СЕРИЯ УНИВЕРСИТЕТСКИХ МОДУЛЕЙ

Киберпреступность **5**

РАССЛЕДОВАНИЕ КИБЕРПРЕСТУПЛЕНИЙ

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 5

РАССЛЕДОВАНИЕ КИБЕРПРЕСТУПЛЕНИЙ

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*.

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

Существует большое количество различных заинтересованных сторон (т.е. учреждений, организаций, коммерческих предприятий и частных лиц), которые принимают участие в расследовании киберпреступлений. Характер и степень их участия зависят от типа совершенного киберпреступления. Участие заинтересованных сторон также определяется географическим местоположением заинтересованных сторон и законами о киберпреступности, действующими в соответствующих странах. В данном модуле 5, при составлении которого в качестве основы использовался модуль 4: «Введение в цифровую криминалистику», критически рассматриваются процедуры представления информации о киберпреступлениях, а также ключевые субъекты, ответственные за расследование киберпреступлений. Особое внимание уделяется препятствиям, возникающим в ходе расследований киберпреступлений (для получения информации о международном сотрудничестве в расследовании киберпреступлений см. модуль 7: «Международное сотрудничество в борьбе с киберпреступностью», а также серию университетских модулей по организованной преступности, в частности, модуль 11: «Международное сотрудничество в области борьбы с транснациональной организованной преступностью»), и роль процессов управления знаниями в расследованиях киберпреступлений. Модуль 6: «Практические аспекты расследования киберпреступлений и цифровой криминалистики» будет охватывать аспекты, относящиеся к способам проведения расследований киберпреступлений и цифровой судебной экспертизы.

Результаты обучения

- Обсудить и оценить процедуры подачи сообщений о киберпреступлениях
- Определить и обсудить ключевых субъектов, принимающих участие в расследованиях киберпреступлений
- Разъяснить и критически оценить ресурсы, привлекаемые во время расследования киберпреступлений, и препятствия, возникающие в ходе расследований киберпреступлений
- Описать и оценить роль процессов управления знаниями в расследованиях киберпреступлений

Основные вопросы

Расследования киберпреступлений могут быть упреждающими, т.е. проводиться при поступлении оперативных данных, или «реактивными», т.е. проводиться при выявлении киберпреступления и/или получении сообщения о киберпреступлении соответствующими органами. Надзорный орган и/или иной ключевой субъект, который получает сообщение о киберпреступлении, принимает решение о том, кто будет участвовать в расследовании. Многочисленные учреждения, организации, коммерческие предприятия и частные лица внутри страны (и даже за ее пределами), включая органы уголовного правосудия и национальной безопасности, международные организации, частный сектор и организации гражданского общества, могут тем или иным образом участвовать в проведении расследований киберпреступлений. В данном модуле рассматриваются эти ключевые субъекты и их функции в расследованиях киберпреступлений, а также практика сообщения информации о киберпреступлениях, сложности, связанные с расследованиями киберпреступлений, и роль управления знаниями в расследованиях киберпреступлений.

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).

> *Знаете ли вы?*
>
> Европол открыл веб-страницу, на которой размещена информация о европейских странах, в которых действуют механизмы сообщения информации о киберпреступлениях в режиме онлайн.
>
> Для получения дополнительной информации см.: Europol. (n.d.). Reporting Cybercrime Online. https://www.europol.europa.eu/report-a-crime/report-cybercrime-online.

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 (Wall, 2007, p. 194; 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 Cyber Crime 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 (для получения информации о механизмах оценки см. модуль 8 серии модулей по киберпреступности: «Кибербезопасность и предупреждение киберпреступности: стратегии, политика и программы»).

Кто проводит расследования киберпреступлений?

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 и/или устройства информационно-коммуникационных технологий, использованные для совершения преступления с использованием киберсетей и/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 (Maras, 2014; см. модуль 4 серии модулей по киберпреступности: «Введение в цифровую

криминалистику» для получения дополнительной информации об обоснованности и достоверности цифровых доказательств).

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, 2016c). 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, 2016d), 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, 2017c).

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, 2017b). 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, 2017b).

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); см. «Пример уровня ЗНС для следователя по делам о киберпреступности» во вставке ниже), 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, 2017a, 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) (для ознакомления с отчетами о других странах см. портал Глобального центра развития потенциала в области кибербезопасности).

Пример уровня ЗНС следователя по делам о киберпреступности

Структура трудовых ресурсов в области кибербезопасности (Cybersecurity Workforce Framework), разработанная в рамках Национальной образовательной инициативы США в сфере кибербезопасности (NICE) (рассматривается в модуле 8 серии модулей по киберпреступности: «Кибербезопасность и предупреждение киберпреступности: стратегии, политика и программы»), включает в себя ЗНС для штатных должностей, связанных с кибербезопасностью и киберпреступностью. Например, в Структуре трудовых ресурсов в области кибербезопасности NICE перечислены следующие уровни знаний, навыков и способностей для следователя по делам о киберпреступности (US National Initiative for Cybersecurity Careers and Studies, n.d.):

Знания

K0001: Знание концепций построения компьютерных сетей, сетевых протоколов и методологий обеспечения безопасности сети.
K0002: Знание процессов управления рисками (например, методов оценки и снижения риска).
K0003: Знание законов, правил, политики и этики, относящихся к кибербезопасности и конфиденциальности.
K0004: Знание принципов обеспечения кибербезопасности и сохранения конфиденциальности.
K0005: Знание киберугроз и уязвимостей.
K0006: Знание конкретных оперативных последствий недочетов в системе обеспечения кибербезопасности.
K0046: Знание методологий и методов обнаружения вторжений для обнаружения вторжений на уровне узла и сети.
K0070: Знание угроз безопасности и уязвимостей системы и приложений (например, переполнение буфера, мобильный код, межсайтовый скриптинг, процедурный язык/язык структурированных запросов [PL/SQL] и внедрение SQL-кода, состояние гонки, скрытый канал, воспроизведение, возвратно-ориентированные атаки, вредоносный код).
K0107: Знание инструментов и законов/регламентов для проведения расследования инсайдерских угроз и составления отчетов.
K0110: Знание тактики, методов и процедур, используемых злоумышленниками.

K0114: Знание электронных устройств (например, компьютерных систем/компонентов, устройств контроля доступа, цифровых камер, цифровых сканеров, электронных органайзеров, жестких дисков, карт памяти, модемов, сетевых компонентов, сетевых приборов, сетевых устройств управления домом, принтеров, съемных устройств хранения данных, телефонов, копировальных устройств, факсимильных аппаратов и т.д.).

K0118: Знание процедур изъятия и сохранения цифровых доказательств.

K0123: Знание законных методов управления, связанных с обеспечением допустимости доказательств (например, норм доказательственного права).

K0125: Знание процессов сбора, упаковки, транспортировки и хранения электронных доказательств в рамках системы охраны доказательств.

