МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Кафедра «Информационная безопасность систем и технологий»

Отчет о выполнении практических заданий
по дисциплине «Организационное и правовое обеспечение информационной безопасности»
на тему «Преступления в сфере компьютерной информации»

Выполнили студенты: Глебов И. Д.,
Гусев Д. А., Соколенко Н. С.
Группа: 21ПИ1
Работа принята с оценкой:
Дата сдачи:
Принял: ст. преподаватель
Щербакова А.Ю.

2024

1 Тема 1. Понятие и характеристика компьютерного преступления. Состав преступления. Психологический портрет компьютерного преступника.

1.1 Цель работы. Задание к работе.

Целью работы является закрепление основных положений и правовых норм в области компьютерных преступлений.

Задание к работе:

- Установить наличие состава преступления и квалифицировать его в соответствии с УК РФ на основе описания совершенного деяния в сфере компьютерной информации. Описать непосредственный объект, обязательные признаки объективной стороны, субъекта, последствия, санкции и т.п.

- Идентифицировать следственную ситуацию и выбрать схему расследования.

- Сформулировать возможные цели, мотивы и характеристику преступника. Разработать психологический портрет компьютерного преступника

1.2 Результаты работы

Гражданин Г. обладающий навыками пользования компьютерной техникой ДД.ММ.ГГГГ используя персональный компьютер, осуществил вход через Интернет, на сайт, с которого, незаконно скопировал на принадлежащие ему на USB- накопители <данные изъяты> вредоносные компьютерные программы <данные изъяты> предназначенную для нейтрализации средств защиты программного продукта <данные изъяты> и <данные изъяты> предназначенную для нейтрализации средств защиты программного продукта <данные изъяты>. Реализуя задуманное, Г. использовал компьютерные программы, в ходе проведения ОРМ <данные изъяты> с корыстной целью сбыл сотрудникам ОЭБ и ПК ЛО МВД России на транспорте, за денежное вознаграждение в размере <данные изъяты> рублей, путем инсталляции на жесткий диск компьютера <данные изъяты> незаконно приобретенные программные продукты: <данные изъяты> стоимостью <данные изъяты>

рублей, <данные изъяты> стоимостью <данные изъяты> рублей, <данные изъяты> стоимостью <данные изъяты> рублей и <данные изъяты> стоимостью <данные изъяты> рублей, при этом использовал вредоносные компьютерные программы <данные изъяты> и <данные изъяты> которые позволили запустить установленные им экземпляры указанного программного продукта без установленного правообладателем аппаратного ключа защиты.

Был установлен состав преступления.

Гражданин Г. осуществил незаконный доступ к защищенной информации путем копирования вредоносных программ и их использования с целью запуска программного обеспечения без ключа продукта.

Гражданин Г. установил незаконно приобретенные программные продукты на компьютеры других лиц без соответствующих прав и лицензий.

Гражданин Г. реализовал сбыт незаконно приобретенных программных продуктов сотрудникам за денежное вознаграждение.

1.2.1 С учётом вышеперечисленных действий, Гражданин Г. может быть квалифицирован по следующим статьям УК РФ:

- Статья 272. Незаконный доступ к компьютерной информации. Наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

Объектом преступления является программное обеспечение, которое гражданин Г. незаконно скопировал и запустил, а также права правообладателей на это программное обеспечение.

Объективная сторона состоит в незаконном использовании и модификации программного обеспечения без согласия законного обладателя, а так же хранение, использование и сбыт незаконно приобретенных программных

продуктов, инсталляция незаконно приобретенных программ на жесткий диск компьютера.

Субъектом преступления является гражданин Г., обладающий навыками пользования компьютерной техникой, совершивший преступление.

Субъективная сторона преступления выражается в прямом умысле совершения запрещенных действий, то есть осознании и желании лица модифицировать и использовать программное обеспечение незаконно с целью сбыта и получения прибыли.

- Статья 273. Создание, использование и распространение вредоносных компьютерных программ. Наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

Объектом преступления является незаконно скопированное на USB-накопитель вредоносное программное обеспечение.

Объективная сторона состоит в копирование и получении вредоносных программ для нейтрализации средств защиты программного продукта.

Субъектом преступления является Гражданин Г., обладающий навыками пользования компьютерной техникой, совершивший преступление.

Субъективная сторона включает прямой умысел гражданина Г. на совершение незаконных действий, а именно использование вредоносных программ, осознание беззаконности своих действий и наличие корыстных целей при совершении преступления.

Место преступления — организация ОЭБ и ПК ЛО МВД, где злоумышленник установил программный продукт.

Способом реализации преступления является использование компьютера и интернета для доступа к информации и передачи данных.

Орудиями совершения преступления являются: компьютер, USB-накопители, вредоносные программы, незаконно приобретенные программные продукты.

Мотив Г. связан с корыстной целью - заработком денег за счет незаконной деятельности с компьютерными данными и программным обеспечением.

Целью Г. было преднамеренное использование украденного программного обеспечения и вредоносных программ для личной выгоды.

1.2.2 Схема расследования

Пострадавшая сторона ОЭБ и ПК ЛО МВД обратилась в правоохранительные органы, так как приобретенное программное обеспечение перестало запускаться.

Для выявления преступника провести анализа улик, осуществить поиск и фиксацию цифровых следов, связанных с деятельностью Г., включая использованные IP-адреса, файлы, программы и т. д, изъять видеоматериалы с камер видеонаблюдения пострадавшей организации.

Провести допросов потерпевших, свидетелей и возможных соучастников для получения дополнительной информации о совершенном преступлении.

Подать запрос провайдеру на получение информации о действиях с подозрительных IP-адресов, которые могли быть использованы в процессе совершения преступления.

Произвести осмотр места происшествия, выявить подозреваемого, провести обыск, произвести выемку компьютерной техники и документации, назначить экспертизу.

1.2.3 Психологический портрет.

С учетом обнаруженной информации о субъекте преступления, психологический портрет компьютерного преступника содержит следующие:

Мужчина 20 — 40 лет, стремится к легкому заработку, возможно, безразличен к закону. Обладает профессиональной квалификацией в области информационных технологий. Имеет опыт работы или обучения в сфере IT.

Обладает навыками социальной инженерии. Психически здоров, демонстрирует рациональное поведение и четкую логику в действиях.

1.3 Вывод

Таким образом, закрепили основные положения и правовых норм в области компьютерных преступлений.

2 Тема 2. Тактика обнаружения, изъятия и фиксации компьютерной информации при производстве следственных действий. Осмотр места происшествия. Обыск

2.1 Цель работы. Задание к работе.

Целью работы является закрепление тактики обнаружения, изъятия и фиксации компьютерной информации при производстве следственных действий.

Задание к работе:

- Составить отчет об осмотре заданного гипотетического места преступления.
- Составить отчет об обыске заданного гипотетического места преступления.

2.2 Результаты работы

2.2.1 Был проведен осмотр места преступления. Был выявлен подозреваемый, протокол осмотра приведен в приложении А.

2.2.2 Был проведен обыск, протокол обыска приведен в приложении Б.

2.3 Вывод.

Таким образом, были закреплены тактики обнаружения, изъятия и фиксации компьютерной информации при производстве следственных действий.

3 Тема 3. Тактика обнаружения, изъятия и фиксации компьютерной информации при производстве следственных действий. Следственные версии. Последующие этапы расследования компьютерных преступлений

3.1 Цель работы. Задание к работе

Целью работы является изучение тактики обнаружения, изъятия и фиксации компьютерной информации при производстве следственных действий.

- Составить отчет о выдвинутых следственных версиях заданного гипотетического преступления.

- Составить отчет о проведении следственного эксперимента при расследовании заданного гипотетического преступления.

3.2 Были составлены 4 следственные версии, проведен допрос, а также был составлен протокол следственного эксперемента.

3.2.1 Версия 1: Гражданин Г. действовал в одиночку. Он использовал свои навыки и знания в области компьютерной техники для незаконного доступа к сайту и копирования вредоносных программ. Затем он использовал эти программы для запуска другого программного обеспечения без ключа продукта с целью получения прибыли.

3.2.2 Версия 2: Гражданин Г. был частью организованной группы. Он был ответственен за техническую сторону операции, включая незаконное копирование и использование вредоносных программ, а другие члены группы занимались сбытом незаконно приобретенного программного обеспечения (созданием объявлений, поиском клиентов).

