Дело № 1-322/2017

П О С Т А Н О В Л Е Н И Е

г. Новочебоксарск 25 декабря 2017 года

Новочебоксарский городской суд Чувашской Республики

под председательством судьи Ефимова Д.Е.,

при секретаре судебного заседания Лисицыной М.А.,

с участием:

государственного обвинителя – старшего помощника прокурора г. Новочебоксарска Чувашской Республики Михайлова Ю.П.,

подсудимого Кузнецова В.В., его защитника – адвоката Демяшкина И.К., представившего ордер и удостоверение,

рассмотрев в открытом судебном заседании в помещении городского суда уголовное дело в особом порядке, предусмотренном главой 40.1 УПК РФ, в отношении

КУЗНЕЦОВА Валерия Валерьевича, ДД.ММ.ГГГГ года рождения, гражданина Российской Федерации, уроженца <адрес>, зарегистрированного по месту жительства по адресу: <адрес>, ´ ные изъяты> детей, работающего <данные изъяты>», ранее не судимого,

обвиняемого в совершении преступлений, предусмотренных ч.2 ст.273, ч.1 ст. 273 Уголовного кодекса Российской Федерации (далее – УК РФ),

у с т а н о в и л :

Кузнецов В.В. совершил преступления, при следующих обстоятельствах.

Так, Кузнецов В.В., период с ДД.ММ.ГГГГ по ДД.ММ.ГГГГ, более точное время предварительным следствием не установлено, имея совместный с ФИО3 преступный умысел, направленный на использование и распространение вредоносных компьютерных программ, находясь по месту своего жительства, расположенном по адресу: <адрес>, используя свой ноутбук «Apple MacBook», Serial № №», подключенный к ОТКС Интернет через провайдера АО «ЭР-Телеком Холдинг», предоставляющего услуги доступа в ОТКС Интернет, действуя совместно с ФИО3, который проживал по адресу: <адрес>, и использовал ноутбук «Apple MacBook Pro», Serial № №, имевший выход в ОТКС Интернет через провайдера ООО «Новочебоксарское кабельное телевидение», реализуя единый преступный умысел, направленный на распространение и использование вредоносных компьютерных программ, при неустановленных предварительным следствием обстоятельствах, через ОТКС Интернет получили доступ на правах аренды к учетной записи с именем пользователя «admin» в программной оболочке сервера с IP-адресом №, на котором размещалось программное обеспечение (далее - ПО), называемое связкой эксплойтов «Nuclear». Кузнецов В.В. и ФИО3 из хакерских форумов в сети Интернет достоверно зная, что указанная связка эксплойтов «Nuclear» является вредоносной компьютерной программой и содержит в себе следующие элементы:

- вредоносная компьютерная программа «HEUR:Exploit.SWF.Agent.gen», способная скрыто эксплуатировать программную уязвимость CVE-2014-0556 в программном обеспечении Adobe Flash Player № (эксплуатация возможна и в иных версиях ПО Adobe Flash Player), используемом в частном случае в качестве расширения браузера Internet Explorer № в операционной системе (далее - ОС) Windows 7 x86. Эксплуатация происходит при посещении пользователем с помощью указанного ПО сетевого ресурса, с которого загружается и запускается данная программа;

- вредоносная компьютерная программа «HEUR:Exploit.SWF.Agent.gen», способная скрыто эксплуатировать программную уязвимость CVE-2015-0336 в ПО Adobe Flash Player №(эксплуатация возможна и в иных версиях ПО Adobe Flash Player), используемом в частном случае в качестве расширения браузера Internet Explorer № в ОС Windows 7 x86. Эксплуатация происходит при посещении пользователем с помощью указанного ПО сетевого ресурса, с которого загружается и запускается данная программа;