K0128: Знание типов и наборов постоянно хранимых данных.

K0144: Знание социальной динамики взломщиков компьютеров в глобальном контексте.

K0155: Знание закона об электронных доказательствах.

K0156: Знание правовых норм доказательственного права и процедур судопроизводства.

K0168: Знание применимых законов, статутов (например, в титулах 10, 18, 32, 50 Кодексе США), президентских директив, директивных указаний органов исполнительной власти и/или административных/уголовно-правовых руководящих принципов и процедур.

K0209: Знание методов скрытой связи.

K0231: Знание протоколов, процедур и методов управления кризисными ситуациями.

K0244: Знание физического и физиологического поведения, которое может указывать на подозрительную или ненормальную активность.

K0251: Знание судебных процедур, включая процедуры представления фактов и доказательств.

K0351: Знание применимых статутов, законов, положений и принципов, регулирующих кибератаки и киберэксплуатацию.

K0624: Знание рисков для безопасности приложений (например, список Топ-10 сообщества «Открытый проект обеспечения безопасности веб-приложений»)

Навыки

S0047: Навыки сохранения целостности доказательств в соответствии со стандартными операционными процедурами или национальными стандартами.
S0068: Навыки сбора, обработки, упаковки, транспортировки и хранения электронных доказательств с целью недопущения изменений, потери, физического повреждения или уничтожения данных.
S0072: Навыки использования научных правил и методов для решения проблем.
S0086: Навыки оценки надежности поставщика и/или продукта.

Способности

A0174: Способность осуществлять поиск и навигацию по темной паутине с помощью сети TOR для поиска рынков и форумов.
A0175: Способность исследовать цифровые носители на нескольких платформах операционных систем.

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»; Maras, 2014, p. 29; рассматривается в модуле 4 серии модулей по киберпреступности: «Введение в цифровую криминалистику», а также в модуле 6: «Практические аспекты расследования киберпреступлений и цифровой криминалистики»). 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 Cyber Security 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 (см. модуль 14 серии модулей

по киберпреступности: «Хактивизм, терроризм, шпионаж, дезинформационные кампании и войны в киберпространстве» для получения дополнительной информации).

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; Maras, 2016) и *кибернаступательные* возможности (т.е. меры, которые «предназначены для проникновения в системы противника и причинения им вреда или ущерба» и/или реагирования на кибератаку; Maras, 2016, p. 391). Именно признание киберпространства в качестве еще одной сферы ведения боевых действий (пятая сфера наряду с сушей, морем, воздухом и космосом; также известна под названием сфера операций, см. вставку «Знаете ли вы?» ниже), привело к расширению деятельности органов национальной безопасности в киберпространстве (Smeets, 2018; Kremer, 2014; 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 (Smeets, 2018; Kremer, 2014; Kallender and Hughes, 2017; Ingeniería de Sistemas para la Defensa de España, n.d.). Организация Североатлантического договора (НАТО) также признала киберпространство пятой сферой ведения боевых действий (NATO CCDCE, 2016).

> *Знаете ли вы?*
>
> На Филиппинах предпочитают использовать термин «сфера операций». Согласно статье 2 Конституции страны, «Филиппины отказываются от войны как инструмента осуществления национальной политики, перенимают и используют общепринятые принципы международного права как часть законодательства собственной страны и придерживаются политики мира, равенства, справедливости, свободы, сотрудничества и мирных отношений между всеми нациями».

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) (для получения дополнительной информации об этих киберпреступлениях и прочих видах киберзависимых преступлений и преступлений с использованием киберсетей, см. модуль 2 серии модулей по киберпреступности: «Основные виды киберпреступности»).

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.).

Знаете ли вы?

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).

«Сети и системы командования и управления, предназначенные для поддержки производственных процессов» на объектах критически важной инфраструктуры, известны под названием *системы управления технологическими процессами* (СУ ТП) (ENISA, n.d.). Как отмечает *Европейское агентство по сетевой и информационной безопасности,*

СУ ТП претерпели значительные преобразования, превратившись из закрытых изолированных систем в системы открытой архитектуры и стандартных технологий, тесно связанные с другими корпоративными сетями и Интернетом. Сегодня продукты СУ ТП в основном основаны на стандартных платформах встроенных систем, применяемых в различных устройствах, таких как маршрутизаторы или кабельные модемы, и они зачастую используют коммерческое готовое программное обеспечение. Все это привело к снижению затрат, удобству в использовании и позволило осуществлять дистанционное управление и мониторинг из разных мест. Однако существенным недостатком, связанным с подключением к интрасетям и сетям связи, является повышенная уязвимость к атакам на основе компьютерных сетей (ENISA, n.d.).

Именно эти уязвимости, а также те, которые являются результатом ненадлежащих мер по обеспечению физической безопасности и защите от злоумышленных действий персонала (например, работник может принести зараженный флэш-накопитель на объект критически важной инфраструктуры и физически подключить его к системам этой инфраструктуры; см. модуль 9 серии модулей по киберпреступности: «Кибербезопасность и предупреждение киберпреступности: практические методы и меры» для получения дополнительной информации о практических мерах обеспечения кибербезопасности), делают возможными атаки киберпреступников на объекты критически важной инфраструктуры.

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 (для получения дополнительной информации о мерах, реализуемых с целью предотвращения и смягчения последствий киберпреступлений и реагирования на них, см. модуль 9 серии модулей по киберпреступности: «Кибербезопасность и предупреждение киберпреступности: практические методы и меры»). 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) (Maras, 2014; Maras, 2016).

Несообщение информации об утечке данных компанией Yahoo Inc.

Компания Yahoo Inc. (теперь известная под названием Altaba) сообщила об одном случае (из нескольких случаев) утечки данных, с которым она столкнулась, спустя два года после инцидента. В результате такого раскрытия информации «цена акций Yahoo упала на 3 процента, что привело к потере около 1,3 миллиардов долларов США рыночной капитализации. Кроме того, компания, которая [в тот момент времени] вела переговоры о продаже своего бизнеса компании Verizon, была вынуждена согласиться со скидкой в размере 7,25 процентов на предложенную цену покупки, что снизило ее на 350 млн. долларов США» (Dicke and Caloza, 2018). Из-за несвоевременного раскрытия сведений об утечке данных компания Yahoo была также оштрафована на 35 млн. долларов Комиссией по ценным бумагам и биржам США (US Securities and Exchange Commission, 2018).