3.2.3 Версия 3: Гражданин Г. был использован третьей стороной или сторонами. Он мог не осознавать полную картину своих действий или последствий, возможно, ему было предложено выполнить эти действия в обмен на денежное вознаграждение.

3.2.4 Версия 4: Гражданин Г. действовал под принуждением или угрозой. В этом случае он мог быть вынужден совершить эти действия под давлением или угрозами со стороны других лиц.

3.2.5 Был составлен протокол следственного эксперимента. Протокол приведен в приложении В. Допросы и опросы представленны в приложении Г, а также в приложении Д.

3.3 Вывод.

Таким образом, была изучена тактика обнаружения, изъятия и фиксации компьютерной информации при производстве следственных действий.

4 Тема 5. Экспертиза преступлений в области компьютерной информации. Аппаратно-компьютерная экспертиза.

4.1 Цель работы. Задание к работе

Целью работы является изучение экспертиз преступлений в области компьютерной информации. Изучение объектов компьютерно-технической экспертизы и аспекты исследования машинных носителей информации.

- Составить отчет о аппаратно-компьютерной экспертизе гипотетического компьютерного преступления.

4.2 Было составлено постановление апаратно-компьютерной экспертизы. Постановление находится в приложении Е.

4.3 Было составлено заключение эксперта. Заключение находится в приложении З.

5 Тема 6. Экспертиза преступлений в области компьютерной информации. Программно-компьютерная экспертиза.

5.1 Цель работы. Задание к работе

Целью работы является получение знаний о судебной программно-компьютерной экспертизе преступлений в области компьютерной информации. Изучить аспекты исследования программного обеспечения.

5.2 Было составлено постановление программно-компьютерной экспертизы. Постановление находится в приложении И.

5.3 Было составлено заключение эксперта. Заключение находится в приложении К.

Приложение А

Протокол осмотра

г. Санкт-Петербург « 3 » декабря 2023 г.

(место составления)

Осмотр начат в 10 ч 00 мин

Осмотр окончен в 15 ч 25 мин

старший следователь СО по Центральному р-н СУСК при пр-ре РФ по Сб юрист 2 класса

(должность следователя (дознавателя),

Калганов Н. С. ,

классный чин или звание, фамилия, инициалы)

получив сообщение от Строкова Вадима Игоревича о мошеннических действиях со стороны

(от кого, о чем)

лица, осуществляющего установку программного обеспечения ,

прибыл В организацию ОЭБ и ПК ЛО МВД по адресу г Петербургул. Рубинштейна, д.23, пом.

(куда)

103

и в присутствии понятых:

1. Симонов Виктор Петрович

(фамилия, имя, отчество

г. Пенза, ул Лермонтова 28/4 кв., тел. 76-34-72

и место жительства понятого)

2. Сковпень Роман Семенович

(фамилия, имя, отчество

Пенза, ул. Красная 9/2 кв., моб. 8-913-567-23-98

и место жительства понятого)

с участием потерпевшего Строкова Вадима Игоревича, работающего ОЭБ и ПК ЛО МВД

(процессуальное положение, фамилия, имя, отчество каждого лица,

начальником управления, а также эксперта в области договоров возмездного оказания услуг

участвовавшего в следственном действии, а в необходимых случаях

Глазырин С. П.

его адрес и другие данные о его личности)

в соответствии со ст. 164, 176 и частями первой-четвертой и шестой ст. 177 УПК РФ

произвел осмотр Офисных помещений ОЭБ и ПК ЛО МВД по адресу г Петербург ул.

(чего)

Рубинштейна, д.23

Перед началом осмотра участвующим лицам разъяснены их права, ответственность, а также порядок производства осмотра места происшествия.

Понятым, кроме того, до начала осмотра разъяснены их права, обязанности и ответственность, предусмотренные ст. 60 УПК РФ.

(подпись понятого)

(подпись понятого)

Специалисту (эксперту) Глазырину Сергею Павловичу

(фамилия, имя, отчество)

разъяснены его права и обязанности, предусмотренные ст. 58 (57) УПК РФ.

(подпись специалиста

(эксперта)

Лица, участвующие в следственном действии, были заранее предупреждены

о применении при производстве следственного действия технических средств

фотоаппарат «Canon »

Осмотр производился в условиях солнечной погоды, при температуре +2 С при

(погода, освещенность)

естественном освещении на прилегающей территории и искусственном освещении внутри помещения организации

Осмотром установлено: Офисное помещение представляет собой коридор с несколькими

помещениями. Было осмотрено рабочее помещение, дверь в которое находится во второй двери справа от входа. Помещение представляет совой квадратное помещение с десятью рабочими местами, представляющими собой столы с персональными компьютерами. Компьютеры были Во включенном состоянии, их экраны были сняты на фотоаппарат. Далее было осмотрено Помещение слева от входа, являющееся рабочим кабинетом Строкова Вадима Игоревича, Которое представляет собой рабочее место с персональным компьютером и шкаф с рабочими Документами. По просьбе Строкова Вадима Игоревича был осмотрен документ, который, со слов потерпевшего, был заключён с Георгиевым Владимиром Игоревичем, оказывавшем Услуги по установке ПО на персональные компьютеры. Страницы документа были сняты на Фотоаппарат. Были осмотрено серверное помещение, находящееся в подвальном помещении Офиса. В помещении присутствует системный блок чёрного цвета, выполняющий, со слов Строкова Вадима Игоревич функции сервера организации. Помещение было детально Сфотографировано.

В ходе осмотра проводилась Фотосъемка
(фотосъемка, видео-, аудиозапись и т.п.)
фотоаппаратом «Canon »

Приложение Б

Протокол Обыска

Санкт-Петербург « 04 » Декабря 2023 г.

(место составлени)

Обыск (выемка) начат в 12 ч 21 мин

Обыск (выемка) окончен в 17 ч 20 мин

Я старший следователь СО по Центральному р-н СУСК при пр-ре РФ по Сб юрист

(должность следователя (дознавателя),

2 класса Калганов Н. С.

классный чин или звание, фамилия, инициалы)

в присутствии понятых:

1. Туманов Ренат Исхакович, Сб, ул. О.Дундича, д.36, корп. 1, кв. 428

(фамилия, имя, отчество и место жительства понятого)

2. Глебов Алексей Петрович, г. Астрахань, ул. Крупской, д.22

(фамилия, имя, отчество и место жительства понятого)

с участием[1] С участием владельца квартиры Георгиева Владимира Игоревича, опера

(процессуальное положение, фамилия, имя, отчество каждого лица,

Уполномоченного Осипова Арсена Даниловича.

участвовавшего в следственном действии, а в необходимых случаях его адрес и другие данные о его личности)

на основании постановления от 03 декабря 2023 г. и в соответствии с частями четвертой-шестнадцатой ст. 182 (частями второй, третьей и пятой ст. 183) УПК РФ произвел обыск (выемку) г. Санкт-Петербург ул. Романа Абрамова д.10 кв. 65

(где именно)

в целях отыскания и изъятия ЭВМ и носителей информации имеющих отношение у делу о

(каких именно предметов, документов,

распространении вредоносного ПО

ценностей, имеющих значение для уголовного дела)

Перед началом обыска (выемки) участвующим лицам разъяснены их права, ответственность, а также порядок производства обыска (выемки).

Участвующие лица: Калганов Н. С.

(подпись)

1

Туманов Р. И.

(подпись)

Глебов А. П.

(подпись)

Георгиев В. И.

(подпись)

Осипов А. Д.

(подпись)

Понятым, кроме того, до начала обыска (выемки) разъяснены их права, обязанности и ответственность, предусмотренные ст. 60 УПК РФ.

(подпись понятого)

(подпись понятого)

Лица, участвующие в следственном действии, были заранее предупреждены о применении при производстве следственного действия технических средств ф/а – цифровой «Panasonic» DMC-F220, применяемый Осиповым А. Д.

(каких именно и кем именно)

Перед началом обыска (выемки) следователем (дознавателем) было предъявлено постановление о производстве обыска (выемки) от « 03 » декабря 2023 г., после чего Георгиеву В. И.

(кому именно)

было предложено выдать ЭВМ, на которых установлено вредоносное ПО.

Указанные предметы, документы и ценности были выданы добровольно.

В ходе обыска (выемки) изъято: Квартира расположена на 10 этаже многоквартирного

(излагаются обстоятельства производства обыска

Дома. В подъезде данная квартира расположена справа от входа.