- вредоносная компьютерная программа «HEUR:Exploit.SWF.Agent.gen», способная скрыто эксплуатировать программные уязвимости CVE-2015-5122, CVE-2015-7645, CVE-2016-1019 в ПО Adobe Flash Player, используемом в частном случае в качестве расширения браузера Internet Explorer № в ОС Windows 7 x86. В зависимости от версии ПО Adobe Flash Player программой эксплуатируется соответствующая ей уязвимость (для версии № - CVE-2015-5122, 19.0.0.207 - CVE-2015-7645, 20.0.0.228 - CVE-2016-1019). Эксплуатация происходит при посещении пользователем с помощью указанного ПО сетевого ресурса, с которого загружается и запускается данная программа;

- вредоносная компьютерная программа Javascript-сценарий «HEUR:Paranoid.Script.Detect», способная скрыто эксплуатировать программную уязвимость CVE-2015-2413 в браузере Internet Explorer версии № в ОС Windows 7 x86. Эксплуатация происходит при посещении пользователем с помощью указанного ПО сетевого ресурса, на котором содержится данный сценарий;

- вредоносная компьютерная программа «HEUR:Exploit.Script.Generic» способная скрыто эксплуатировать программные уязвимости CVE-2014-6332, CVE-2015-2413 в браузере Internet Explorer. В зависимости от версии браузера и ОС Windows программа эксплуатирует уязвимость CVE-2014-6332 для ПО Internet Explorer № и ОС Windows XP, уязвимость CVE-2015-2419 - для ПО Internet Explorer № и ОС Windows 7, эксплуатация которых происходит при посещении пользователем с помощью указанного ПО сетевого ресурса, на котором содержится данный сценарий.

Кузнецов В.В. и ФИО3 достоверно осознавали, что в результате эксплуатации указанной связки эксплойтов - вышеуказанные вредоносные компьютерные программы способны скрытно от пользователя – потенциальной «жертвы» компьютерной атаки выполнять следующие действия:

- сохранять и запускать программу, загруженную с заданного сетевого ресурса;

- загружать программу в адресное пространство стороннего процесса, имя которого соответствует маске «*.exe» с заданного сетевого ресурса с последующим ее исполнением.

Продолжая реализовывать свой совместный преступный план ФИО3 по согласованию с Кузнецовым В.В., из корыстной заинтересованности, направленной на продажу «взломанных» ЭВМ третьим лицам, в указанный период времени, при неустановленных следствием обстоятельствах, у неустановленного пользователя форума «exploit.in», умышленно приобрел экземпляр вредоносной компьютерной программы известной под наименованием «Andromeda Bot», а также средства её настройки с панелью администрирования с модулями, которые расширяли её функциональность.

При этом Кузнецов В.В. и ФИО3, достоверно знали, что указанная программа, определяющаяся антивирусным программным обеспечением как вредоносная компьютерная программа, относящаяся к типу «Backdoor.Win32.Androm.jmvq» способна скрытно от пользователя – потенциальной «жертвы» компьютерной атаки выполнять следующие действия:

осуществлять установку себя в ОС, включая добавление себя в список программ, автоматически выполняемых после входа пользователя в ОС.

отправлять серийный номер системного раздела ОС, версию ОС, языковые настройки ОС, IP-адрес ЭВМ, а также данные, полученные от своих модулей на управляющие сервера <данные изъяты>.

по команде управляющего сервера скрытно выполнять следующие действия:

загружать свои модули по ссылке, указанной в команде, и запускать их.

обновлять свой исполняемый файл.

удалять свои сохраненные модули из альтернативных потоков своего исполняемого файла.

удалять себя, а также следы оставляемые программой.

загружать в файл по ссылке, указанной в команде, стороннюю программу и запускать ее.

осуществлять запуск своих ранее сохраненных модулей, содержащихся в альтернативных потоках своего исполняемого файла.

останавливать службы Windows «SharedAccess», «wuauserv», «MpsSvc», «WinDefend», а также отключать их автоматический запуск при загрузке ОС.

отключать службу Windows «Контроль учетных записей (UAC)».

отключать отображение всплывающих уведомлений Windows.

скрывать значок службы Windows Центр поддержки из области уведомлений.

отключать отображение скрытых файлов и каталогов, заранее, до производства описанных действий.

