ТЕМА 5.6: ОСМОТР КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ (ПРОГРАММНО-ТЕХНИЧЕСКИЕ АСПЕКТЫ): ИНТЕРНЕТ-РЕСУРС; ЭЛЕКТРОННАЯ ПОЧТА (E-MAIL)

Нормативное закрепления порядка проведения осмотра компьютерной информации:

Статья 173. Порядок и сроки рассмотрения заявлений и сообщений о преступлении

1. Решение по заявлению или сообщению должно быть принято в срок не позднее трех суток, а при необходимости проверки достаточности наличия или отсутствия оснований к возбуждению уголовного дела – не позднее десяти суток.

2. До возбуждения уголовного дела могут быть получены объяснения, образцы для сравнительного исследования, истребованы дополнительные документы, назначена проверка финансово-хозяйственной деятельности в случаях, предусмотренных законодательными актами, произведены осмотр места происшествия, помещения или иного законного владения, не являющегося жилищем, компьютерной информации, трупа, местности, предметов, документов, освидетельствование, задержание и личный обыск при задержании, проведены экспертизы, а также может быть проведено извлечение трупа из места захоронения (эксгумация).

Статья 204. Порядок проведения осмотра

…

3[1]. При невозможности или нецелесообразности изъятия объекта, содержащего компьютерную информацию, имеющую значение для уголовного дела или материалов проверки, при осмотре может осуществляться ее копирование (фиксация) в отображаемой форме, в том числе создание образа носителя компьютерной информации. При копировании (фиксации) компьютерной информации должны обеспечиваться условия, исключающие возможность ее утраты, использоваться процедуры и методы, обеспечивающие действительность копируемой (фиксируемой) компьютерной информации. Об осуществлении копирования (фиксации) компьютерной информации в протоколе делается запись.

…

Статья 204[1]. Осмотр компьютерной информации

1. Осмотр компьютерной информации проводится на месте производства следственного действия.

2. Осмотр компьютерной информации, доступ к которой осуществляется посредством аутентификации пользователя либо которая содержит информацию

о частной жизни лица, сведения, составляющие охраняемую законом тайну, или иную информацию, распространение и (или) предоставление которой ограничено, проводится только с согласия обладателя информации и в его присутствии или по постановлению следователя, органа дознания с санкции прокурора или его заместителя, если иное не предусмотрено частью 5 настоящей статьи. В случаях, не терпящих отлагательства, осмотр компьютерной информации может быть проведен по постановлению следователя, органа дознания без санкции прокурора с последующим направлением ему в течение 24 часов сообщения о проведенном осмотре.

3. В ходе осмотра компьютерной информации следователем, органом дознания могут производиться действия, предусмотренные функционалом информационных систем, информационных ресурсов, а также использоваться научно-технические средства, оборудование, аппаратура, приборы, компьютерные программы.

4. В протоколе осмотра компьютерной информации должны быть указаны использованные научно-технические средства, оборудование, аппаратура, приборы, компьютерные программы и описаны порядок осуществления доступа к компьютерной информации, произведенные в ходе осмотра действия и полученные результаты.

5. Осмотр компьютерной информации, хранящейся в компьютерной системе, сети или на машинных носителях, изъятых при производстве процессуальных действий, санкционированных прокурором, проводится без санкции прокурора.

6. О проведении осмотра компьютерной информации составляется протокол с соблюдением требований статей 193 и 194 настоящего Кодекса.

ТИПИЧНЫЕ СЛЕДСТВЕННЫЕ СИТУАЦИИ, ВОЗНИКАЮЩИЕ ПРИ ОСЩУЕСТВЛЕНИИ ОСМОТРА ИНТЕРНЕТ-РЕСУРСОВ:

1. Интернет-ресурс на момент осмотра компьютерной информации доступен;
2. Интернет-ресурс на момент осмотра компьютерной информации не доступен.

Алгоритм действий при первой следственной ситуации:

1. Установить принадлежность интернет-ресурса (хостинг-провайдера, DNS-адрес ресурса, контактная информация о владельце ресурса) – 2ip.ru, myip.ms;
2. Сохранить рабочую копию ресурса посредством онлайн сервиса - https://archive.ph;
3. Изготовить фотоснимки экрана отображения интернет-ресурса на момент осмотра – браузерное расширение FireShot;
4. Составить процессуальный документ по итогам проведения осмотра.