(выемки), предусмотренные частями десятой,

Вход в квартиру осуществляется через дверной проем.

тринадцатой и четырнадцатой ст. 182 УПК РФ,

Дверной проем оборудован металлической дверью темно-коричневого цвета, имеющей

перечень и индивидуальные признаки

запорное устройство в виде интегрированного в тело двери замка. Сотрудниками был

изъятых предметов, их упаковка)

осуществлён звонок в дверь, после чего был предъявлен ордер на обыск, после чего подозреваемый сам открыл дверь и впустил сотрудников и понятых в квартиру, представляющую собой одно жилое помещение, кухню и санитарный узел. В жилом помещении был обнаружен персональный компьютер и ноутбук, которые были изъяты и помещены в ударопрочные кейсы. По требованию сотрудников Георгиевым Владимиром Игоревичем были выданы имеющиеся у него жёсткие диски и флеш-накопители, которые были изъяты и помещены в полиэтиленовые пакеты с красной маркировкой. Также были изъяты мобильный телефон и договор с ОЭБ и ПК ЛО МВД по адресу г Петербург ул. Рубинштейна, д.23, обнаруженные в ящике шкафа в жилом помещении. Остальные помещения были обысканы, но материалов для следствия обнаружено не было.

Приложение В

Протокол эксперимента

ул. Ломоносова д. 25, Санкт-Петербург « 16 » марта 2023 г.

(место составления)

Следственный эксперимент начат в 12 ч 20 мин

Следственный эксперимент окончен в 16 ч 35 мин

старший следователь СО по Центральному р-н СУСК при пр-ре РФ по Сб юрист 2 класса

Калганов

в присутствии понятых:

1. Смирнова Мария Петровна, ул. Приморская д. 12, Санкт-Петербург
2. Иванов Павел Сергеевич, пр. Невский д. 35, Санкт-Петербург

с участием эксперта в сфере информационной безопасности и вредоносного ПО Смирнова

А. И. Проживающего по адресу Ленина, 58, а также работника офиса Соколова Н. А

в соответствии со ст. 181 УПК РФ произвел следственный эксперимент по уголовному делу

№ 2938 с целью воссоздания хронологии событий, получения новых улик

и доказательств, проверки возможно ли установить на компьютеры, находящиеся в офисе организации, нелицензионное ПО с использованием вредоносного ПО

Перед началом следственного эксперимента участвующим лицам разъяснены их права, ответственность, а также порядок производства следственного эксперимента.

Понятым, кроме того, до начала осмотра разъяснены их права, обязанности и ответственность, предусмотренные ст. 60 УПК РФ.

Смирнова М. П.

(подпись понятого)

Иванов П. С.

(подпись понятого)

Специалисту (эксперту) Смирнову А. И.

(фамилия, имя, отчество)

разъяснены его права и обязанности, предусмотренные ст. 58 (57) УПК РФ.

(подпись специалиста
(эксперта)

(подпись понятого)

(подпись понятого)

Лица, участвующие в следственном эксперименте, были заранее предупреждены о применении при производстве следственного действия технических средств ноутбука с виртуальной машиной с операционной системой Windows 10

Следственный эксперимент производился в условиях В офисе с использованием искуственного освещения, а также естественного освещения из окон при ясной погоде.

Следственным экспериментом установлено: Смирнов А. И. и Следователь Калганов Прибыли в офис компании в 9:30. Смирновым А. И. Была настроена операционная система На виртуальной машине ноутбука, аналогичная операционной системе, находящийся На компьютерах организации. Смирнов А. И. Использовал тестовое ПО, аналогичное большинству активаторов по способу реализации и внедрения.

Встроенное антивирусное ПО не смогло обнаружить использование вредоносного ПО.

Смирнов А. И. Заключил, что на компьютерах организации используется устаревшая защита,

Имеющая уязвимости, вследствие чего, злоумышленник на самом деле мог установить

Нелицензионное ПО на компьютеры в офисе

В ходе следственного эксперимента проводилась Видео-аудео съемка на камеры,

установелнные в офисе

К протоколу прилагаются видеозаписи на флеш накопителе

Протокол предъявлен для ознакомления всем лицам, участвовавшим в следственном действии. При этом указанным лицам разъяснено их право делать подлежащие внесению в протокол оговоренные и удостоверенные подписями этих лиц замечания о его дополнении и уточнении. Ознакомившись с протоколом путем

(личного прочтения или оглашения протокола следователем (дознавателем)

участники следственного действия сделали следующие замечания о его дополнении и уточнении

(указываются процессуальное положение, фамилия и инициалы участника следственного действия и сделанные им дополнения и уточнения к содержанию протокола)

Приложение Г

ПРОТОКОЛ
допроса подозреваемого

_____ «___» _____ 20___ г.
(место составления)

Допрос начат в _____ ч ____ мин
Допрос окончен в _____ ч ____ мин

_____
(должность следователя (дознавателя),
_____ ,
классный чин или звание, фамилия, инициалы)
в помещении _____
(каком именно)
в соответствии с частью второй ст. 46, ст. 189, 190 (частью первой ст. 223[1]) УПК РФ допросил
по уголовному делу № _____ в качестве подозреваемого:

1. Фамилия, имя, отчество _____
2. Дата рождения _____
3. Место рождения _____
4. Место жительства и (или) регистрации _____
_____
телефон _____
5. Гражданство _____
6. Образование _____
7. Семейное положение, состав семьи _____
_____
8. Место работы или учебы _____
_____
телефон _____
9. Отношение к воинской обязанности _____
(где состоит на
_____
воинском учете)
10. Наличие судимости _____
(когда и каким судом был осужден,
_____
по какой статье УК РФ, вид и размер
_____
наказания, когда освободился)
_____

11. Паспорт или иной документ, удостоверяющий личность подозреваем__ _____

_____

12. Иные данные о личности подозреваемого _____

Подозреваемый _____
(подпись)

с участием _____
(процессуальное положение, фамилия, имя, отчество каждого лица, участвовавшего в следственном

_____
действии, а в необходимых случаях его адрес и другие данные о его личности)

_____

Участвующим лицам объявлено о применении технических средств _____

_____
(каких именно, кем именно)

_____

Мне разъяснено, что в соответствии с частью четвертой ст. 46 УПК РФ я вправе:

1) знать, в чем я подозреваюсь, и получить копию постановления о возбуждении против меня уголовного дела, либо копию протокола задержания, либо копию постановления о применении ко мне меры пресечения;

2) давать объяснения и показания по поводу имеющегося в отношении меня подозрения либо отказаться от дачи объяснений и показаний. Я предупрежден о том, что при моем согласии дать показания мои показания могут быть использованы в качестве доказательств по уголовному делу, в том числе и при моем последующем отказе от этих показаний, за исключением случая, предусмотренного п. 1 части второй ст. 75 УПК РФ;

3) пользоваться помощью защитника с момента, предусмотренного пунктами 2 – 3^1 части третьей статьи 49 УПК РФ, и иметь свидание с ним наедине и конфиденциально до моего первого допроса;

4) представлять доказательства;

5) заявлять ходатайства и отводы;

6) давать показания и объяснения на родном языке или языке, которым я владею;

7) пользоваться помощью переводчика бесплатно;

8) знакомиться с протоколами следственных действий, произведенных с моим участием, и подавать на них замечания;

9) участвовать с разрешения следователя или дознавателя в следственных действиях, производимых по моему ходатайству, ходатайству моего защитника либо законного представителя;

10) приносить жалобы на действия (бездействие) и решения суда, прокурора, руководителя следственного органа, следователя, органа дознания и дознавателя в порядке, предусмотренном главой 16 УПК РФ;

11) защищаться иными средствами и способами, не запрещенными УПК РФ.

Мне разъяснено также, что в соответствии со ст. 51 Конституции Российской Федерации я не обязан свидетельствовать против самого себя, своего супруга (своей супруги) и других близких родственников, круг которых определен п. 4 ст. 5 УПК РФ.

Подозреваемый___ _____
(подпись)

Подозреваемому _____ объявлено, что он
(фамилия, инициалы)

подозревается в совершении _____
(излагаются обстоятельства преступления,

_____
в совершении которого данное лицо подозревается)

_____,

то есть в совершении преступления, предусмотренного _____

_____ УК РФ.

Подозреваемый _____
(подпись)

По существу подозрения могу показать следующее: _____
(показания подозреваемого

_____
излагаются от первого лица, по возможности дословно,

Подозреваемый _____
(подпись)

_____
а также записываются поставленные ему вопросы и ответы на них в той последовательности,

_____
которая имела место в ходе допроса, отражаются все вопросы, в том числе те, которые были отведены следователем,

_____
или на которые отказалось отвечать допрашиваемое лицо, с указанием мотивов отвода или отказа)

Дата и время: 15 апреля 2024 года, 10:00 утра.