Так же, как и правоохранительные органы, частные компании и организации проводят расследования при выявлении киберпреступления или получении сообщения о киберпреступлении. Расследование проводится с целью получения информации об инциденте и возбуждения дела в отношении исполнителя (исполнителей) киберпреступления (киберпреступлений). В зависимости от размера и ресурсов частных компаний и организаций, расследование может проводиться штатными следователями или следователями, нанятыми извне (Maras, 2014). В число лиц, принимающих участие в расследованиях киберпреступлений, входят представители частных компаний, отраслевых организаций, торговых организаций и компаний, предоставляющие услуги по обеспечению безопасности, расследованиям и цифровой криминалистике (Hunton, 2012). Бывали случаи, когда специалисты по информационным технологиям и эксперты в области цифровой криминалистики из негосударственного сектора использовались частными компаниями и организациями для сбора и сохранения цифровых доказательств. Однако эти специалисты могут не иметь необходимых знаний, навыков и способностей для проведения расследований киберпреступлений и надлежащего обращения с цифровыми доказательствами киберпреступления, чтобы обеспечить их допустимость в судах общего права (Maras, 2014).

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 (Shore, Du, and Zeadally, 2011). 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 2Centre (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 (Cybercrime Centres of Excellence Network for Training, Research and Education, n.d.).

В дополнении к ГЧП были созданы национальные целевые группы для оказания помощи в расследовании киберпреступлений. Эти целевые группы позволяют правоохранительным органам, обладающими разными юрисдикциями и полномочиями

в своих странах (будь то местные, региональные или федеральные/национальные органы) осуществлять сотрудничество по делам, связанным с киберпреступностью. Эти группы, в зависимости от конкретной страны и/или региона, могут также включать в свой состав представителей научных кругов и частных компаний и организаций. В качестве примера можно привести Национальную объединенную оперативную группу по киберрасследованиям (NCIJTF) Федерального бюро расследований США, которая

состоит из… представителей учреждений-партнеров, входящих в структуры правоохранительных органов, разведывательного сообщества и Министерства обороны, которые базируются в одном месте и тесно взаимодействуют с целью выполнения задачи организации на основе общегосударственного подхода. Являясь уникальным межведомственным кибернетическим центром, NCIJTF в первую очередь отвечает за координацию, обобщение и обмен информацией в поддержку исследований киберугроз, выполнение анализа оперативных данных и представление его результатов лицам, принимающим решения, и оказание содействия другим непрерывным усилиям по борьбе с киберугрозами национальной безопасности (FBI, n.d.).

Были созданы и другие целевые группы, которые занимаются конкретными видами киберпреступлений. Например, Целевая *группа* по борьбе с электронными преступлениями (ECTF), специальная группа секретной службы США, отвечает за предотвращение, смягчение последствий, выявление и расследование киберпреступлений, в том числе совершенных в отношении систем финансовых расчетов и объектов критически важной инфраструктуры (US Secret Service, n.d.). В соответствии с Законом «О сплочении и укреплении Америки путем обеспечения надлежащими средствами, требуемыми для пресечения и воспрепятствования терроризму» («ПАТРИОТИЧЕСКИЙ акт») 2001 года, секретная служба США создала сеть целевых групп по борьбе с электронными преступлениями (ECTF) по всей территории Соединенных Штатов. Эти целевые группы взаимодействуют с местными, региональными и федеральными правоохранительными органами, а также с другими работниками системы уголовного правосудия (например, прокурорами), представителями научного сообщества и частного сектора (US Secret Service, n.d.). Европейская целевая группа по борьбе с электронными преступлениями (EECTF) была создана в 2009 году. EECTF осуществляет сбор, анализ и распространение информации о передовой практике.

Хотя органы уголовного правосудия, органы национальной безопасности, частный сектор, ГЧП и целевые группы являются основными действующими лицами при проведении расследований киберпреступлений, независимые расследования киберпреступлений могут также проводиться институтами гражданского общества, журналистами и общественностью. Примером может служить лаборатория Citizen Lab, опубликованные исследования которой включают в себя «расследование цифрового шпионажа против гражданского общества, документальное подтверждение фильтрации

Интернет-контента и других технологий и методов, оказывающих негативное воздействие на осуществление права на свободу слова в Интернете, анализ средств контроля конфиденциальности, безопасности и информационных потоков, используемых в популярных приложениях, а также изучение механизмов обеспечения прозрачности и подотчетности во взаимоотношениях между корпорациями и государственными учреждениями в сфере защиты персональных данных и прочих видов надзора» (Citizen Lab, n.d.). Кроме того, представители общественности могут оказывать правоохранительным органам добровольное содействие путем проведения собственных независимых расследований в сети Интернет; такой случай наблюдался после взрывов в Бостоне в 2013 году (Nhan, Huey, and Broll, 2017). Более того, некоторые аспекты расследования киберпреступности (например, выявление незаконных материалов в Интернете) могут поручаться и уже поручались общественности путем проведения открытого конкурса (этот процесс именуется *краудсорсингом*). Например, «Европол выступил с краудсорсинговой инициативой для привлечения широкой общественности к расширенному поиску источников происхождения изображений сексуального насилия над детьми. С момента запуска проекта, реализация которого началась 1 июня 2017 года, в Европол было отправлено более 22.000 полезных подсказок, в результате рассмотрения которых уже опознано восемь детей, и один преступник задержан благодаря помощи простых граждан» (Europol, 2018a).

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 (Maras, 2016; см. модуль 10 серии модулей по киберпреступности: «Конфиденциальность и защита данных» для получения дополнительной информации об анонимности). Существуют несколько методов анонимизации, которые используют киберпреступники (см. вставку «Примечание» ниже). 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 (Chow, 2012).

Примечание

Методы анонимизации используются как на законных, так и незаконных основаниях. Существуют законные основания для того, чтобы оставаться анонимным и сохранять защиту анонимности в сети (см. модуль 10 серии модулей по киберпреступности: «Конфиденциальность и защита данных»). Например, анонимность способствует свободному потоку информации и сообщений без опасений последствий за высказывание нежелательных или непопулярных мыслей (Maras, 2016) (если только не существуют законных оснований, имеющих преимущественную юридическую силу, для ограничения права на выражение таких мнений; см. модуль 3 серии модулей по киберпреступности: «Правовая база и права человека» для ознакомления с законными и легитимными ограничениями права на свободу выражения мнения).

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).

Знаете ли вы?

Луковый маршрутизатор (или Tor https://www.torproject.org/), 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; Finklea, 2017). 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 (Dredge, 2013). Таким образом, эти анонимные сети используются для доступа к сайтам в Даркнет (или Темной паутине) (см. вставку «Всемирная паутина: основные сведения» ниже).

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 (Finklea, 2017).

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) (Lin, 2016). Использование инструментов, повышающих анонимность, может затруднить идентификацию устройств и/или лиц, ответственных за совершение киберпреступления.

Знаете ли вы?

На веб-сайте Информационного центра электронной приватности (The Electronic Privacy Information Center) содержится информация об «инструментах повышения анонимности» и имеются ссылки на эти инструменты (Lin, 2016).

Процесс атрибуции еще более усложняется из-за использования зараженных вредоносными программами компьютеров-зомби (или *бот-сетей*; этот вопрос рассматривается в модуле 2 серии модулей по киберпреступности: «Основные виды киберпреступности») 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.

