Р.А. Медиев
С.А. Августхан

Актуальность создания автоматизированной компьютерной системы для повышения эффективности фиксации цифровых следов в сети Интернет

Актуальность противодействия преступлениям, совершаемым с использованием сети Интернет и электронных информационных ресурсов, растет с каждым годом во всем мире.

Эта тенденция связана с глобальной цифровизацией всех структур жизнедеятельности человека и ростом пользователей.

Вопросы противодействия такому виду преступности находится на особом контроле руководства страны Республики Казахстан, создаются уполномоченные органы, структурные подразделения, внедряются государственные программы.

Примером тому является создание 30 июня 2017 года системы «Киберщит Казахстана» для достижения и поддержания уровня защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз, обеспечивающих

[1]Сазонов А.И. Современные возможности Главного управления криминалистики (Криминалистического центра) в сфере технико-криминалистического обеспечения расследования преступлений// Вестник Главного управления криминалистики (криминалистического центра), ноябрь 2022, № 11 (80) с. 15-16.

устойчивое развитие Республики Казахстан в условиях глобальной конкуренции[1].

Основополагающие концепцией многих программ по кибербезопасности, является база использования системы классификации способов совершения уголовных правонарушений в сфере современных цифровых технологий, являющийся кодификатор Генерального секретариата Интерпола, где отдельно предусмотрена классификация компьютерных преступлений[2].

В Европе, еще в 2001 году была подписана Конвенция Совета Европы о преступности в сфере компьютерной информации ETS № 185[3], которая более известна в Казахстане под условным названием «Конвенция о киберпреступлениях». Кроме того, Европейским комитетом по проблемам преступности Совета Европы в 1990 году, с целью определения в Европе преступлений, связанных с использованием современных компьютерных и информационных технологий, были подготовлены рекомендации о включении в законодательство европейских стран уголовных норм «минимального списка» и «необязательного списка» в отношении кберпреступлений. Все указанные законы, конвенции и подзаконные акты содержат в себе определение и классификацию различных правонарушений в сфере цифровых технологии.

Однако надо отметить, что самой большой проблемой в сфере расследования преступлений совершенных в сети Интернет, является выявление и фиксации цифровых следов правонарушения. Это связано с тем, что в случае, когда хаккер совершает противоправные действия на отдельно взятом компьютере потерпевшего лица или использует для этого свой компьютер, то даже после удаления с компьютера цифровых следов правонарушения, следственно-оперативная группа все равно может цифровые данные найти,

---

[1]. Постановление Правительства Республики Казахстан № 676 «Об утверждении Плана мероприятий по реализации Концепции кибербезопасности ("Киберщит Казахстана") до 2022 года» от 28 октября 2017 года https://adilet.zan.kz/rus/docs/P1700000676

[2]. Указ Президента Республики Казахстан № 897 «Об утверждении Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации» от 25 июня 2002 года. https://adilet.zan.kz/rus/docs/U020000897_

[3]. Классификация компьютерных преступлений по кодификатору международной уголовной полиции генерального секретариата Интерпола. http://surl.li/ghugp

восстановить и изъять в качестве доказательств. Другое дело, когда следы правонарушения находятся в сети Интернет.

Это может быть переписка между преступниками, или переписка между преступником и потерпевшим лицом. Также это могут быть материалы ксенофобного, или порнографического характера. В случае, если преступник удалит информацию преступного направление с интернет ресурса, то в таких случаях уже возникают проблемы сохранения информации, интересующей сотрудников правоохранительных органов, ведь компьютер, на котором физически была размещена информация преступного направления может находиться, например, в Аргентине, и изъять его для проведения экспертизы будет затруднено, а в большинстве случаев даже невозможно.

На сегодняшний день на территории Республики Казахстана сложилась такая практика фиксации следов правонарушения в сети Интернет, как изготовление в присутствии понятых цифрового снимка «print screen» экрана монитора компьютера, на котором отображается интернет ресурс со следами правонарушения, после чего данное изображение распечатывается, и приобщаются к другим материалам уголовного дела, а сами страницы Интернет ресурса сохраняются на жесткий диск, а затем записываются на CDR или DVDR диск. Но в случае удаления информации преступного характера со страниц интернет ресурса, описанный выше цифровой снимок теряет свою процессуальную силу.

Для того, чтобы упростить процедуру изготовления цифрового снимка «print screen» экрана монитора компьютера, на котором отображается интернет ресурс со следами правонарушения, и использовать его, как один из видов доказательства во время досудебного расследования, нами предлагается создать программное обеспечение для функционирования автоматизированной компьютерной системы (далее - программное обеспечение АКС).

Данное программное обеспечение АКС должна основываться на определенных принципах, и иметь в себе информационные блоки, отдельно, так например:

1) Программное обеспечение АКС должна иметь блок взаимодействия с Единым реестром досудебного расследования (далее - ЕРДР), где должна иметь вид блока расширения функций указанного ЕРДР. То есть вход в такую систему лицом, производящее

досудебное расследование должен быть осуществлен с использованием кодов доступа в ЕРДР;

2) Программное обеспечение АКС должна иметь автоматизированный блок изготовления электронного снимка «print screen» любой части или страницы интернет ресурса, а также автоматизированный блок сохранения всей информации, находящейся в любой части или странице интернет ресурса. При таких условиях лицу, производящее досудебное расследование необходимо лишь ввести в данную систему ссылку на тот или иной интернет ресурс на котором есть информация правонарушения, а программное обеспечение АКС уже без участия человека предпримет выше указанные действия с таким интернет ресурсом;

3) Изготовленный цифровой снимок «print screen», а также вся сохраненная информация из любой части или страницы интернет ресурса (например, текст, графическая, аудио и видео информация), должны храниться в виде отдельных разделов данных, которые должны маркироваться с указанием:

- даты создания раздела базы данных;
- номера уголовного дела;
- должность лица, производящее досудебное расследование, создавшего данный раздел;
- название и электронный адрес интернет ресурса, или его части, из которого сделан цифровой снимок и копия информации населенного пункта и страны, где физически находится персональный компьютер, на котором был размещен интернет ресурс с информацией правонарушения, или с информацией, которая является цифровыми следами правонарушения.

На оснований вышеизложенного, можно сделать следующий вывод, что для реализации решения указанных проблем, по созданию программного обеспечения для функционирования автоматизированной компьютерной системы для изготовления цифрового снимка «print screen», необходимо провести соответствующие исследования, результаты которых необходимо ввести в практическую деятельность отделов по борьбе с киберпреступностью Департамента криминальной полиции МВД Республики Казахстан.