Место: Отделение полиции №15, Питербург.

Следователь: Калганов Н.С.

Подозреваемый: Георгиев В.И.

Процесс допроса:

Следователь Калганов начал допрос, представившись и объяснив Георгиеву его права и обязанности. Затем он предъявил обвинение в незаконном доступе к защищенной информации и сбыте незаконно приобретенных программных продуктов.

Следователь Калганов спросил Георгиева о его навыках в области компьютерной техники. Георгиев подтвердил, что обладает достаточными навыками и знаниями, включая знание языков программирования и опыт работы с различными операционными системами.

Затем следователь задал вопросы о действиях Георгиева в указанный день. Георгиев признал, что использовал свой персональный компьютер для доступа к определенным сайтам, но отрицал любые незаконные действия. Он утверждал, что просто искал информацию для личного обучения и развития.

Когда следователь спросил о вредоносных программах, Георгиев заявил, что не знает, как они попали на его USB-накопитель. Он утверждал, что никогда не использовал такие программы и не знает, как они работают.

Наконец, когда следователь спросил о сбыте программ, Георгиев заявил, что никогда не продавал программное обеспечение и что все его действия были направлены на улучшение его навыков в области информационных технологий.

На основе ответов Георгиева и других доказательств следователь Калганов пришел к выводу, что есть основания полагать, что Георгиев действовал в одиночку, использовал свои навыки и знания в области компьютерной техники для незаконного доступа к сайту и копирования вредоносных программ. Это соответствует первой следственной версии. Однако следователь Калганов решил продолжить расследование, чтобы подтвердить эту версию и исключить возможность других версий.

Приложение Д

ПРОТОКОЛ
допроса свидетеля

_____ «___» _____ 20___ г.
(место составления)

Допрос начат в _____ ч _____ мин
Допрос окончен в _____ ч _____ мин

_____
(должность следователя (дознавателя),
_____
классный чин или звание, фамилия, инициалы)
в помещении _____
(каком именно)
в соответствии со ст. 189 и 190 (191) УПК РФ допросил по уголовному делу № _____
в качестве свидетеля:

1. Фамилия, имя, отчество _____
2. Дата рождения _____
3. Место рождения _____
4. Место жительства и (или) регистрации _____
_____
телефон _____
5. Гражданство _____
6. Образование _____
7. Семейное положение, состав семьи _____
_____
8. Место работы или учебы _____
_____
телефон _____
9. Отношение к воинской обязанности _____
(где состоит на
_____
воинском учете)
10. Наличие судимости _____
(когда и каким судом был осужден,
_____
по какой статье УК РФ, вид и размер
_____
наказания, когда освободился)
_____

Свидетель _____
(подпись)

11. Паспорт или иной документ, удостоверяющий личность свидетеля _____

12. Иные данные о личности свидетеля _____

с участием _____
(процессуальное положение, фамилия, имя, отчество каждого лица,
участвовавшего в следственном действии, а в необходимых случаях его адрес и другие данные о его личности)

Лица, участвующие в следственном действии, были заранее предупреждены о применении при производстве следственного действия технических средств _____
(каких именно)

Перед началом допроса мне разъяснены права и обязанности свидетеля, предусмотренные частью четвертой ст. 56 УПК РФ:

1) отказаться свидетельствовать против самого себя, своего супруга (своей супруги) и других близких родственников, круг которых определен п. 4 ст. 5 УПК РФ. При согласии дать показания я предупрежден о том, что мои показания могут быть использованы в качестве доказательств по уголовному делу, в том числе и в случае моего последующего отказа от этих показаний;

2) давать показания на родном языке или языке, которым я владею;

3) пользоваться помощью переводчика бесплатно;

4) заявлять отвод переводчику, участвующему в допросе;

5) заявлять ходатайства и приносить жалобы на действия (бездействие) и решения дознавателя, следователя, прокурора и суда;

6) являться на допрос с адвокатом в соответствии с частью пятой ст. 189 УПК РФ;

7) ходатайствовать о применении мер безопасности, предусмотренных частью третьей ст. 11 УПК РФ.

Об уголовной ответственности за отказ от дачи показаний по ст. 308 УК РФ и за дачу заведомо ложных показаний по ст. 307 УК РФ предупрежден

Свидетель _____
(подпись)

По существу уголовного дела могу показать следующее: _____
(излагаются показания свидетеля,

а также поставленные перед ним вопросы и ответы на них)

Свидетель _____
(подпись)

Дата и время: 16 апреля 2024 года, 14:00.
Место: Отделение полиции №15, Питербург
Следователь: Калганов Н.С.
Свидетель: Симонов Виктор Петрович.
Процесс опроса:

Следователь Калганов начал опрос, представившись и объяснив Симонову его права и обязанности как свидетелю. Затем он попросил Симонова рассказать о своем опыте покупки программного обеспечения.

Симонов рассказал, что он хотел купить программное обеспечение для нескольких рабочих ПК в офисе. Он нашел объявление о продаже программного обеспечения в Интернете и связался с продавцом, который оказался Георгиевым.

Симонов рассказал, что Георгиев пришел в офис и установил программное обеспечение на рабочие ПК. Симонов заметил, что Георгиев использовал USB-накопитель и что процесс установки был быстрее, чем обычно. Симонов заплатил Георгиеву согласованную сумму.

Однако через несколько дней после использования, программное обеспечение перестало работать. Это вызвало подозрения у Симонова, и он решил обратиться в полицию.

Дата и время: 16 апреля 2024 года, 15:30.

Место: Отделение полиции №15, Питербург, улица Рубенштейна, 23.

Следователь: Калганов Н.С.

Свидетель: Иванов Алексей Сергеевич, сотрудник офиса, где работает Симонов.

Процесс опроса:

Следователь Калганов начал опрос, представившись и объяснив Иванову его права и обязанности как свидетелю. Затем он попросил Иванова рассказать о своих наблюдениях в день, когда Георгиев пришел в офис.

Иванов подтвердил, что видел Георгиева в офисе в указанный день. Он заметил, что Георгиев провел некоторое время за рабочим местом Симонова и использовал USB-накопитель.

Когда следователь спросил о работе программного обеспечения, Иванов подтвердил, что через несколько дней после визита Георгиева, программное обеспечение на нескольких ПК в офисе перестало работать.

Приложение Е

Постановление аппаратно-компьютерной экспертизы.

ПОСТАНОВЛЕНИЕ

о назначении аппаратно-компьютерной **судебной экспертизы**
(какой именно)

Санкт-Петербург « 15 » Декабря 2023 г.
(место составления)

старший следователь СО по Центральному р-н СУСК при пр-ре РФ по Сб юрист 2 класса
(должность следователя (дознавателя),
Калганов Н. С. ,
классный чин или звание, фамилия, инициалы)
рассмотрев материалы уголовного дела № _____ ,

У С Т А Н О В И Л :

4 декабря 2023 был совершён обыск в квартире подозреваемого Георгиева Владимира
(излагаются основания назначения
Игоревича. В ходе обыска были изъяты системный блок и электронные носители. На изъятых
судебной экспертизы)
электронных носителях предположительно находится вредоносное ПО при помощи которого
подозреваемый осуществил преступные действия.

На основании изложенного и руководствуясь ст. 195 (196) и 199 УПК РФ,

П О С Т А Н О В И Л :

1. Назначить аппаратно-компьютерную
(какую именно)
судебную экспертизу, производство которой поручить Левину Алексею Егоровичу

(фамилия, имя, отчество эксперта либо

наименование экспертного учреждения)

2. Поставить перед экспертом вопросы:

Системный блок и жесткий диск какой модели представлены на исследование? Каковы технические характеристики системных блоков и жесткого диска?
(формулировка каждого вопроса)

Исправны ли системные блоки и жесткий диск, представленные на исследование?

Содержат ли информацию предъявленные на экспертизу системные блоки и жесткий диск, возможно ли ее использовать?

Имеется ли удаленная информация на представленных системных блоках и жестком диске? Возможно ли ее восстановление?