Знаете ли вы?

В научной литературе обсуждался вопрос создания международной организации для кибер-атрибуции.

Хотите знать больше?

David II, John S., Benjamin Boudreaux, Jonathan William Welburn, Jair Aguirre, Cordaye Ogletree, Geoffrey McGovern, and Mihcael S. Chase. (2017). Stateless Attribution: Toward International Accountability in Cyberspace. RAND. https://www.rand.org/pubs/research_reports/RR2081.html.

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 (Pihelgas, 2013). 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 (Pihelgas, 2013; Lin, 2016). 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» (т.е. DDoS-атаку) на систему или веб-сайт (для получения дополнительной информации об этих киберпреступлениях см. модуль 2 Серии модулей по киберпреступности: «Основные виды киберпреступности»).

Администрация адресного пространства Интернет (IANA) Интернет-корпорации по присвоению имен и номеров (ICANN), помимо выполнения прочих задач, руководит распределением IP-адресов среди Региональных Интернет-регистратур (РИР), которые отвечают за надзор над регистрацией IP-адресов в своих регионах (Maras, 2014, p. 288-289). Существуют пять РИР: Африканский сетевой информационный центр (AFRINIC); Азиатско-Тихоокеанский сетевой информационный центр (APNIC); Американская регистратура для числовых абонентов Интернет (ARIN); Латиноамериканский и Карибский сетевой информационный центр (LACNIC); и Координационный центр европейской континентальной сети (RIPE NCC). РИР предоставляют информацию об IP-адресах, организациях, связанных с IP-адресами, и контактную информацию этих организаций (например, адреса электронной почты и номера телефонов).

Чтобы определить Интернет-провайдера, связанного с IP-адресом, следователь по делам о киберпреступности может использовать сервис WHOIS – инструмент ICANN для формирования запросов. РИР предоставляют доступ к сервисам WHOIS через свои веб-сайты. Данные WHOIS представляют собой регистрационную информацию, предоставляемую физическими лицами, корпорациями, организациями и правительствами при регистрации *доменных имен* (например, gmail.com), которая включает в себя имена и контактную информацию (например, номера телефонов, почтовые адреса и адреса электронной почты) (ICANN WHOIS, n.d.). Инструмент формирования запросов WHOIS может использоваться для определения контактной

информации и местонахождения организации, связанной с доменным именем (Maras, 2014, p. 290). Инструмент WHOIS также можно использовать для определения контактной информации и местонахождения организации, связанной с IP-адресом (Maras, 2014, p. 289). Однако Общий регламент Европейского союза (ЕС) по защите данных (GDPR), единый закон о защите данных, вступивший в силу 25 мая 2018 года, который регламентирует обработку, хранение, использование данных и обмен данными в государствах-членах ЕС и других странах, учреждениях и частных организациях за пределами ЕС, которые предоставляют товары и услуги ЕС и обрабатывают данные резидентов ЕС (см. модуль 10 серии модулей по киберпреступности: «Конфиденциальность и защита данных» для получения дополнительной информации о GDPR), повлиял на доступность данных WHOIS (в частности, данных, которые считаются персональными данными в соответствии с GDPR; для получения дополнительной информации см. TrendMicro, 2018; и ICANN, n.d.).

После того как будет определен Интернет-провайдер, следователи, расследующие киберпреступление, могут связаться с этим Интернет-провайдером, связанным с IP-адресом, чтобы получить информацию об абоненте, использующем этот IP-адрес (Lin, 2016). Однако Интернет-провайдеров не всегда можно принудить к предоставлению личной информации без соответствующих юридических документов, и в некоторых случаях уже существующее законодательство о неприкосновенности частной жизни/защите персональных данных может запрещать выдачу таких документов (Mayeda, 2015). Юридический документ (например, повестка в суд, ордер на обыск или судебный ордер), используемый для получения этой информации, варьируется в зависимости от конкретной страны (см. модули 6 и 7 Серии модулей по киберпреступности для получения дополнительной информации о юридических документах, используемых при расследовании киберпреступлений).

Знаете ли вы?

WHOIS (англ. «кто это?») не является акронимом; «это система, которая задает вопрос: кто отвечает за доменное имя или IP-адрес?» (ICANN WHOIS, n.d.).

Хотите знать больше?

См.: https://whois.icann.org/en

Различия в положениях законодательства разных стран в области киберпреступности, отсутствие международных стандартов, касающихся требований в отношении представления доказательств (как с точки зрения допустимости доказательств в суде, так

и с точки зрения международной ответственности государства), механизмов оказания взаимной правовой помощи по делам, связанным с киберпреступностью, и своевременного сбора, сохранения цифровых доказательств и обмена ими между странами также являются препятствием для расследования киберпреступлений (см. модуль 3 Серии модулей по киберпреступности: «Правовая база и права человека» и модуль 7 Серии модулей по киберпреступности: «Международное сотрудничество в борьбе с киберпреступностью»). Что касается некоторых типов киберпреступлений, особенно политически мотивированных киберпреступлений, то наблюдается общее отсутствие воли стран к сотрудничеству по таким делам (см. модуль 14 Серии модулей по киберпреступности: «Хактивизм, терроризм, шпионаж, дезинформационные кампании и войны в киберпространстве» для получения дополнительной информации о таких киберпреступлениях).

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 (см. модуль 4 Серии модулей по киберпреступности: «Введение в цифровую криминалистику» для получения дополнительной информации о цифровых доказательствах, цифровых устройствах и инструментах цифровой криминалистики). Более того, следователи могут не иметь необходимого оборудования и инструментов цифровой криминалистики, необходимых для надлежащего проведения расследований киберпреступлений, предполагающих использование цифровых устройств (см. модуль 7 Серии модулей по киберпреступности: «Международное сотрудничество в борьбе с киберпреступностью»).

К прочим препятствиям для расследования киберпреступлений можно отнести ограниченные возможности правоохранительных органов для проведения таких расследований (Lepppanen and Kankaanranta, 2017). 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 (Hinduja, 2004; Köksal, 2009; УНП ООН, 2013; Lepppanen and Kankaanranta, 2017). 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; важность укрепления национального потенциала, необходимого для расследования киберпреступлений, и способы решения

проблемы нехватки национального потенциала для расследования киберпреступлений подробно рассматриваются в модуле 7 Серии модулей по киберпреступности: «Международное сотрудничество в борьбе с киберпреступностью»). Кроме того, эти ограниченные возможности правоохранительных органов еще больше усугубляются коротким сроком актуальности профессиональных знаний следователей по делам о киберпреступлениях (Harkin, Whelan, and Chang, 2018, p. 530). 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 (Harkin, Whelan, and Chang, 2018, p. 530). Эти проблемы, связанные с потенциалом и кадровыми ресурсами, должны быть внимательно изучены странами, поскольку они являются серьезным препятствием для расследований киберпреступлений (Sucio, 2015; PBS, 2018).

