DOI 10.35264/1996-2274-2019-2-80-87

ПРЕСТУПНОСТЬ В КИБЕРПРОСТРАНСТВЕ

Я.С. Тейван-Трейновский, дек. фак. Даугавпилсского университета (Латвия, Даугавпилс), д-р юрид. наук, эксперт Научного совета Латвии, проф., *janis.teivans@du.lv*
Д.А. Игнатов, лект. каф. Даугавпилсского университета (Латвия, Даугавпилс), *deniss.ignatovs@gmail.com*

Рецензент: В. Меньшиков

Согласно данным Евростата, в 2017 г. доступ к Интернету в Евросоюзе имели 85% домашних хозяйств и 97% предприятий, в то время как в 2010 г. доступ к Интернету в Евросоюзе имели лишь 70% домашних хозяйств. Следует отметить, что это достаточно спорное достижение, учитывая то, что в киберпространство ворвалось достаточно большое количество дилетантов, зачастую становящихся жертвами киберпреступности и ее «спонсорами». Потери мировой экономики от киберпреступности в 2017 г. составили 600 млрд долл., что является 25%-ным ростом по отношению к 2014 г. Учитывая глобальный характер этой тенденции, обусловленный отсутствием границ в киберпространстве, в ближайшее время общество столкнется с серьезными вызовами в сфере обеспечения информационной безопасности общества и отдельных граждан. Решение этой проблемы требует глубокого анализа динамики преступности в информационной среде и возможностей эффективного сдерживания его развития.

Ключевые слова: киберпространство, киберпреступность, преступление, информационная безопасность, сеть.

CRIME IN CYBERSPACE

Ya.S. Teivan-Treinovsky, Dean of Faculty, Daugavpils University (Latvia, Daugavpils), Ph.D., Expert of the Scientific Council of Latvia, professor, *janis.teivans@du.lv*
D.A. Ignatov, Lecturer, Daugavpils University (Latvia, Daugavpils), *deniss.ignatovs@gmail.com*

According to Eurostat, in 2017, 85% of households and 97% of enterprises had access to the Internet in the European Union, while in 2010 only 70% of households had access to the Internet in the European Union. It should be noted that this is a rather controversial achievement, given that a sufficiently large number of amateurs broke into cyberspace, often becoming victims of cybercrime and its «sponsors». The loss of the global economy from cybercrime in 2017 amounted to 600 billion dollars, which is a 25% increase compared to 2014. Given the global nature of this trend, due to the lack of borders in cyberspace, society will soon face serious challenges in ensuring the information security of society and individuals. Solving this problem requires a deep analysis of the dynamics of crime in the information environment and the possibilities for effectively deterring its development.

Keywords: cyberspace, cybercrime, crime, information security, web.

Относительным неологизмом в сфере уголовного права является само понятие киберпреступности. Данная сфера уголовно наказуемых деяний появилась одновременно с развитием информационных технологий, а также с появлением практически неограниченного доступа населения к компьютерной технике и возможности свободного выхода в сети общего пользования.

Возникновение виртуального или киберпространства создало благоприятную среду для реализации уголовно наказуемых деяний, которые невозможны в реальном мире [14, с. 19].

Учитывая связанное с этим изменение реалий, актуализировалась проблема понятия преступления, и в особенности киберпреступления. Было высказано утверждение, что само понятие киберпреступления является не чем иным, как указанием на наличие вредоносного поведения, так или иначе связанного с компьютером. Спустя 10 лет этот аргумент остается верным для многих стран, которые до сих пор имеют в своих конституциях очень смутные представления о киберпреступности [11, с. 150]. Данное определение, несомненно, объясняет суть киберпреступления, однако формулировка является настолько общей, что не позволяет понять всю суть нового явления, которое постепенно проникает во все сферы жизни.