Возможно ли восстановление дефектных магнитных носителей информации?

3. Предоставить в распоряжение эксперта материалы: Системный блок персонального компьютера, жёсткие диск

(какие именно)

4. Поручить: Осипову А. Д.

(кому именно)

разъяснить эксперту права и обязанности, предусмотренные ст. 57 УПК РФ, и предупредить его об уголовной ответственности в соответствии со ст. 307 УК РФ за дачу заведомо ложного заключения[1].

Следователь (дознаватель) _____

(подпись)

Права и обязанности, предусмотренные ст. 57 УПК РФ, мне разъяснены «____» _____ 20___ г.

Одновременно я предупрежден об уголовной ответственности в соответствии со ст. 307 УК РФ за дачу заведомо ложного заключения.

Эксперт _____

(подпись)

1 Данная графа заполняется в случаях, предусмотренных частью второй ст. 199 УПК РФ.

Приложение 3

Заключение эксперта об аппаратно-компьютерной экспертизе

Подписка

Мне, сотруднику , в соответствии с ч.2 ст.199 УПК России разъяснены права и ответственность эксперта, предусмотренные ст.57 УПК России.

Об ответственности за дачу заведомо ложного заключения по ст.307 УК России и за разглашение данных предварительного расследования предупрежден.

З А К Л Ю Ч Е Н И Е Э К С П Е Р Т А

№ от 2023 г.

Эксперт произвел компьютерно-техническую судебную экспертизу. на судебную экспертизу поступили:

1. Системный блок.

2. Ноутбук

3. Накопитель на жестком магнитном диске (НЖМД).

4. Флеш-накопитель

5. Постановление о назначении экспертизы.

Перед экспертом поставлены вопросы:

1) Системные блоки и жесткий диск какой модели представлены на исследование? Каковы технические характеристики системных блоков и жесткого диска?

2) Исправны ли системные блоки и жесткий диск, представленные на исследование?

3) Содержат ли информацию предъявленные на экспертизу системные блоки и жесткий диск, возможно ли ее использовать?

5) Имеется ли удаленная информация на представленных системных блоках и жестком диске? Возможно ли ее восстановление?

6) Возможно ли восстановление дефектных магнитных носителей информации?

Внешний осмотр поступившей на экспертизу компьютерной техники

-Системный блок (эксперт вводит обозначение - системный блок №1) в корпусе серого цвета типоразмера «MiddleTower» максимальными размерами 44,5Х19,5Х46,0 см (высота Х ширина Х длина). Лицевая сторона системного блока и часть верхней крышки системного блока заклеены фрагментом бумаги белого цвета на поверхности которого находятся оттиски мастичной круглой печати и две подписи. Задняя сторона системного блока и части боковых крышек системного блока заклеены фрагментом бумаги белого цвета на поверхности которого находятся оттиски мастичной круглой печати и пояснительный рукописный текст: «Понятые: (подпись) (подпись) Следователь (подпись)». Описанные фрагменты бумаги не повреждены. Левая боковая сторона системного блока имеет прозрачную вставку.

-Прозрачный бесцветный полимерный пакет горловина которого перевязана шпагатом белого цвета. Концы шпагата заклеены листом бумаги на поверхности которого имеется рукописный текст « Понятые: (подпись) (подпись) Следователь: (подпись)». Целостность упаковки видимых повреждений не имеет. При вскрытии упаковки извлечен накопитель на жестких магнитных дисках (эксперт вводит обозначение – НЖМД №4) фирмы Seagate марки U Series 5 модель ST320413A серийный номер 5ED3GC22.

ИССЛЕДОВАНИЕ

1. План исследования Исследование компьютерной техники, поступившей на экспертизу, проводилось в следующей последовательности:

1.Исследование состояния системного блока и определения его технических характеристик.

2.Исследование состояния накопителя (НЖМД) и определение его технических характеристик.

3. Исследование загрузочных разделов и разделов для хранения информации.

4. Исследование разделов носителей на наличие удаленной информации.

2. Методика исследования системных блоков.

2.1. Исследование состояния каждого системного блока проводилось по следующей методике:

- производилось вскрытие корпуса системного блока;

- визуальным осмотром устанавливался состав внутренних аппаратных компонентов (комплектующих устройств) представленного на исследование системного
блока;

- из системного блока извлекался НЖМД; процедура изъятия носителя данных обусловлена требованием полной сохранности исследуемой информации путем обеспечения условий, исключающих какую-либо запись на них новых данных;

- к системному блоку в соответствии с эксплуатационными правилами подключалось электропитание, монитор и клавиатура;

- системный блок включался, производилась загрузка операционной системы с
системной дискеты эксперта, определение установленной системной даты и времени,

диагностирование входящих в системный блок устройств.

2.2. Исследование состояния носителей данных .

2.2.1. Исследование состояния НЖМД проводилось последовательно по следующей методике:

- визуальным осмотром устанавливался интерфейс, состояние перемычек и переключателей НЖМД;

- исследуемый НЖМД помещался во внешний корпус для быстрой смены НЖМД, подключался к лабораторному компьютеру по USB-порту (сохранность данных на исследуемых НЖМД обеспечивалось программой NCSF Software Write-block XP организации National Center For Forensic Science);

- производилась загрузка операционной системы с системной дискеты эксперта и определялись технические параметры НЖМД (количество цилиндров, сторон (головок), секторов на треке, количество секторов, размеров секторов и емкости);

- выявлялись таблицы разделов НЖМД с определением их основных параметров (начало и конец раздела, тип файловой системы, идентификаторы и метки разделов, размер и количество кластеров);

- определялась логическая адресация системных областей разделов НЖМД;

- производился поиск признаков повреждения целостности структуры данных
(несоответствие заявленных параметров раздела фактическим, наличие сбойных, потерянных кластеров) и устанавливалась возможность доступа к данным на исследуемых НЖМД;

- производилось создание файлов-образов, содержащих точные копии исследуемых НЖМД на вспомогательном НЖМД лабораторного компьютера путем посекторного копирования с фиксацией технических параметров форматов носителей с использованием специального программного обеспечения для экспертного исследования компьютерных

носителей информации;

- осуществлялся вывод в файл на НЖМД лабораторного компьютера списка всех папок (каталогов) и файлов логических дисков исследуемых НЖМД.

3. Экспертное оборудование и методическая литература, использованные при проведении исследования

3.1. Аппаратно-программный комплекс для экспертного исследования компьютерных носителей информации в составе: - персональная ЭВМ на базе процессора Intel Celeron 2,4 ГГц; - лазерный принтер «HP LaserJet 1200» производства «Hewlett Packard» (США). -программное обеспечение для экспертного исследования компьютерных носителей информации «EnCase Forensic Edition v.4.20» производства «Guidance Software Inc.» ; -операционная система «Microsoft Windows XP Professional» производства «Microsoft» ; - прикладное программное обеспечение «Microsoft Office XP Professional» производства «Microsoft» (США); -сервисное программное обеспечение PowerQuest Partition Magic 8.0; -сервисное программное обеспечение NTFS Software Write-block XP (блокиратор записи разработанного National Center For Forensic Science); -сервисное программное обеспечение WinRAR 3.0.

4. Результаты исследования

4.1. Исследование состояния системного блока №1 Визуальным осмотром выявлено, что корпус внешних повреждений не имеет. Представленный системный блок состоит из следующих комплектующих:

Таблица №1.

Комплектующие	Фирма изготовитель, Марка	Модель	Серийный номер	Примечание
Материнская плата	LanParty	LP NFII Ultra B	P35-1K1-1FD9	P/N: NF2001-5 Другие маркировочные обозначения:

				000129F06356 и 000129F0633F
Процессор	AMD, Athlon		TO89236I41313	Другие маркировочные обозначения: AXDA2600DKV4D И UQYHA0437EPMW
Модуль памяти	nynix	PC3200U30330 512MB DDR 400MHZ	HYMD26464B8R-D43	
Дисковод (НГМД)	ALPS ELECTRIC CO., LTD	DF354H168F	8A177204	
НЖМД	Seagate, Barracuda 7200.7	ST3120026A	3JT1AP04	Эксперт вводит обозначение - НЖМД №1
Видео-карта	ATI, ATI 9600 TV/DVI 128D	VD0092 0442010305	0442010305	
Модем	ACORP	Sprinter 56k Soft PCI	HH0204938790	

Для последующего исследования на стендовом экспертном оборудовании произведено изъятие из системного блока указанного НЖМД №1.

