Changing Your Internet (продолжительность: 5:45). *New York Times*, 9 August 2016. https://www.nytimes.com/video/technology/100000004574648/china-internet-wechat.html. Это видео рассказывает о китайских приложениях и их использовании, в частности, о WeChat.
- Khan Academy. (2018) How Computers Work. Computer Science (продолжительность: 26:49) https://www.khanacademy.org/computing/computer-science/how-computers-work2. Как видно из названия, видео рассказывает о том, как работают компьютеры.
- PBS. The Personal Computer Revolution: Crash Course Computer Science #25. (продолжительность: 10:14) https://www.youtube.com/watch?v=M5BZou6C01w&index=26&list=PL8dPuuaLjXtNlUrzyH5r6jN9ullgZBpdo. Как следует из названия, видео содержит краткий обзор персонального компьютера.

- PBS. The Internet: Crash Course Computer Science #29 (продолжительность: 2:44) https://www.youtube.com/watch?v=tpIctyqH29Q&list=PL8dPuuaLjXtNlUrzyH5r6jN9ulIgZBpdo. Как видно из названия, видео дает краткий обзор Интернета.
- PBS. Computer Networks: Crash Course Computer Science #28 (продолжительность: 12:19) https://www.youtube.com/watch?v=3QhU9jd03a0. Как следует из названия, на видео предоставлен краткий обзор компьютерных сетей.
- PBS. The World Wide Web: Crash Course Computer Science #30 (продолжительность: 11:36) https://www.youtube.com/watch?v=guvsH5OFizE&index=31&list=PL8dPuuaLjXtNlUrzyH5r6jN9ulIgZBpdo. Как видно из названия, на видео дается краткий обзор Всемирной паутины.
- PBS. Early Computing: Cybersecurity: Crash Course Computer Science #31 (продолжительность: 12:29) https://www.youtube.com/watch?v=bPVaOlJ6ln0. Как следует из названия, на видео предоставлен краткий обзор кибербезопасности.

UNODC
United Nations Office on Drugs and Crime

Vienna International Centre, P.O. Box 500, 1400 Vienna, Austria
Tel.: (+43-1) 26060-0, Fax: (+43-1) 26060-3389, www.unodc.org