Более детальное определение киберпреступности формулируется следующим образом: киберпреступление – это виновно совершенное общественно опасное уголовно наказуемое вмешательство в работу компьютеров, компьютерных программ, компьютерных сетей, несанкционированная модификация компьютерных данных, а также иное противоправное общественно опасное деяние, совершенное с помощью или посредством компьютеров, компьютерных сетей и программ, а также с помощью или посредством иных устройств доступа к моделируемому с помощью компьютера информационному пространству [8, с. 1]. Данное определение киберпреступления, которое в своей диссертации дает кандидат юридических наук Т. Тропина, является практически исчерпывающим, однако следует также добавить, что преступления, совершаемые в сфере телефонии, также можно отнести к области киберпреступлений.

Термин «киберпреступность» в настоящее время часто употребляется наряду с термином «компьютерная преступность», причем нередко эти понятия используются как синонимы [5, с. 47].

Киберпреступления различаются по своим целям, объектам воздействия, способам и средствам совершения противоправного действия. В соответствии с выделенными основаниями киберпреступления по критерию цели совершения делятся на:

– экономические;
– политические;
– идеологические;
– социально-психологические.

Чаще всего киберпреступления совершают ради экономических целей. Это может быть, например, нанесение экономического ущерба в виде хищения денежных средств и конфиденциальной информации. К другим видам целей относятся политические: нанесение ущерба основным государственным и политическим институтам, подрывающее систему властных отношений и доверие к власти. Третий вид целей – идеологические: распространение идей и идеология в целях вербовки интернет-пользователей в ряды, например, радикально террористических и националистических группировок. К четвертому виду целей относятся социально-психологические, такие как нанесение морального и психологического вреда гражданам [3, с. 47].

Министерство юстиции США, имеющее наиболее длительный опыт борьбы с данным видом преступности, все киберпреступления разделяет на три группы: к первой группе относятся преступления, объектом посягательства которых являются компьютерные устройства, в качестве примера такого преступления может служить несанкционированный доступ к сетям различного типа; второй тип киберпреступлений – это действия с компьютерными устройствами, при которых компьютерная техника используется как оружие, например создание условий, при которых пользователи не могут получить доступ к необходимому информационному объекту (denail-of-Service DoS), и к третьей группе относятся преступления, в которых компьютер используется как устройство для хранения запрещенных данных [12, с. 1].

С позиции системного подхода такую классификацию можно было бы считать ущербной, так как абсолютно нелогичным кажется отсутствие единых критериев. Зачастую такой подход характерен для уголовного права стран англосаксонской системы, однако это не мешает достаточно эффективному отправлению правосудия в этих странах.

Установить точный день, когда впервые был упомянут термин «киберпреступление», достаточно проблематично, однако первые упоминания о киберпреступлениях появились уже в 70-х гг. XX в. Так, согласно данным портала [10, с. 1] в 1971 г. Джон Драпер (John Draper) смог «обмануть» телефонную сеть и совершать бесплатные телефонные междугородные звонки. Утверждать, что именно это преступление явилось первым в киберпространстве, – сложно, но сказать, что оно было одним из первых, можно с большой долей вероятности. Дальнейшее развитие киберпреступлений напоминало лавину, которая постепенно захватывала все большие сферы жизнедеятельности человека. Второй этап развития киберпреступности связан с появлением компьютерных преступлений, субкультуры хакеров и с количественным ростом преступности в глобальной сети. На тот момент киберпреступления осуществлялись лишь ограниченным кругом специалистов. Первым зафиксированным интернет-взломом было преступное деяние, совершенное группой несовершеннолетних подростков, называющих себя «©группа 414[a]». В течение девяти суток «©группа 414[a]» взломала более 60 ПК, среди которых были компьютеры Лос-Аламосской государственной лаборатории, занимающейся исследованием ядерного оружия. В это же время срочно создается Центр исследования интернет-безопасности CERT для фиксирования и исследования нового вида преступности [2, с. 882]. Стоит отметить, что киберпреступность Латвии также имеет «детское лицо». Так, согласно данным, приводимым начальником 3-го отдела Управления по борьбе с экономическими преступлениями Государственной полиции Латвии Дмитрия Хоменко, большинство всех кибернападений, раскрытых в Латвии, совершаются именно несовершеннолетними [4, с. 1].