Кузнецов В.В. и ФИО3 осознавая, что вышеуказанные дополнительные модули включали в себя:

- компьютерную вредоносную программу «Pony», определяющуюся антивирусным программным обеспечением как «Trojan-PSW.Win32.Tepfer.gen», которая способна скрыто копировать и отправлять на управляющий сервер данные о версии ОС «жертвы», ее разрядности, языковых настройках, свой уникальный идентификатор, данные, содержащиеся в хранилище учетных данных пользователей, хранилище сертификатов, данные, содержащиеся в системном реестре ОС «Windows» жертвы, включающие в себя сохраненные там логины и пароли к различным сервисам в сети Интернет;

- модуль, способный скрытно функционировать на ЭВМ «жертвы» в качестве прокси-сервера;

- модуль, способный скрытно собирать текстовые данные, вводимые пользователем в формы ввода на веб-страницах при использовании браузеров «Firefox», «Internet Explorer», «Google Chrome»;

- модуль, способный обеспечивать скрытное удаленное управления зараженной СВТ с использованием компьютерной программы «TeamViewer ДД.ММ.ГГГГ QS», после чего дополнили этими модулями вредоносную компьютерную программу «Andromeda bot» в целях повышения её эффективности.

Для обеспечения функционирования вредоносной компьютерной программы «Andromeda Bot» и вышеуказанных модулей к ней ФИО3 по предварительному сговору с Кузнецовым В.В., при вышеуказанных обстоятельствах, у неустановленных пользователей сервиса «Jabber», специализирующихся на услугах по регистрации доменных имен, арендовали доменные имена <данные изъяты> которые предназначались для серверов удаленного управления программой «Andromeda Bot», а также доменное имя <данные изъяты>» для сервера управления модулем «Trojan-PSW.Win32.Tepfer.gen» («Pony»).

Кузнецов В.В. для достижения совместных с ФИО3 преступных целей в 2016 г., более точная дата и время предварительным следствием не установлена, находясь по месту своего жительства, имея совместный с ФИО3 преступный умысел, направленный на использование и распространение вредоносных компьютерных программ, арендовал в ОТКС Интернет сервер с IP-адресом № у провайдера хостинга «Megahoster Network» с использованием их сайта в сети Интернет, расположенном по адресу «http://megahoster.net», предварительно зарегистрировав на указанном сайте учетную запись, имеющую привязку к используемому им адресу зарегистрированной <данные изъяты>. Далее Кузнецов В.В., действуя согласно разработанному совместно с ФИО3преступному плану, на указанном сервере разместил компьютерное программное обеспечение «TDS», предназначенное для управления процессом перенаправления пользователей с различных ресурсов в ОТКС Интернет на используемый Кузнецовым В.В. и ФИО3 вышеуказанный сервер с IP-адресом №.

Кузнецов В.В. и ФИО3 достоверно зная, что ПО «TDS» на сервере с IP-адресом № имело возможность анализировать сетевые запросы Интернет - пользователей, обращавшихся на подконтрольные Кузнецову В.В. и ФИО3 сайтов в ОТКС Интернет, осуществлять отбор Интернет-пользователя по таким параметрам как: локация пользователя (по расположению государства); операционная система; наименование, версия браузера; сайт в сети Интернет, с которого перенаправлен Интернет-пользователь. В дальнейшем Кузнецов В.В. действуя совместно с ФИО3 в указанных целях скрыто перенаправлял потенциальные «жертвы», посетившие данный сайт, на указанную связку эксплойтов с целью внедрения в ЭВМ «жертвы» перечисленные вредоносные компьютерные программы. При этом Кузнецов В.В. для более эффективного достижения совместных с ФИО3 преступных целей, в целях предотвращения обнаружения сервера связки эксплойтов антивирусным ПО умышленно перенаправлял трафик «жертв» на связку эксплойтов через дополнительный промежуточный узел - так называемый «прокси-сервер».