В результате исследования состояния системного блока без НЖМД установлено:

- Значение системной даты, имеющееся в представленном на исследование системном блоке соответствует текущей.

- Значение системного времени, имеющееся в представленном на исследование системном блоке, отстает от текущего на 3 минуты.

- Процесс загрузки операционной системы с загрузочного диска эксперта производится полностью.

- Имеющийся накопитель на гибких магнитных дисках (3,5 дюйма) – находится в работоспособном состоянии (осуществляется чтение и запись на гибкий магнитный диск эксперта).

- Имеющийся накопитель (DVD-RW) фирмы NEC Corporation находится в работоспособном состоянии (осуществляется чтение и запись на диск (DVD-R) эксперта).

4.2.Исследование состояния накопителей на жестких магнитных дисках (НЖМД №№1-4). Исследуемый НЖМД №1 подключаллся к лабораторному компьютеру в качестве внешнего съемного диска по USB-шине. Исследуемые НЖМД защищались от записи с помощью программного средства блокирования записи NTFS Software Write-block XP (блокиратора записи разработанного National Center For Forensic Science). Основные характеристики НЖМД №1 получены с помощью программного обеспечения для экспертного исследования компьютерных носителей информации EnCase Forensic Edition v.4.20 и программы partinfo.exe из комплекта PowerQuest Partition Magic 8.0. В результате исследования установлено:

- Количество цилиндров в системе адресации CHS 14593;
- Количество головок в системе адресации CHS 255 ;
- Количество секторов на дорожке в системе адресации CHS 63;
- Значение хэш-функции, рассчитанное для НЖМД по алгоритму MD5; 17B21A8B364CA77DA9BC537442795EDB ;
- Раздел №1 (C:);
- Тип раздела FAT32X;
- Номер раздела 41B6376B;
- Метка раздела SYSTEM ;
- Объем раздела (байт) 120031478784 ;
- Занято (байт) 51420562432;

Исследуемый НЖМД №1 не имеют повреждений целостности структуры данных, доступ к данным возможен.

В Ы В О Д Ы :

1) На экспертизу был представлен НЖМД фирмы Seagate марки U Series 5 модель ST320413A и системный блок (в которых находялся НЖМД 1). Так как представленный системный блок не являются фирменной сборкой, отнести их к каким-то конкретным моделям не представляется возможным. Комплектация представленного системного блока описана в таблице 1 заключения эксперта.

2) При использовании специализированного технологического оборудования, было определено, что представленный НЖМД и комплектующие, входящие в состав системного блока, находятся в исправном состоянии. Это подтверждает их работоспособность и пригодность для дальнейшего исследования.

3) Было установлено, что все разделы загрузки системы на жестком диске и системных блоках находятся в исправном состоянии, они не повреждены. Это включает в себя как системные разделы, так и разделы для хранения файлов. Структура файловой системы сохранена, что позволяет без проблем загружать операционную систему и обращаться к файлам. Это подтверждает возможность использования данных без ограничений и готовность системы к дальнейшей работе.

4) На представленном жестком диске имеется удаленная информация. Разделы диска не были полностью стерты перезаписаны или другими данными, также некоторые из этих разделов помечены как доступные для перезаписи. Удаленная информация остается доступной для восстановления.

5) Все исследованные носители информации, включая жесткий диск и системные блоки, находятся в исправном состоянии и не требуют восстановления.

Приложение И

Постановление программно-компьютерной экспертизы.

ПОСТАНОВЛЕНИЕ

о назначении программно-компьютерной **судебной экспертизы**
(какой именно)

Санкт-Петербург « 21 » Декабря 2023 г.
(место составления)

старший следователь СО по Центральному р-н СУСК при пр-ре РФ по Сб юрист 2 класса
(должность следователя (дознавателя),
Калганов Н. С. ,
классный чин или звание, фамилия, инициалы)
рассмотрев материалы уголовного дела № _____ ,

У С Т А Н О В И Л :

4 декабря 2023 был совершён обыск в квартире подозреваемого Георгиева Владимира
(излагаются основания назначения
Игоревича. В ходе обыска были изъяты системный блок и электронные носители. На изъятых
судебной экспертизы)
электронных носителях предположительно находится вредоносное ПО при помощи которого
подозреваемый осуществил преступные действия.

На основании изложенного и руководствуясь ст. 195 (196) и 199 УПК РФ,

П О С Т А Н О В И Л :

1. Назначить программно-компьютерную
(какую именно)
судебную экспертизу, производство которой поручить Левину Алексею Егоровичу

(фамилия, имя, отчество эксперта либо

наименование экспертного учреждения)

2. Поставить перед экспертом вопросы:

Какую информацию и файлы содержат предъявленные на экспертизу системные блоки и жесткий диск?

Какие программы содержатся на предъявленных системных блоках и жестком диске?

Имеется ли удаленная информация на представленных системных блоках и жестком диске? Возможно ли ее восстановление? Если да, то каково ее содержание, возможности использования?

3. Предоставить в распоряжение эксперта материалы: Системный блок персонального
(какие именно)

компьютера, жёсткие диск

4. Поручить: Осипову А. Д.
(кому именно)

разъяснить эксперту права и обязанности, предусмотренные ст. 57 УПК РФ, и предупредить его об уголовной ответственности в соответствии со ст. 307 УК РФ за дачу заведомо ложного заключения[2].

Следователь (дознаватель) _____
(подпись)

Права и обязанности, предусмотренные ст. 57 УПК РФ, мне разъяснены «____» _____ 20___ г.

Одновременно я предупрежден об уголовной ответственности в соответствии со ст. 307 УК РФ за дачу заведомо ложного заключения.

Эксперт _____
(подпись)

2 Данная графа заполняется в случаях, предусмотренных частью второй ст. 199 УПК РФ.

Приложение К

Заключение эксперта о программно-компьютерной экспертизе

Подписка

Мне, сотруднику , в соответствии с ч.2 ст.199 УПК России разъяснены права и ответственность эксперта, предусмотренные ст.57 УПК России.

Об ответственности за дачу заведомо ложного заключения по ст.307 УК России и за разглашение данных предварительного расследования предупрежден.

З А К Л Ю Ч Е Н И Е Э К С П Е Р Т А

№ от 2024 г.

Эксперт произвел компьютерно-техническую судебную экспертизу. на судебную экспертизу поступили:

1. Системный блок.

2. Ноутбук

3. Накопитель на жестком магнитном диске (НЖМД).

4. Флеш-накопитель

5. Постановление о назначении экспертизы.

Перед экспертом поставлены вопросы:

1) Какую информацию и файлы содержат предъявленные на экспертизу системные блоки и жесткий диск?

2) Какие программы содержатся на предъявленных системных блоках и жестком диске?

3) Имеется ли уничтоженная информация на представленных системных блоках и жестком диске? Возможно ли ее восстановление? Если да, то каково ее содержание, возможности использования?

ИССЛЕДОВАНИЕ

1. План исследования Исследование компьютерной техники, поступившей на экспертизу, проводилось в следующей последовательности:

1.1.Исследование файловой системы и информации на НЖМД.

1.2.Исследование программного обеспечения на НЖМД.

1.3.Исследование компьютерной информации с целью поиска текстовых файлов.

1.4.Исследование компьютерной информации с целью поиска удаленных файлов и их последующего восстановления.

2 Методика исследование файловой системы и информации на НЖМД.

2.1. Исследование файловой системы и информации на НЖМД системных блоков, поступивших на экспертизу проводилось по следующей методике:

- производился поиск файлов с расширением имен, соответствующим программамархиваторам; выявленные архивные файлы разархивировались в отдельную папку (каталог) на НЖМД лабораторного компьютера;

- производился поиск удаленных файлов; файлы, подлежащие восстановлению, восстанавливались в отдельную папку (каталог) НЖМД лабораторного компьютера;

- производился поиск скрытых (зашифрованных) данных (логических и виртуальных дисков, папок (каталогов) и файлов данных);

- определялись признаки поиска информации (ключевые слова, изображения, расширения имен файлов и т.д.), соответствующие задачам исследования;

- производился поиск файлов, содержащих искомые признаки с помощью

специальных программ поиска информации на исследуемом носителе данных (точной копии) и в каталогах с восстановленными и разархивированными файлами на лабораторном компьютере;

- осуществлялся просмотр (визуализация) выявленных файлов, содержащих искомые признаки с помощью соответствующего программного обеспечения;

- производилась распечатка информации из файлов, содержание которых соответствует задачам исследования;

- производилась запись файлов, содержание которых соответствует задачам исследования, на оптический компакт-диск.