Волна киберпреступлений постепенно стала охватывать все больше сфер общественной жизни, в результате чего как перед государством в целом, так и перед отдельными компаниями встал вопрос о защите своих информационных систем от кибератак.

В отличие от традиционного преступления, которое совершается в одном географическом месте, киберпреступление совершается в Интернете, и оно часто не имеет четкой связи с каким-либо географическим местоположением [6, с. 226]. Поэтому требуется скоординированный глобальный ответ на проблему киберпреступности. Во многом это связано с тем, что существует ряд проблем, которые препятствуют эффективному сокращению киберпреступности. Некоторые из основных проблем возникают в результате недостатков технологии, законодательства и киберкриминологии [11, с. 152].

Для того чтобы оценить объем киберпространства и понять, какие масштабы оно способно охватить, необходимо проанализировать статистику использования Интернета в мире.

Учитывая тот факт, что киберпреступления стали затрагивать почти все сферы жизнедеятельности, перед теоретиками уголовного права возникла необходимость разделения всех преступлений в информационной среде на отдельные группы, что позволило бы более эффективно противодействовать каждому из них.

Однако, прежде чем делить данные преступления на отдельные типы, необходимо оценить потенциальную аудиторию киберпреступников, проанализировать статистические данные по использованию Интернета в различных странах (табл. 1).

Данные об использовании Интернета приведены за 2016 г., они получены на интернет-портале: www.internetlivestats.com [13, с. 1].

Анализируя приведенные данные, можно прийти к выводу, что на 2016 г. в странах с развитой экономикой и относительно высоким уровнем жизни доступ к Интернету имели в среднем 82,73 % населения. Однако не стоит забывать, что общемировая статистика, согласно данным того же портала, говорит о том, что общее число пользователей Интернета со-

ставляет примерно 58,5% от всего населения Земли. Стоит учитывать, что основную массу этих людей составляют именно жители развитых стран.

Таблица 1

Статистические данные по использованию Интернета в различных странах

Страна	Количество интернет-пользователей		Общее население	Изменение количества пользователей Интернета, %
	чел.	% от общего населения		
Латвия	1,491,951	76,3	1,955,742	−0,5
Литва	2,199,938	77,2	2,850,030	1,1
Эстония	1,196,521	91,4	1,309,104	2,2
Россия	102,258,256	71,3	143,439,832	0,3
США	286,942,362	88,5	324,118,787	1,1
Германия	71,016,605	88,0	80,682,351	0,6
Франция	55,860,330	86,4	64,668,129	1,4

Необходимо отметить, что незначительный годовой прирост среди пользователей Интернета в развитых странах говорит о том, что на данный момент количество пользователей находится практически на грани максимального значения. Что же касается Латвии, то, как видно из таблицы, количество пользователей даже снижается. К сожалению, Латвия входит в список трех стран, в которых в 2016 г. число пользователей Интернета сократилось. С уверенностью можно утверждать, что данная ситуация связана с демографическими проблемами, и в первую очередь со старением населения.

Рассматривая данную статистику в контексте киберпреступлений, становится понятно, что именно это и есть целевая аудитория киберпреступников.

Возвращаясь к вопросу разделения всех киберпреступлений на отдельные группы, следует обратиться к Европейской конвенции по киберпреступлениям, которая была принята в Будапеште 23.11.2001. Анализируя данную Конвенцию и руководствуясь ее второй главой, все виды киберпреступлений можно разделить на группы и подгруппы:

1. Преступления против конфиденциальности, целостности и доступности компьютерных данных и систем:
– незаконный доступ;
– незаконный перехват;
– вмешательство в данные;
– вмешательство в систему;
– ненадлежащее использование устройств.
2. Преступления, связанные с компьютерами:
– подлог компьютерных данных;
– компьютерное мошенничество.
3. Правонарушения, связанные с содержанием:
– преступления, связанные с детской порнографией.
4. Преступления, связанные с нарушением авторского права и смежных прав:
– нарушения, связанные с нарушениями авторских и смежных прав [1, ст. 1–10].