Алгоритм действий при второй следственной ситуации:

1. Установить принадлежность интернет-ресурса (хостинг-провайдера, DNS-адрес ресурса, контактная информация о владельце ресурса) – 2ip.ru, myip.ms;

2. Просмотреть последнюю кэшированную поисковыми системами версию ресурса (поисковый оператор cache: название ресурса), зафиксировав полученную информацию посредством изготовления снимка(-ов) экрана;

3. Просмотреть последнюю проиндексированную версию ресурса - https://web.archive.org, зафиксировав полученную информацию посредством изготовления снимка(-ов) экрана;

4. Составить процессуальный документ по итогам проведения осмотра.

ВАЖНО: при получении информации о принадлежности интернет-ресурса, исходные файлы (скрипты, медиафайлы, информационные материалы) Вы можете получить у хостинг-провайдера, на серверах которого был размещен интернет-ресурс, посредством проведения следственных действий.

ЗАДАНИЕ ДЛЯ САМОСТОЯТЕЛЬНОГО ВЫПОЛНЕНИЯ:

В ходе выполнения задания Вам необходимо составить процессуальный документ о ходе и результатах осмотра интернет-ресурса – ***amia.by, https://www.kufar.by/item/156718845, https://raidforums.com/index.php*** *оформив в соответствии с действующим законодательством о правилах ведения делопроизводства и норм УПК РБ.*

По окончании составления осмотра ресурса(-ов) в результирующем документе ответьте на следующие вопросы:

1. Что такое DNS-адрес, доменные имена и их уровни, доменные имена, используемые странами СНГ?

2. Назовите хостинг-провайдеров, зарегистрированных в Республике Беларусь?

3. Каким образом запрашивается информация у хостинг-провайдеров?

4. Аргументировано ответьте отличается ли получение информации о содержимом ресурса до и после возбуждения уголовного дела?

5. Разновидности угроз, посредством которых может быть нарушена работа интернет-ресурса?

6. Кого рекомендуется привлекать к осмотру интернет-ресурса организации (например, в случае осуществления DDoS-атаки)? Кто может выступать в качестве специалиста в данных ситуациях?

ТИПИЧНЫЕ СЛЕДСТВЕННЫЕ СИТУАЦИИ, ВОЗНИКАЮЩИЕ ПРИ ОСУЩЕСТВЛЕНИИ ОСМОТРА ЭЛЕКТРОННЫХ ПОЧТОВЫХ АДРЕСОВ:

1. Электронный почтовый адрес (далее – e-mail) доступен и осматривается в присутствии владельца:

1.1. осматривается e-mail с предположительно фишинговым письмом;

1.2. осматривается e-mail к которому осуществлен несанкционированный доступ;

2. E-mail не доступен вследствие утраты доступа к нему, например при осуществлении несанкционированного доступа к нему.

Алгоритм действий при первой следственной ситуации:

1. Перед началом проведения осмотра необходимо получить согласие на проведение осмотра электронного почтового адреса, так как данное следственное действие ограничивает конституционное право граждан на тайну корреспонденции;

2. Владелец электронного почтового адреса самостоятельно вводит авторизационные данные, после чего начинается осмотр e-mail непосредственно сотрудником;

3. Составить процессуальный документ по итогам проведения осмотра.

При второй следственной ситуации порядок аналогичен первому, за исключением того, что первоначально необходимо воспользоваться функционалом восстановления доступа сервисов, на которых зарегистрированы e-mail.

ЗАДАНИЕ ДЛЯ САМОСТОЯТЕЛЬНОГО ВЫПОЛНЕНИЯ:

1. В директории с заданием ознакомьтесь с методическими рекомендациями по осмотру e-mail.

2. В директории с заданием расположены два файла формата PDF, с заголовком «Заголовки служебного письма», которые необходимо осмотреть.

3. Составить результирующий документ по осмотру e-mail.