ДД.ММ.ГГГГ ФИО3, находясь у себя дома по указанному адресу, действуя согласно распределенным преступным ролям, и реализуя с Кузнецовым В.В. единый преступный умысел, направленный на использование и распространение вредоносных компьютерных программ, для организации прохождения трафика потенциальных «жертв» через указанные «прокси-сервера» зарегистрировал доменные имена <данные изъяты>, на 1 год у регистратора доменных имен ООО «Телекоммуникационная компания Рустелеком» (ИНН: №), расположенном по адресу: г. Москва, Пыжевский пер., д. 5, стр. 1, офис 308, с использованием принадлежащего указанной организации сайта в ОТКС Интернет «roboname.com», на котором у ФИО3 имелась учетная запись, привязанная к используемому им адресу электронной почты «<данные изъяты>.ru».

Далее в «системе управления трафиком» на сервере с IP-адресом № Кузнецов В.В., действуя совместно с ФИО3 в указанных преступных целях, произвел настройки, исключающие возможность перенаправления «жертв» из России и стран СНГ на используемую ими связку эксплойтов, в целях избежания возможного их обнаружения и дальнейшего преследования правоохранительными органами указанных государств.

Тогда же ФИО3, действуя согласованно с Кузнецовым В.В., в целях достижения указанного единого преступного умысла, с использованием программного обеспечения, установленного на сервере с IP-адресом № произвел настройки связки эксплойтов на данном сервере таким образом, чтобы актуальный URL-адрес прокси-сервер выдавался связкой только при обращении к ней с используемого ими сервера системы управления трафиком с IP-адресом № в целях предотвращения обнаружения вышеуказанных вредоносных компьютерных программ антивирусным ПО.

ДД.ММ.ГГГГ в этих же целях ФИО3 и Кузнецов В.В. при аналогичных обстоятельствах арендовали на 1 год доменное имя «myclassicshoes.net» у регистратора доменных имен ООО «Телекоммуникационная компания Рустелеком», и загрузили на данный сайт созданный ими контент по внешнему виду схожий с Интернет-магазином по продаже обуви и различных аксессуаров в целях привлечения по методу социальной инженерии большего количества посетителей и скрытия от них фактического назначения – внедрение в память их ЭВМ указанных вредоносных компьютерных программ.

В это же время ФИО3, реализуя указанный совместный преступный умысел с Кузнецовым В.В., на сайте «myclassicshoes.net» разместил скрытый программный код, перенаправляющий посетителя данного сайта помимо его воли на вышеуказанный сервер системы управления трафиком с IP-адресом №.

ДД.ММ.ГГГГ в 16 часов 27 минут, после настройки программы «Andromeda Bot», ФИО3 при вышеуказанных обстоятельствах действуя согласованно с Кузнецовым В.В., реализуя совместный преступный план, направленный на использование и распространение вредоносных компьютерных программ из корыстной заинтересованности, имея доступ к учетной записи «admin» на сервере в ОТКС Интернет с IP-адресом №находясь в квартире по указанному адресу, через провайдера ООО «Новочебоксарское кабельное телевидение», разместил на указанном сервере исполняемый файл «ADrtr.exe» - исполняемый файл экземпляра вредоносной компьютерной программы «Andromeda Bot» для ОС Windows, в целях его дальнейшего использования путем внедрения в память ЭВМ пользователей ОТКС Интернет вышеуказанных вредоносных компьютерных программ.

Кузнецов В.В., продолжая осуществлять указанный единый с ФИО3 преступный умысел, в конце апреля 2016 г., более точная дата и время предварительным следствием не установлены, находясь по месту своего жительства по указанному адресу, обеспечил перенаправление неустановленных пользователей на сайт «myclassicshoes.net» путем покупки веб-трафика на одной из электронных бирж трафика, размещенных в ОТКС Интернет. Контроль за процессом распространения Кузнецов В.В. и ФИО3 осуществляли путем обращения к серверу связки эксплойтов, расположенных по URL-адресу «<данные изъяты>

В результате этих действий посетители сайта «myclassicshoes.net» скрытно, помимо их воли перенаправлялись на указанный ФИО3 и Кузнецовым В.В. сервер системы управления трафиком с IP-адресом №, который анализировал браузер пользователя, а также страну, из которой шло обращение. В дальнейшем, используя уязвимые версии ПО браузера Internet Explorer или Adobe Flash Player, пользователей ОТКС Интернет через прокси-сервер с сервера связки эксплойтов с IP-адресом № Кузнецов В.В. и ФИО3 загружали «жертве» вредоносные компьютерные программы и сценарии, эксплуатирующие программные уязвимости, тем самым нейтрализуя средства защиты компьютерной информации указанных «жертв» с последующей скрытой загрузкой на их ЭВМ исполняемого файла «ADrtr.exe», размещенного ФИО3 и Кузнецовым В.В. на сервере связки эксплойтов с IP-адресом №.