Угрозу безопасности имуществу в сети, как правило, создают три основных направлений киберпреступности:

– кража финансовых средств непосредственно со счетов с использованием специализированных программ;
– мошенничество с ложным предложением товаров и услуг;
– кража личных данных с последующим использованием их в разных операциях.

Но имущественные преступления не являются единственной угрозой в сети. Угрозам подвергаются приватность лиц, нравственность пользователей (детская порнография) и, в некоторых случаях, общественная безопасность, так как все чаще сеть используется в целях пропаганды и дестабилизации ситуации в обществе различными радикальными группировками.

Не менее актуальной проблемой является культивация межэтнической, межконфессиональной и другой розни в Интернете, а также публикация заведомо ложной резонансной информации.

Из всего этого следует, что наша зависимость от Интернета делает общество уязвимым. Основной риск здесь – киберпреступность, которая может принимать разнообразные формы:

– спектр повседневных угроз обширен: от спама до вирусов, хакерства, кражи личных данных, мошенничества и сексуальных домогательств в отношении детей;

– потенциальные угрозы включают кибертерроризм, т.е. разрушение основной инфраструктуры или использование компьютеров как оружия для блокировки важнейших систем или создания угрозы для целых групп населения;

– информационно-коммуникационные технологии предоставляют тем, кто вовлечен в организованную преступность, новые инструменты для совершения преступлений старого типа, а также возможности для новых форм преступности;

– группы организованной преступности используют Интернет для широкомасштабного мошенничества и краж. Для облегчения своей преступной деятельности они могут воспользоваться различиями в юридических системах разных стран;

– Интернет облегчает отмывание денег, получаемых от «традиционных» преступлений: эти методы включают выставление завышенных или заниженных счетов и кибераукционы. Электронные банки облегчают для преступников передвижение потоков «грязных денег»;

– Интернет также позволяет преступникам действовать анонимно и создавать сети с другими преступниками [7, ст. 1].

Это означает, что в последние годы существенно усилились риски, связанные с отрицательным воздействием возрастания вовлеченности в интернет-среду на криминогенную обстановку.

Развитие киберпреступности оказывает существенное отрицательное воздействие на научно-технический прогресс. В определенном плане это оказало тормозящее воздействие на развитие информационного общества.

Поиск предложения товаров и услуг в сети продолжает расти, однако стала наблюдаться тенденция роста расчетов в очном порядке.

Для успешного противодействия киберпреступности необходима четкая нормативная база. Возникает закономерный вопрос, как привлечь специалистов в правоохранительные органы и как им обеспечить достойное вознаграждение, чтобы поддержать мотивацию на достойном уровне. Законодательство очень многих государств (тут называют Беларусь, Болгарию, Индонезию, Македонию, Молдавию, Украину, Таиланд) заметно опаздывает, так что некоторые деяния вполне могут оказаться за рамками уголовного кодекса. В итоге преступники или остаются безнаказанными или, что называется, отделываются легким испугом. К тому же эти преступления не связаны с насилием, что нередко вводит в заблуждение судей и прокуроров, даже если речь идет о хищении очень больших сумм. По-настоящему безжалостны к киберпреступникам лишь в Китае и США [9, с. 1].

Несмотря на то что такие понятия, как виртуальное пространство и киберпреступления, прочно вошли в наш быт, большинство людей до сих пор в полной мере не осознают потенциальные риски, которым они могут быть подвержены. В современном мире полностью исключить виртуальное пространство из жизни просто невозможно. В виртуальном мире расположены развлечения, работа, финансы и многие другие сферы нашей жизни, поэтому вопрос безопасности киберпространства является краеугольным камнем общей безопасности как отдельного человека, так и всего общества в целом.