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 (Acharyulum 2011). Обмен знаниями, являющийся неотъемлемой частью процесса управления знаниями в правоохранительной деятельности (Hunton, 2012), 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 (Dixon, 2000). 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 (эти вопросы рассматриваются в модуле 3 Серии модулей по киберпреступности: «Правовая база и права человека»), 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 (Brown and Duguid, 1998). 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).

Заключение

Транснациональный характер киберпреступности и взаимозависимость систем и цифровых устройств, подключенных к Интернету, в пределах и за пределами территорий стран требуют осуществления обмена информацией о киберпреступлениях между странами (этот вопрос рассматривается в модуле 7 Серии модулей по киберпреступности: «Международное сотрудничество в борьбе с киберпреступностью»). Кроме того, необходимо осуществлять обмен знаниями о передовых методах расследования киберпреступлений. Огромное количество заинтересованных сторон, участвующих в расследованиях киберпреступлений, требует принятия скоординированных ответных мер реагирования на киберпреступления и обмена явными и неявными знаниями между всеми заинтересованными сторонами. Подходы к расследованию киберпреступлений и знания о расследованиях варьируются в зависимости от заинтересованных сторон и конкретной страны, в которой они проживают и/или осуществляют деятельность. Процессы управления этими знаниями внутри страны и за ее пределами необходимы для обеспечения эффективного расследования киберпреступлений на национальном и международном уровнях. Меры, предполагающие использование информационно-коммуникационных технологий для облегчения обмена знаниями, имеют первостепенное значение, поскольку они

позволяют обмениваться явными и неявными знаниями независимо от географического местоположения распространителей и получателей знаний.

Список использованной литературы

- Acharyulum, G.V.R.K. (2011), Information Management in a Health Care System: Knowledge Management Perspective. *International Journal of Innovation, Management and Technology*, Vol. 2(6), 534–537.
- Biros, David P., Mark Weiser and John Witfield. (2007). Managing digital forensic knowledge an applied approach. Proceedings of the 5th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia. https://ro.ecu.edu.au/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1010&context=adf.
- Brown, John Seely and Paul Duguid. (1998). Organizing Knowledge. *California Management Review*, Vol. 40(3), 90-111.
- Chang, Weiping and Peifang Chung. (2014). Knowledge Management in Cybercrime Investigation – A Case Study of Identifying Cybercrime Investigation Knowledge in Taiwan. *Pacific-Asia Workshop on Intelligence and Security Informatics* (PAISI 2014: Intelligence and Security Informatics), pp. 8-17.
- Chow, Peter. (2012). Surfing the Web Anonymously - The Good and Evil of the Anonymizer. SANS Institute InfoSec Reading Room. https://www.sans.org/reading-room/whitepapers/detection/surfing-web-anonymously-good-evil-anonymizer-33995.
- Citizen Lab (n.d.). Research. https://citizenlab.ca/category/research/.
- Cybercrime Centres of Excellence Network for Training, Research and Education. (n.d.). 2Centre. http://www.2centre.eu/.
- Dean, Geoff, Cathrine Filstad, and Petter Gottschalk. (2006). Knowledge Sharing in Criminal Investigations: An Empirical Study of Norwegian Police as Value Shop. *Criminal Justice Studies*, Vol. 19(4), 423-437.
- Dicke, Michael S. and Alexis I. Caloza. (2018). Yahoo's $35M SEC Settlement: Takeaways from the First Enforcement Action for Failure to Disclose a Data Breach. Fenwick and West LLP, 3 May 2018. https://www.fenwick.com/publications/Pages/Yahoos-$35M-SEC-Settlement-Takeaways-from-the-First-Enforcement-Action-for-Failure-to-Disclose-a-Data-Breach.aspx.
- Dixon, Nancy M. (2000). *Common knowledge. How companies thrive by sharing what they know*. Harvard Business School Press.

- Doan, Quang, Camille Rosenthal-Sabroux, and Michel Grundstein. (2011). A reference model for knowledge retention within small and medium size enterprises. *KMIS*, 306-311.
- Dredge, Stuart. (2013). What is Tor? A beginner's guide to the privacy tool. *The Guardian*, 5 November 2013. https://www.theguardian.com/technology/2013/nov/05/tor-beginners-guide-nsa-browser.
- FBI. (n.d.). Cyber Crime. https://www.fbi.gov/investigate/cyber.
- FBI. (n.d.). National Cyber Investigative Joint Task Force. https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force.
- Europol. (2018c). Darknet Euro Counterfeiter Arrested in Poland. https://www.europol.europa.eu/newsroom/news/darknet-euro-counterfeiter-arrested-in-poland.
- Europol. (n.d.). About Europol. https://www.europol.europa.eu/about-europol.
- Europol. (2018b). Crime on the Dark Web: Law Enforcement Coordination is the Only Cure. https://www.europol.europa.eu/newsroom/news/crime-dark-web-law-enforcement-coordination-only-cure.
- Europol. (2018). 241 Victims of Child Sexual Abuse Safeguarded Thanks to Global Law Enforcement Efforts. Press Release, 26 October 2018. https://www.europol.europa.eu/newsroom/news/241-victims-of-child-sexual-abuse-safeguarded-thanks-to-global-law-enforcement-efforts
- Finklea, Kristin. (2017). Dark Web. Congressional Research Service. https://fas.org/sgp/crs/misc/R44101.pdf.
- Global Cyber Security Capacity Centre. (2017a). Cybersecurity Capacity Review: Kyrgyz Republic. https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM_Kyrgyzstan%20Report%20final_execsummary_1701030.pdf.
- Global Cyber Security Capacity Centre. (2017b). Cybersecurity Capacity Review: Republic of Cyprus. http://www.ocecpr.org.cy/sites/default/files/cmm_cyprus_report_2017_final.pdf.
- Global Cyber Security Capacity Centre. (2017c). Cybersecurity Capacity Review: Republic of Iceland. https://www.stjornarradid.is/lisalib/getfile.aspx?itemid=f3bb2c35-4c76-11e8-942b-005056bc530c.
- Global Cyber Security Capacity Centre. (2017d). Cybersecurity Capacity Review: Republic of Lithuania.

https://www.nrdcs.lt/file/repository/resources/Lithuania_Report_10_8_2017_FINAL.pdf.