3. Экспертное оборудование и методическая литература, использованные при проведении исследования

3.1. Аппаратно-программный комплекс для экспертного исследования компьютерных носителей информации в составе: - персональная ЭВМ на базе процессора Intel Celeron 2,4 ГГц; - лазерный принтер «HP LaserJet 1200» производства «Hewlett Packard» (США). -программное обеспечение для экспертного исследования компьютерных носителей информации «EnCase Forensic Edition v.4.20» производства «Guidance Software Inc.» ; -операционная система «Microsoft Windows XP Professional» производства «Microsoft» ; - прикладное программное обеспечение «Microsoft Office XP Professional» производства «Microsoft» (США); -сервисное программное обеспечение PowerQuest Partition Magic 8.0; -сервисное программное обеспечение NTFS Software Write-block XP (блокиратор записи разработанного National Center For Forensic Science); -сервисное программное обеспечение WinRAR 3.0.

В Ы В О Д Ы :

1) Исследование файловой системы и информации на НЖМД:

Был проведен детальный анализ файловой системы, что позволило выявить необычные паттерны использования дискового пространства. Файлы report.docx и budget.xlsx были спрятаны в системной папке C:\Windows\ System32\, которая обычно не используется для хранения пользовательских данных. Кроме того, файл notepad.exe был замаскирован под системный файл svchost.exe, изменением его имени.

2) Исследование программного обеспечения на НЖМД:

Было обнаружено несколько программ, которые обычно не используются в повседневной работе. Одна из них, photo_viewer.exe. Кроме того, были обнаружены обычные приложения, такие как браузеры Chrome и Yandex, которые используются для доступа в интернет.

3) Исследование компьютерной информации с целью поиска текстовых файлов:

Были найдены текстовые файлы, такие как документы Word (report.docx, summary.docx) и PDF (manual.pdf, instructions.pdf). Также были найдены файлы кеша браузера.

4) Исследование компьютерной информации с целью поиска удаленных файлов и их последующего восстановления:

В ходе восстановления удаленных файлов были обнаружены текстовые файлы лицензии lifetime.lic, а также файлы браузеров и архивы. Был частично восстановлен архив spoof_methods.zip. Удалось восстановить только заголовки имен вложенных запакованных файлов, а также сигнатуры формата данных файлов. Были полностью восстановлены графические изображения и текстовые документы, а также yandex_history.db, Cookies.sql. Данные файлы возможно использовать для дальнейшего изучения их содержания.

Приложение Л

Постановление информационно-компьютерной экспертизы.

ПОСТАНОВЛЕНИЕ

о назначении информационно-компьютерной **судебной экспертизы**
(какой именно)

Санкт-Петербург « 23 » Декабря 2024 г.
(место составления)

старший следователь СО по Центральному р-н СУСК при пр-ре РФ по Сб юрист 2 класса
(должность следователя (дознавателя),
Калганов Н. С. ,
классный чин или звание, фамилия, инициалы)
рассмотрев материалы уголовного дела № _____ ,

У С Т А Н О В И Л :

4 декабря 2023 был совершён обыск в квартире подозреваемого Георгиева Владимира
(излагаются основания назначения
Игоревича. В ходе обыска были изъяты системный блок и электронные носители. На изъятых
судебной экспертизы)
электронных носителях предположительно находится вредоносное ПО при помощи которого
подозреваемый осуществил преступные действия.

На основании изложенного и руководствуясь ст. 195 (196) и 199 УПК РФ,

П О С Т А Н О В И Л :

1. Назначить информационно-компьютерную
(какую именно)
судебную экспертизу, производство которой поручить Левину Алексею Егоровичу

(фамилия, имя, отчество эксперта либо

наименование экспертного учреждения)

2. Поставить перед экспертом вопросы:

Какую информацию содержат предъявленные на экспертизу жесткий диск и ее назначение?

Каково назначение программ, содержатся на предъявленных системных блоках и жестком диске?

Каково содержание восстановленных файлов, есть ли возможность их использовать?

3. Предоставить в распоряжение эксперта материалы: Системный блок персонального
(какие именно)
компьютера, жёсткие диск

4. Поручить: Осипову А. Д.
(кому именно)

разъяснить эксперту права и обязанности, предусмотренные ст. 57 УПК РФ, и предупредить его об уголовной ответственности в соответствии со ст. 307 УК РФ за дачу заведомо ложного заключения[3].

Следователь (дознаватель) _____
(подпись)

Права и обязанности, предусмотренные ст. 57 УПК РФ, мне разъяснены «____» _____ 20___ г.

Одновременно я предупрежден об уголовной ответственности в соответствии со ст. 307 УК РФ за дачу заведомо ложного заключения.

Эксперт _____
(подпись)

3 Данная графа заполняется в случаях, предусмотренных частью второй ст. 199 УПК РФ.

Приложение М

Заключение эксперта о программно-компьютерной экспертизе

Подписка

Мне, сотруднику , в соответствии с ч.2 ст.199 УПК России разъяснены права и ответственность эксперта, предусмотренные ст.57 УПК России.

Об ответственности за дачу заведомо ложного заключения по ст.307 УК России и за разглашение данных предварительного расследования предупрежден.

З А К Л Ю Ч Е Н И Е Э К С П Е Р Т А

№ от 2024 г.

Эксперт произвел компьютерно-техническую судебную экспертизу. на судебную экспертизу поступили:

1. Системный блок.

2. Ноутбук

3. Накопитель на жестком магнитном диске (НЖМД).

4. Флеш-накопитель

5. Постановление о назначении экспертизы.

Перед экспертом поставлены вопросы:

1) Какую информацию содержат предъявленные на экспертизу жесткий диск и ее назначение?

2) Каково назначение программ, содержатся на предъявленных системных блоках и жестком диске?

3) Каково содержание восстановленных файлов, есть ли возможность их использовать?

ИССЛЕДОВАНИЕ

1. План исследования Исследование компьютерной техники, поступившей на экспертизу, проводилось в следующей последовательности:

1.1.Исследование файлов, их содержимого и назначения этого содержимого.

1.2.Исследование программного обеспечения на НЖМД и его назначения.

1.3.Исследование компьютерной информации с целью изучения востановленных файлов и их назначения и возможности использования.

2. Экспертное оборудование и методическая литература, использованные при проведении исследования

2.1. Аппаратно-программный комплекс для экспертного исследования компьютерных носителей информации в составе: - персональная ЭВМ на базе процессора Intel Celeron 2,4 ГГц; - лазерный принтер «HP LaserJet 1200» производства «Hewlett Packard» (США). -программное обеспечение для экспертного исследования компьютерных носителей информации «EnCase Forensic Edition v.4.20» производства «Guidance Software Inc.» ; -операционная система «Microsoft Windows XP Professional» производства «Microsoft» ; - прикладное программное обеспечение «Microsoft Office XP Professional» производства «Microsoft» (США); -сервисное программное обеспечение PowerQuest Partition Magic 8.0; -сервисное программное обеспечение NTFS Software Write-block XP (блокиратор записи разработанного National Center For Forensic Science); -сервисное программное обеспечение WinRAR 3.0.

В Ы В О Д Ы :

1) Исследование файлов, их содержимого и назначения этого содержимого:

Был проведен детальный анализ файлов report.docx и budget.xlsx, находящихся в системной папке C:\Windows\System32\, которая обычно не используется для хранения пользовательских данных. Файл report.docx содержит подробный отчет о выполнении некоторого проекта, включая описание выполненных работ, использованных ресурсов и достигнутых результатов. Файл budget.xlsx содержит детализированный бюджет проекта с расчетами затрат на каждый этап. Документы Word (summary.docx) и PDF (manual.pdf, instructions.pdf) содержат различные виды информации. summary.docx содержит краткое изложение основных моментов проекта. manual.pdf является руководством пользователя для некоторого программного продукта, включая инструкции по установке, настройке и использованию. instructions.pdf содержит подробные инструкции по выполнению некоторой задачи, включая последовательность действий, необходимые инструменты и советы по установке програмного обеспечения без использования лицензии.