Расследование киберпреступлений является достаточно трудоемким мероприятием, которое требует от лица, которое уполномочено вести уголовный процесс, знаний не только в сфере уголовного или уголовно-процессуального права, но и в сфере информационных технологий. Возникает закономерный вопрос, где взять такого специалиста или каким образом его мотивировать для работы в правоохранительных органах, учитывая тот факт, что финансовое вознаграждение в данной сфере в частном секторе является более конкурентоспособным.

При расследовании дел данной категории основным источником доказательной базы, как правило, служат различные электронные носители, где хранится либо хранилась информация, либо те же электронно-вычислительные механизмы, с помощью которых производились различного рода противоправные действия.

Согласно данным сайта бюро государственных судебных экспертиз Латвии, для проведения экспертизы в сфере информационных технологий необходим срок продолжительностью до 5 недель, при условии, что в постановлении о проведении экспертизы указана веская причина, по которой данный случай можно считать чрезвычайным. Однако если событие не имеет статус чрезвычайного, то продолжительность экспертизы может составлять до 35 недель. Кроме того, для осмотра носителей данных необходимо до 16 недель – это 3,5 месяца [15, с. 1]. Стоит отметить, что сроки проведения данных экспертиз не соответствуют запросам времени. В ходе проведения экспертизы ее объект, учитывая скорость развития технологий, особенно в сфере компьютерной техники, может серьезно видоизмениться.

Имеет ли данная проблема эффективное решение – вопрос неоднозначный. Определенно можно утверждать лишь то, что для небольших стран с ограниченными ресурсами решение данной задачи является непосильным, и одной из возможных мер могло бы явиться создание международного экспертного центра в сфере информационных технологий. Данное решение могло бы повысить престиж профессии эксперта в сфере информационных технологий, обеспечить достойное и мотивирующее вознаграждение за данную работу, а также обеспечить более быстрый обмен опытом между специалистами разных стран.

Невзирая на развитие средств расследования киберпреступлений, основным направлением все-таки должна считаться профилактическая деятельность.

Развитие электронной коммерции, ее реклама, электронные переводы, денежные переводы включают много правовых аспектов, которые необходимо учитывать при ведении данного вида бизнеса.

Правовое регулирование электронной коммерции (которая является наиболее частым объектом противоправного воздействия) в странах Европы постоянно совершенствуется.

Перед тем как регистрировать интернет-страницу, которая будет использоваться для ведения бизнеса, необходимо зарегистрировать соответствующий домен и торговую марку. Постепенно происходит свертывание института анонимности и усиления ответственности в Интернете.

Активное расширение использования интернет-пространства обусловлено прежде всего развитием технологий, а также широкими возможностями для ведения бизнеса. Технологии в данной ситуации играют роль как возможностей, так и угроз для интернет-коммерции.

С одной стороны, развитие технологий усугубляет модернизацию правовых предписаний и регулирований интернет-среды, с другой стороны, технологии предлагают способы устранения возможных угроз в среде безопасности, целостности и подлинности электронных данных.

Освоение пользователями Интернета основных правил безопасного функционирования в интернет-среде позволяет минимизировать данные риски и сосредоточиться на получении желаемого результата.

Более того, развитие информационного общества само по себе обусловливает создание безопасных систем, повышение уровня образованности населения, что, в свою очередь, оказывает прямое воздействие на правовую культуру и, как следствие, на снижение уровня преступности.

Список литературы

1. Европейская конвенция по киберпреступлениям (преступлениям в киберпространстве). Будапешт. 23.11.2001. URL: http://www.alppp.ru/law/pravosudie/46/konvencija-o-prestupnosti-v-sfere-kompyuternoj-informacii-185-rus-angl.html (дата обращения: 21.05.2019).