- Global Cyber Security Capacity Centre. (2016a). Cybersecurity Capacity Review of the Republic of Madagascar. https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/cmm_rapport_final_cybersecurite_madagascar.pdf.
- Global Cyber Security Capacity Centre. (2016b). Cybersecurity Capacity Review of the Republic of Senegal. https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Senegal-Report-v4%20.pdf.
- Global Cyber Security Capacity Centre. (2016c). Cybersecurity Capacity Review of the United Kingdom. https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Cybersecurity%20Capacity%20Review%20of%20the%20United%20Kingdom.pdf.
- Global Cyber Security Capacity Centre. (2016d). Cybersecurity Capacity Review: Republic of Sierra Leone. https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM_Sierra%20Leone%20report_final_0.pdf.
- Gottschalk, Peter. (2007). Information systems in police knowledge management. *Electronic Government*, Vol. 4(2), 191–203.
- Harkin, Diarmaid, Chad Whelan and Lennon Chang (2018). The challenges facing specialist police cyber-crime units: an empirical analysis. *Police Practice and Research*, Vol. 19(6), 519-536.
- Hauck, Roslin V. and Hsinchun Chen. (1999). COPLINK: A case of intelligent analysis and knowledge management. Proceedings of the International Conference of Information Systems, Charlotte, North Carolina. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.92.4444&rep=rep1&type=pdf.
- Hinduja, Sameer. (2007). Computer Crime Investigations in the United States: Leveraging Knowledge from the Past to Address the Future. *International Journal of Cyber Criminology* Vol. 1(1), 1–26.
- Hunton, Paul. (2012). Managing the technical resource capability of cybercrime investigation: a UK law enforcement perspective. *Public Money & Management*, Vol. 32(3), 225-232.
- ICANN. (n.d.). About WHOIS. https://whois.icann.org/en/about-whois.
- Ingeniería de Sistemas para la Defensa de España. (n.d.). The Joint Cyber-Defence Command organized with the collaboration of Isdefe the Cyber-Defence Conference 2016.

https://www.isdefe.es/noticias/joint-cyber-defence-command-organises-collaboration-isdefe-cyber-defence-conference-2016?language=en.

- INTERPOL. (n.d.). Activities: Operations and Investigations. https://www.interpol.int/Crime-areas/Cybercrime/Activities/Operations-investigations.
- INTERPOL. (n.d.). Kaspersky Lab. https://www.interpol.int/About-INTERPOL/International-partners/Kaspersky-Lab.
- INTERPOL. (n.d.) Strategic Partners. https://www.interpol.int/About-INTERPOL/International-partners/Strategic-Partners.
- Japan Cybercrime Control Center. (JC3). (2014). Establishment of "Japan Cybercrime Control Center," a New Organization for Fighting Cybercrime. https://www.jc3.or.jp/media/pdf/pressreleaseEnglish.pdf.
- Kallender, Paul and Christopher W. Hughes. (2017). Japan's Emerging Trajectory as a 'Cyber Power': From Securitization to Militarization of Cyberspace. *Journal of Strategic Studies*, Vol. 40(1-2), 118-145.
- Kremer, Jens. (2014) Policing cybercrime or militarizing cybersecurity? Security mindsets and the regulation of threats from cyberspace. *Information & Communications Technology Law*, Vol. 23(3), 220-237.
- Leppänen, Anna and Kankaanranta, Terhi. (2017) Cybercrime investigation in Finland. *Journal of Scandinavian Studies in Criminology and Crime Prevention*, Vol. 18(2), 157-175.
- Lin, Herbert. (2017). Attribution of Malicious Cyber Incidents. Hoover Institution, Aegis Paper Series No. 1607. https://www.hoover.org/sites/default/files/research/docs/lin_webready.pdf.
- Maras, Marie-Helen. (2014). *Computer Forensics: Cybercriminals, Laws and Evidence*, second edition. Jones and Bartlett.
- Maras, Marie-Helen. (2014). Inside Darknet: The Takedown of Silk Road. *Criminal Justice Matters*, Vol. 98(1), 22-23.
- Maras, Marie-Helen. (2016). *Cybercriminology*. Oxford University Press.
- Mayeda, G. (2015). Privacy in the age of the internet: Lawful access provisions and access to ISP and OSP subscriber information. *The Alberta Law Review 53*(3), 709-746
- McGuire, Mike and Samantha Dowling. (2013). Chapter 4: Improving the cyber crime evidence base. Cyber crime: A review of the evidence. Research Report 75. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246756/horr75-chap4.pdf.
- Morgan, Anthony, Christopher Dowling, Rick Brown, Monique Mann, Isabella Voce, and Marc Smith. (2016). Evaluation of the Australian Cybercrime Online Reporting Network. Australian Institute of Criminology, Australian Government. https://aic.gov.au/sites/default/files/2018/08/acorn_evaluation_report_.pdf.

- National Cyber Forensics and Training Alliance. (n.d.). About us. https://www.ncfta.net/home-2/about-us/.
- National Cyber Security Centre (2018). Ghana' National Cybercrime Awareness Programme. https://cybersecurity.gov.gh/wp-content/uploads/2018/10/NCSAM2018Brochure.pdf.
- National Cyber Security Centre (2018). Ghana' National Cyber Security Awareness Week 2017 (NCSAW 2017) Report. https://cybersecurity.gov.gh/wp-content/uploads/2018/10/NCSW-2017-Brochure.pdf.
- National Initiative for Cybersecurity Careers and Studies. (n.d.). NICE Cybersecurity Workforce Framework. https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework.
- Nhan, Johnny, Laura Huey, and Ryan Broll. (2017). Digilantism: An Analysis of Crowdsourcing and the Boston Marathon Bombings. *British Journal of Criminology*, Vol. 57, 341–361.
- North Atlantic Treaty Organization (NATO) Cooperative Cyber Defence Centre of Excellence. (2016). NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit. https://ccdcoe.org/nato-recognises-cyberspace-domain-operations-warsaw-summit.html.
- PBS. (2018). The FBI's cybersecurity brain drain has long-term implications, 4 August 2018. https://www.pbs.org/newshour/show/the-fbis-cybersecurity-brain-drain-has-long-term-implications.
- Pihelgas, Mauno. (2013). Back-tracing and Anonymity in Cyberspace. In Katharina Ziolkowski (ed.). *Peacetime Regime for State Activities in Cyberspace International Law, International Relations and Diplomacy* (pp. 31-60). NATO Cooperative Cyber Defence Centre of Excellence. http://www.ccdcoe.org/publications/books/Peacetime-Regime.pdf.
- Shore, M., Du, Y., & Zeadally, S. (2011). A Public-Private Partnership Model for National Cybersecurity. *Policy & Internet*, *3*(2), 1-23.
- Smeets, Max. (2018). Integrating offensive cyber capabilities: meaning dilemmas, and assessment. Defence Studies, Vol. 18(4), 395-410.
- Suciu, Peter. (2015). Cyber security's ever-growing brain drain. *Fortune*, 9 September 2015. http://fortune.com/2015/09/09/cyber-securitys-ever-growing-brain-drain/.
- Tcherni, Maria, Andrew Davies, Giza Lopes, and Alan Lizotte. (2016). The Dark Figure of Online Property Crime: Is Cyberspace Hiding a Crime Wave? *Justice Quarterly*, Vol. 33(5), 890-911.