2) Исследование программного обеспечения на НЖМД и его назначения:

Было обнаружено несколько программ, которые обычно не используются в повседневной работе. Одна из них, hidden_crack.exe, была идентифицирована как вредоносное ПО. Это ПО было замаскировано под приложение photo_viewer.exe. Кроме того, в браузерах Chrome и Yandex, было обнаружено использование расширений, не представленных в официальном магазине chrome. Назначение данных расширений не возможно определить, ввиду недостаточной кфалификации эксперта в области сетевых приложений.

Был проведен анализ кэша браузера. Это позволило выявить историю посещения веб-сайтов и получить дополнительную информацию о действиях пользователя. В частности, были обнаружены следы посещения

сайтовmalwareexample.com и phishingexample.net. Назначение данных сайтов не возможно определить, ввиду недостаточной кфалификации эксперта в этой области.

3) Исследование компьютерной информации с целью поиска удаленных файлов и их последующего восстановления:

Был изучен восстановленный архив personal_photos.zip. Файлы архива содержат заголовки, которые обычно ассоциируются с графическими изображениями. Некоторые из этих заголовков файлов не соответствовали ожидаемым форматам изображений, что указывает на возможную попытку скрыть иные типы файлов. Файл лицензии lifetime.lic содержит ключ активации некоторого програмного обеспечения. Файлы yandex_history.db, Cookies.sql содержат историю посещений веб ресурсов, а также сохраненные сессии сайтов. Данные в базе данных Cookies.sql защифрованы и нет возможности их дальнейшего использования. Файл yandex_history.db доступен к чтению и изменению.

Приложение Н

Постановление компьютерно-сетевой экспертизы.

ПОСТАНОВЛЕНИЕ

о назначении информационно-компьютерной **судебной экспертизы**
(какой именно)

Санкт-Петербург « 23 » Декабря 2024 г.
(место составления)

старший следователь СО по Центральному р-н СУСК при пр-ре РФ по Сб юрист 2 класса
(должность следователя (дознавателя),
Калганов Н. С. ,
классный чин или звание, фамилия, инициалы)
рассмотрев материалы уголовного дела № _____ ,

У С Т А Н О В И Л :

4 декабря 2023 был совершён обыск в квартире подозреваемого Георгиева Владимира
(излагаются основания назначения
Игоревича. В ходе обыска были изъяты системный блок и электронные носители. На изъятых
судебной экспертизы)
электронных носителях предположительно находится вредоносное ПО при помощи которого
подозреваемый осуществил преступные действия.

На основании изложенного и руководствуясь ст. 195 (196) и 199 УПК РФ,

П О С Т А Н О В И Л :

1. Назначить компьютерно-сетевая
(какую именно)
судебную экспертизу, производство которой поручить Левину Алексею Егоровичу

(фамилия, имя, отчество эксперта либо

наименование экспертного учреждения)

2. Поставить перед экспертом вопросы:

Каковы источники текстовых файлов? Есть ли возможность их определить?

Каковы источники приложений? Есть ли возможность их определить? Каково назначение сетевых приложений?

Каково содержание обнаруженных посещенных сетевых ресурсов?

3. Предоставить в распоряжение эксперта материалы: Системный блок персонального
(какие именно)
компьютера, жёсткие диск

4. Поручить: Осипову А. Д.
(кому именно)

разъяснить эксперту права и обязанности, предусмотренные ст. 57 УПК РФ, и предупредить его об уголовной ответственности в соответствии со ст. 307 УК РФ за дачу заведомо ложного заключения[4].

Следователь (дознаватель) _____
(подпись)

Права и обязанности, предусмотренные ст. 57 УПК РФ, мне разъяснены «____» _____ 20___ г.

Одновременно я предупрежден об уголовной ответственности в соответствии со ст. 307 УК РФ за дачу заведомо ложного заключения.

Эксперт _____
(подпись)

4 Данная графа заполняется в случаях, предусмотренных частью второй ст. 199 УПК РФ.

Приложение О

Заключение эксперта о компьютерно-сетевой экспертизе

Подписка

Мне, сотруднику , в соответствии с ч.2 ст.199 УПК России разъяснены права и ответственность эксперта, предусмотренные ст.57 УПК России.

Об ответственности за дачу заведомо ложного заключения по ст.307 УК России и за разглашение данных предварительного расследования предупрежден.

З А К Л Ю Ч Е Н И Е Э К С П Е Р Т А

№ от 2024 г.

Эксперт произвел компьютерно-техническую судебную экспертизу. на судебную экспертизу поступили:

1. Системный блок.

2. Ноутбук

3. Накопитель на жестком магнитном диске (НЖМД).

4. Флеш-накопитель

5. Постановление о назначении экспертизы.

Перед экспертом поставлены вопросы:

1) Каковы источники текстовых файлов? Есть ли возможность их определить?

2) Каковы источники приложений? Есть ли возможность их определить? Каково назначение сетевых приложений?

3) Какие сетевые ресурсы посещались с устройства? Каково содержание и назначение обнаруженных посещенных сетевых ресурсов?

ИССЛЕДОВАНИЕ

1. План исследования Исследование компьютерной техники, поступившей на экспертизу, проводилось в следующей последовательности:

1.1. Исследование источников текстовых файлов.

1.2. Исследование программного обеспечения, его источников и назначение сетевых приложений.

1.3.Исследование посещенных сетевых ресурсов, их ссодержания и назначение.

2. Экспертное оборудование и методическая литература, использованные при проведении исследования

2.1. Аппаратно-программный комплекс для экспертного исследования компьютерных носителей информации в составе: - персональная ЭВМ на базе процессора Intel Celeron 2,4 ГГц; - лазерный принтер «HP LaserJet 1200» производства «Hewlett Packard» (США). -программное обеспечение для экспертного исследования компьютерных носителей информации «EnCase Forensic Edition v.4.20» производства «Guidance Software Inc.» ; -операционная система «Microsoft Windows XP Professional» производства «Microsoft» ; - прикладное программное обеспечение «Microsoft Office XP Professional» производства «Microsoft» (США); -сервисное программное обеспечение PowerQuest Partition Magic 8.0; -сервисное программное обеспечение NTFS Software Write-block XP (блокиратор записи разработанного National Center For Forensic Science); -сервисное программное обеспечение WinRAR 3.0.

В Ы В О Д Ы :

1) Исследование источников текстовых файлов:

В ходе исследования был проведен детальный анализ файлов report.docx и budget.xlsx, которые находятся в системной папке C:\Windows\System32\. Обычно эта папка не используется для хранения пользовательских данных, что делает нахождение этих файлов в ней необычным. Эти файлы были созданы на данном устройстве, что подтверждает их локальное происхождение. Однако, без дополнительных данных, невозможно определить, выкладывались ли эти файлы в сеть. Документы Word (summary.docx) и PDF (manual.pdf, instructions.pdf) были скачаны из сети интернет. Это было определено по метаданным этих файлов, которые включают информацию о дате создания файла, источнике загрузки — malware.com. Сайт имеет региональные ограничения и оценить его содержимое не предоставляется возможным.

2) Исследование программного обеспечения, его источников и назначение сетевых приложений.

Было исследовано приложение hidden_crack.exe. Файл не содержит метаданных, поэтому определить его проихсождение невозможно. Было произведено исследование расширений Chrome и Yandex. Было обнаружено, что расширения выполняют функцию VPN-сервиса для предоставления доступа к запрещенным сетевым ресурсам. В файле манифеста расширения также было найдено упоминание malware.com, что позволяет заключить, что данное расширение использовалось для получения доступа к этому сайту.

Был проведен анализ кэша браузера. Это позволило выявить историю посещения веб-сайтов и получить дополнительную информацию о действиях пользователя. В частности, были обнаружены следы посещения сайтов malwareexample.com и phishingexample.net. Назначение данных сайтов не

возможно определить, ввиду недостаточной кфалификации эксперта в этой области.

3) Исследование посещенных сетевых ресурсов, их ссодержания и назначение:

Файл лицензии lifetime.lic был получен с сайта phishingexample.net. Был изучен файл yandex_history.db. В файле содержится информация о посещении сайта malwareexample.com, который вероятно является зеркалом malware.com. Данный сайт не имеет региональных ограничений. Было выяснено, что домен сайта находится в Индии. Сайт не имеет сертификата. Сайт представляет собой форум по обсуждению вредоносного ПО. Также на сайте доступны ссылки для скачивания ПО. Эти данные позволяют заключить, что на данном компьютере осуществлялись неоднократные попытки посещения запрещенных на территории РФ сайтов с вредоносным ПО.