2. Зверянская Л.П. Исторический анализ этапов развития киберпреступности и особенности современных киберпреступлений // Науч.-метод. эл. журнал «Концепт». 2016. Т. 15. С. 881–885. URL: http://e-koncept.ru/2016/96090.htm (дата обращения: 21.05.2019).

3. Карпова Д.Н. Киберпреступность: глобальная проблема и ее решения // Власть. 2014. № 8. С. 46–50. URL: https://cyberleninka.ru/article/v/kiberprestupnost-globalnaya-problema-i-ee-reshenie (дата обращения: 21.05.2019).

4. Материалы интервью начальника 3-го отдела Управления по борьбе с экономическими преступлениями Госполиции Латвии Дмитрия Хоменко. URL: http://lr4.lsm.lv/lv/raksts/domskaja-ploschad/u-kiberprestupnosti-v-latvii-detskoe-lico.a83704 (дата обращения: 21.05.2019).

5. Номоконов В.А., Тропина Т.Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. 2012. С. 45–55. URL: https://cyberleninka.ru/article/v/kiberprestupnost-kak-novaya-kriminalnaya-ugroza (дата обращения: 21.05.2019).

6. Серго А.Г. Интернет и право. М.: Бестселлер, 2003. 272 с.

7. Совет Европы и киберпреступность. Основные моменты. 2019. URL: http://www.coe.int/t/DC/Files/Source/FS_cybercrime_ru.doc (дата обращения: 21.05.2019).

8. Тропина Т.В. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы / дисс. и автореф. по ВАК РФ, 12.00.08. Владивосток, 2005. URL: http://www.dissercat.com/content/kiberprestupnost-ponyatie-sostoyanie-ugolovno-pravovye-mery-borby (дата обращения: 21.05.2019).

9. Шпунт Я.Б. Борьба с киберпреступностью. Российский опыт – успехи и проблемы // Intelligent enterprise. 2013. № 5 (251). URL: https://www.iemag.ru/analitics/detail.php?ID=28571 (дата обращения: 21.05.2019).

10. An Abridged History Of Cyber Crime. Le VPN. 2018. URL: https://www.le-vpn.com/history-cyber-crime-origin-evolution (дата обращения: 21.05.2019).

11. Cyber Crime and Cyber Terrorism Investigator's Handbook, Chapter. 12. Publisher: Elsevier Science, Editors: Francesca Bosco, Andrew Staniforth, Babak Akhgar, p. 149–164. 2014.

12. Ferguson K., Rosencrance L. and Cobb M. 2019. URL: https://searchsecurity.techtarget.com/definition/cybercrime (дата обращения: 21.05.2019).

13. Internet Users by Country. 2016. URL: http://www.internetlivestats.com/internet-users-by-country (дата обращения: 21.05.2019).

14. Ķinis U. Kibernoziedzība, kibernoziegumiunjurisdikcija. JUMAVA 2015. P. 51–8l.

15. Valsts tiesu ekspertīžu birojs. Jaunākā informācija par ekspertīžu termiņiem. 2019. URL: http://www.vteb.gov.lv/aktualitates/553 (дата обращения: 21.05.2019).

References

1. *Evropeyskaya konventsiya po kiberprestupleniyam (prestupleniyam v kiberprostranstve)* [European Convention on Cybercrime (crimes in cyberspace)]. Budapest, 23.11.2001. Available at: http://www.alppp.ru/law/pravosudie/46/konvencija-o-prestupnosti-v-sfere-kompyuternoj-informacii-185-rus-angl.html (appeal date: 21.05.2019).

2. Zveryanskaya L.P. (2016) *Istoricheskiy analiz etapov razvitiya kiberprestupnosti i osobennosti sovremennykh kiberprestupleniy* [Historical analysis of the stages of development of cybercrime and features of modern cybercrime] *Nauch.-metod. el. zhurnal «Kontsept»* [Scientific-method. «Concept» electronic magazine]. V. 15. P. 881–885. Available at: http://e-koncept.ru/2016/96090.htm (appeal date: 21.05.2019).