- Tropina, Tatiana. (2009). Cyber-policing: The role of the police in fighting cybercrime. European Police Science and Research Bulletin, Special Conference Issue No. 2. https://bulletin.cepol.europa.eu/index.php/bulletin/article/download/232/200/.
- Исполнительный директорат Контртеррористического комитета Совета Безопасности Организации Объединенных Наций и Контртеррористическое управление Организации Объединенных Наций (2018). Защита критически важных объектов инфраструктуры от террористических нападений: Руководство по передовой практике. https://www.un.org/sc/ctc/wp-content/uploads/2018/06/Compendium-CIP-final-version-120618_new_fonts_18_june_2018_optimized.pdf.
- 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.
- УНП ООН (без даты) ШЕРЛОК https://sherloc.unodc.org/cld/v3/sherloc/.
- UNODC. (n.d.). Cybercrime Repository. https://www.unodc.org/unodc/en/cybercrime/cybercrime-repository.html.
- US National Initiative for Cybersecurity Careers and Studies (n.d.). Work Roles: Cyber Crime Investigator. https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework/workroles?name_selective=Cyber+Crime+Investigator&fwid=All.
- US Secret Service. (n.d.). Investigation. https://www.secretservice.gov/investigation/#.
- US Securities and Exchange Commission. (2018). Altaba, Formerly Known as Yahoo!, Charged With Failing to Disclose Massive Cybersecurity Breach; Agrees To Pay $35 Million. Press Release 2018-71. https://www.sec.gov/news/press-release/2018-71.
- Wall, David S. (2007). Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace. *Police Practice and Research*, Vol. 8(2), 183-205.

Законы

- Закон «О сплочении и укреплении Америки путём обеспечения надлежащими средствами, требуемыми для пресечения и воспрепятствования терроризму» («ПАТРИОТИЧЕСКИЙ акт»). (https://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf).

Упражнения

Упражнение №.1 ~ Кому вы собираетесь звонить?

Поручите своим учащимся изучить механизмы сообщения информации о киберпреступлении, существующие в их стране, до начала занятия. Учащиеся должны быть готовы к обсуждению ответов на нижеследующие вопросы на занятии.

Вопросы для обсуждения

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

Упражнение №.2 ~ Расследование гипотетического киберпреступления

Веб-сайт электронного банка E-Bank был отключен от сети, что препятствует доступу клиентов к веб-сайту. Вас наняли для проведения расследования киберпреступления. У вас есть подозрение, что имела место DDoS-атака.

Вопросы для обсуждения

- С какими препятствиями вы бы могли столкнуться при проведении своего расследования?
- Какие шаги вы предпримете, чтобы попытаться установить личность исполнителя или исполнителей этого киберпреступления?

Упражнение №.3 ~ Кто принимает меры реагирования?

Попросите своих учащихся провести исследование их страны и определить ведомства, принимающие участие в расследовании киберпреступлений. Учащиеся должны быть готовы к обсуждению ответов на нижеследующие вопросы на занятии.

Вопросы для обсуждения

- Кто расследует киберпреступления в вашей стране?
- Какова роль каждого ответственного и вовлечённого в проведение расследования киберпреступлений ведомства/субъекта?
- Какие киберпреступления расследуют эти ведомства/субъекты?
- Существуют ли механизмы государственно-частного партнерства для расследования киберпреступлений? Если да, то какие это механизмы?
- Применяются ли какие-либо методы управления знаниями к расследованиям киберпреступлений? Если да, то какие?

Упражнение №.4 ~ Общий регламент ЕС по защите данных (GDPR) и WHOIS

Попросите своих учащихся рассмотреть Общий регламент Европейского союза (ЕС) по защите данных (GDPR). Поручите учащимся провести исследование, чтобы определить влияние GDPR на доступность данных из WHOIS. Как это влияет на расследования киберпреступлений?

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

Сообщение информации о киберпреступлении

Лекция (30 минут):

- Обсудите и оцените практику сообщения информации о киберпреступлении

Попросите учащихся выполнить «Упражнение №.1 ~ Кому вы собираетесь звонить?» в разделе «Упражнения» данного модуля до начала занятия и попросите их обсудить результаты во время лекции.
[*Напоминание: это упражнение должно быть выполнено до начала занятия].

Кто проводит расследования киберпреступлений?

Лекция (40 минут):

- Определите и обсудите ведомства/субъекты, принимающие участие в расследованиях киберпреступлений

Попросите учащихся выполнить «Домашнее задание №.1 ~ Органы национальной безопасности и их роль в расследованиях киберпреступлений» в разделе «Оценка учащихся» до начала занятия и попросите их обсудить результаты во время лекции.

Перерыв

Время: 10 минут

Препятствия для расследований киберпреступлений

Лекция (50 минут):

- Разъясните и критически оцените препятствия, встречающиеся во время расследований киберпреступлений

Дайте учащимся задание выполнить «Упражнение №.2 ~ Расследование гипотетического киберпреступления» в разделе «Упражнения» данного модуля до начала занятия и попросите их обсудить результаты во время лекции.
[*Напоминание: это упражнение должно быть выполнено до начала занятия].

[*Альтернативный вариант*: попросите учащихся выполнить «Домашнее задание №.2 ~ Региональная Интернет-регистратура» в разделе «Оценка учащихся» 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 просто прийти подготовленными для обсуждения своих результатов на занятии].

[*Альтернативный вариант*: Поручите учащимся выполнить «Упражнение №.4 ~ Общий регламент ЕС по защите данных (GDPR) и WHOIS» 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 просто прийти подготовленными для обсуждения своих результатов на занятии].

Управление знаниями

Лекция (40 минут):

- Опишите роль управления знаниями в расследованиях киберпреступлений

Попросите учащихся выполнить «Упражнение №.3 ~ Кто принимает меры реагирования?» в разделе «Упражнения» данного модуля до начала занятия и попросите их обсудить результаты во время лекции.
[*Напоминание: это упражнение должно быть выполнено до начала занятия].

Список основной литературы

Учащимся следует ознакомиться со следующими публикациями (в основном доступными в открытых источниках), входящими в категорию обязательной для прочтения литературы, до начала занятий по данному модулю:

- Chang, Weiping and Peifang Chung. (2014). Knowledge Management in Cybercrime Investigation – A Case Study of Identifying Cybercrime Investigation Knowledge in Taiwan. *Pacific-Asia Workshop on Intelligence and Security Informatics* (PAISI 2014: Intelligence and Security Informatics), pp. 8-17.
- Domain Tools. Best Practices Guide: Getting Started with Domain Tools for Threat Intelligence and Incident Forensics. http://docs.apwg.org/sponsors_technical_papers/DomainTools-Guide-Cybercrime-Investigation.pdf.
- Fafinski, Stefan, William H. Dutton, and Helen Margetts. (2010). Mapping and Measuring Cybercrime. Oxford Internet Institute, University of Oxford. OII Forum Discussion Paper No 18. https://www.oii.ox.ac.uk/archive/downloads/publications/FD18.pdf.
- Finklea, Kristin. (2017). Dark Web. Congressional Research Service. https://fas.org/sgp/crs/misc/R44101.pdf.
- GLACY. (2014). Good practice study: Cybercrime reporting mechanisms. https://rm.coe.int/168030287c.

- Harkin, Diarmaid, Chad Whelan, and Lennon Chang (2018). The challenges facing specialist police cyber-crime units: an empirical analysis. *Police Practice and Research*, Vol. 19(6), 519-536.
- Lin, Herbert. (2017). Attribution of Malicious Cyber Incidents. Hoover Institution, Aegis Paper Series No. 1607. https://www.hoover.org/sites/default/files/research/docs/lin_webready.pdf.
- Maras, Marie-Helen. (2014). *Computer Forensics: Cybercriminals, Laws, and Evidence*. Jones and Bartlett; Chapters, 8-11.
- Pihelgas, Mauno. (2013). Back-tracing and Anonymity in Cyberspace. In Katharina Ziolkowski (ed.). *Peacetime Regime for State Activities in Cyberspace International Law, International Relations and Diplomacy* (pp. 31-60). NATO Cooperative Cyber Defence Centre of Excellence. http://www.ccdcoe.org/publications/books/Peacetime-Regime.pdf.
- Wall, David S. (2007). Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace. *Police Practice and Research*, 8(2), 183-205.

Список дополнительной литературы

Следующая литература рекомендуется учащимся, заинтересованным в более детальном изучении тематических вопросов, охваченных данным модулем:

- CISCO. (n.d.). Understanding the Ping and Traceroute Commands. https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-software-releases-121-mainline/12778-ping-traceroute.pdf.
- Hilgenstieler, Egon, Elias P. Duarte, Glenn Mansfield-Keeni, and Norio Shiratori. (2010).
- Extensions to the source path isolation engine for precise and efficient log-based IP traceback. *Computers & Security*, Vol. 29(4), 383-392.
- 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.
- Kao, Da-Yu and Wang, Shiuh-Jeng. (2009). The IP address and time in cyber-crime investigation. *Policing: An International Journal*, Vol. 32(2), 194-208.

- Maras, Marie-Helen. (2014). *Computer Forensics: Cybercriminals, Laws, and Evidence*. Jones and Bartlett; Chapter 12.
- Nur, Abdullah Yasin and Tozal, Mehmet Engin. (2018). Record route IP traceback: Combating DoS attacks and the variants. *Computers & Security*, Vol. 72, 13-25
- Singh, Karanpreet, Paramvir Singh, and Krishan Kumar. (2016). A systematic review of IP traceback schemes for denial of service attacks. Computers & Security, Vol. 56, 111-139.
- Steenbergen, Richard A. and Roisman, Dani. (2016). A Practical Guide to (Correctly) Troubleshooting with Traceroute. https://www.arin.net/vault/participate/meetings/on-the-road/presentations/waterloo2016/10_roisman.pdf.
- 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.
- World Economic Forum. (2016). Recommendations for Public-Private Partnership against Cybercrime. http://www3.weforum.org/docs/WEF_Cybercrime_Principles.pdf.

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. Куда направляется сообщение о киберпреступлении?
2. Почему не все случаи киберпреступлений сообщаются?
3. Кто расследует киберпреступления?
4. Что представляют собой государственно-частные партнерства? С какой целью они создаются для расследования киберпреступлений?
5. Какие препятствия встречаются во время расследования киберпреступлений?
6. Что такое управление знаниями? В чем заключаются преимущества управления знаниями?

7. Как процессы управления знаниями могут применяться к расследованиям киберпреступлений?

Домашнее задание

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: Органы национальной безопасности и их роль в расследованиях киберпреступлений

Какие органы национальной безопасности принимают участие в расследовании киберпреступлений в вашей стране? Какую роль играет этот орган (или органы) в расследовании киберпреступлений? Попросите учащихся объяснить их ответы с использованием доводов, основанных на фактах, которые находят подтверждение в публикациях из списка основной и/или дополнительной литературы.

Домашнее задание №.2: Региональная Интернет-регистратура

Попросите учащихся провести исследование их региональной Интернет-регистратуры

- Какова роль РИР?
- Какие ресурсы она предлагает?
- Как эти ресурсы могут использоваться при расследованиях киберпреступлений?

Дополнительные средства обучения

Вебсайты

- Проект «Противодействие киберпреступности» (Украина). http://anticyber.com.ua.
- Cyber Crime Cell (India), Where to make a complaint. http://www.cybercelldelhi.in/Report.html.
- European Cybercrime Centre. (EC3)

https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

- Europol. (n.d.). Reporting Cybercrime Online. https://www.europol.europa.eu/report-a-crime/report-cybercrime-online.
- Freenet. https://freenetproject.org/author/freenet-project-inc.html.
- Global Cyber Security Capacity Centre. https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/front.
- I2P. https://geti2p.net/en/.
- INHOPE. http://www.inhope.org/gns/home.aspx.
- Internet Signalement (France). https://www.internet-signalement.gouv.fr/PortailWeb/planets/Accueil!input.action.
- National Cyber Security Centrum (Netherlands). https://www.ncsc.nl/.
- No More Ransom Project. https://www.nomoreransom.org/en/index.html.
- Stop Fraud. https://cyberpolice.gov.ua/stopfraud/.
- Tor Project. https://www.torproject.org/about/overview.html.en.
- УНП ООН, Глобальная программа по борьбе с киберпреступностью. https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html.
- УНП ООН, ШЕРЛОК. https://sherloc.unodc.org/cld/v3/sherloc/.
- UNODC, Cybercrime Repository. https://www.unodc.org/unodc/en/cybercrime/cybercrime-repository.html.
- Ward, Mark. (2018). Cyber-attack! Would your firm handle it better than this? *BBC News*, 7 August 2018. https://www.bbc.com/news/technology-44482380.

Видео

- ACORN - Report Cybercrime (продолжительность: 0:37) https://www.youtube.com/watch?v=m1_j71Qz8Yg
  >> Это видео является примером австралийской национальной кампании по поощрению сообщений о киберпреступлениях.
- US FBI, The FBI's cybersecurity brain drain has long-term implications (продолжительность: 3:56). https://www.pbs.org/newshour/show/the-fbis-cybersecurity-brain-drain-has-long-term-implications.

>> На этом видео обсуждаются последствия потери базы знаний вследствие ухода ключевых специалистов по кибербезопасности из ФБР.

- US FBI, Reporting Cyber Crime is as Easy as IC3 (продолжительность: 0:32). https://www.youtube.com/watch?v=nD7XQ1yjgB0.
  >> Это видео является примером национальной кампании по поощрению сообщений о киберпреступлениях.

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