3. Karpov D.N. (2014) *Kiberprestupnost': global'naya problema i ee resheniya* [Cybercrime: a global problem and its solutions] *Vlast'* [Power] No. 8. P. 46–50. Available at: https://cyberleninka.ru/article/v/kiberprestupnost-globalnaya-problema-i-ee-reshenie (appeal date: 21.05.2019).

4. *Materialy interv'yu nachal'nika 3-go otdela Upravleniya po bor'be s ekonomicheskimi prestupleniyami Gospolitsii Latvii Dmitriya Khomenko* [Materials interviewed by the head of the 3rd Division of the Office for Combating Economic Crimes of the State Police of Latvia, Dmitry Khomenko]. Available at: http://lr4.lsm.lv/lv/raksts/domskaja-ploschad/u-kiberprestupnosti-v-latvii-detskoe-lico.a83704 (appeal date: 21.05.2019).

5. Nomokonov V.A., Tropina T.L. (2012) *Kiberprestupnost' kak novaya kriminal'naya ugroza [Cybercrime as a new criminal threat] Kriminologiya: vchera, segodnya, zavtra* [Criminology: yesterday, today, tomorrow]. P. 45–55. Available at: https://cyberleninka.ru/article/v/kiberprestupnost-kak-novaya-krimi-nalnaya-ugroza (appeal date: 21.05.2019).

6. Sergo A.G. (2003) *Internet i pravo* [Internet and law] *Bestseller* [Bestseller]. Moscow. P. 272.

7. *Sovet Evropy i kiberprestupnost' (2019)* [Council of Europe and cybercrime] *Osnovnye momenty* [Highlights]. Available at: http://www.coe.int/t/DC/Files/Source/FS_cybercrime_ru.doc (access date: 21.05.2019).

8. Tropina T.V. (2005) *Kiberprestupnost': ponyatie, sostoyanie, ugolovno-pravovye mery bor'by* [Cybercrime: concept, state, criminal law measures of struggle] *Diss. i avtoref. po VAK RF* [Diss. and abstract. in the HAC RF]. 12.00.08. Vladivostok. Available at: http://www.dissercat.com/content/kiberprestupnost-ponyatie-sostoyanie-ugolovno-pravovye-mery-borby (appeal date: 21.05.2019).

9. Shpunt Ya.B. (2013) *Bor'ba s kiberprestupnost'yu* [Fighting cybercrime] *Rossiyskiy opyt – uspekhi i problem* [Russian experience – successes and problems]. Intelligent enterprise. 2013. No. 5 (251). Available at: https://www.iemag.ru/analitics/detail.php?ID=28571 (appeal date: 21.05.2019).

10. An Abridged History of Cyber Crime. Le VPN (2018). Available at: https://www.le-vpn.com/history-cyber-crime-origin-evolution (appeal date: 21.05.2019).

11. Cyber Crime and Cyber Terrorism Investigator's Handbook, Chapter. 12 (2014) Publisher: Elsevier Science, Editors: Francesca Bosco, Andrew Staniforth, Babak Akhgar. P. 149–164.

12. Ferguson K., Rosencrance L. and Cobb M. (2019). Available at: https://searchsecurity.techtarget.com/definition/cybercrime (appeal date: 21.05.2019).

13. Internet Users by Country. 2016. Available at: http://www.internetlivestats.com/internet-users-by-country (appeal date: 21.05.2019).

14. Ķinis U. (2015) Kibernoziedzība, kibernoziegumiunjurisdikcija. JUMAVA. P. 51–8l.

15. Valsts tiesu ekspertīžu birojs. Jaunākā informācija par ekspertīu termiņiem (2019). Available at: http://www.vteb.gov.lv/aktualitates/553 (appeal date: 21.05.2019).