Таким образом, в результате произведенных действий Кузнецов В.В. и ФИО3, в период с января по декабрь 2016 г., распространили и использовали вредоносные компьютерные программы - связка эксплойтов «Nuclear» и «Andromeda Bot», предназначенные для несанкционированного копирования, модификации компьютерной информации и нейтрализации средств защиты компьютерной информации, путём скрытного внедрения вредоносной компьютерной программы «ADrtr.exe» в память 952 ЭВМ неустановленных пользователей сети Интернет, расположенных за рубежом и идентифицирующихся по следующим IP-адресам: <данные изъяты> Он же в период времени с 22.11.2016 по декабрь 2016 г., находясь по месту своего жительства по адресу: <адрес>, имея преступный умысел, направленный на использование и распространение вредоносных компьютерных программ, предназначенных для несанкционированного блокирования, модификации, копирования компьютерной информации, используя свой ноутбук «Apple MacBook», Serial № C02NQS96G085», подключенный к ОТКС Интернет через провайдера АО «ЭР-Телеком Холдинг», предоставляющего услуги доступа в ОТКС Интернет, с использованием ранее созданной им при неустановленных следствием обстоятельствах своей учетной записи «<данные изъяты>.im» коммуникационного сервиса Jabber, предназначенного для общения в ОТКС Интернет, обратился к пользователям указанного коммуникационного сервиса с псевдонимами «<данные изъяты>.im», «<данные изъяты>», данные которых предварительным следствием не установлены, с просьбой предоставить и настроить ему в пользование экземпляры вредоносных программ, так называемых лоадера и бота для мобильных устройств, работающих под ОС Android. 25.11.2016 в 12 часов 29 минут Кузнецов В.В., имея вышеуказанный умысел, в целях использование и распространение вредоносных компьютерных программ, предназначенных для несанкционированного блокирования, модификации, копирования компьютерной информации на устройствах, работающих на ОС Android, приобрел лоадер «CryptoShield» у пользователя с псевдонимом «<данные изъяты>» путем перечисления со своего Bitcoin-кошелька на Bitcoin-кошелек №, используемый пользователем «№», 2№ единицы **криптовалюты** Bitcoin, которая на тот момент была эквивалента 1500.12 долларов США. ДД.ММ.ГГГГКузнецов В.В. в этих же целях при аналогичных обстоятельствах, приобрел бот под условным наименованием mazar у пользователя «<данные изъяты>.im» путем перечисления ему 1.32103886 единиц **криптовалюты** Bitcoin (эквивалент на тот момент составлял 994.52 долларам США) в качестве оплаты со свого Bitcoin-кошелька на его электронный Bitcoin-кошелёк 1PuEZeu1ErsyBEyCYWZ5p3PXay4yxvC4Dh, после чего загрузил себе его на накопитель информации своего ноутбука. При этом достоверно зная, что указанная вредоносная компьютерная программа с наименованием mazar классифицируется антивирусным программным обеспечением как «<данные изъяты>.a», способна скрытно от пользователей устройств, работающих под операционной системой Android, и помимо их воли выполнять следующие действия: отправлять на управляющий сервер http://<данные изъяты>» IMEI (уникальный идентификатор мобильного оборудования), MSISDN (номер мобильного абонента цифровой сети), MCC и MNC (уникальный идентификатор сотового оператора), версию ОС Android, №

Он же в период времени с 22.11.2016 по декабрь 2016 г., находясь по месту своего жительства по адресу: <адрес>, имея преступный умысел, направленный на использование и распространение вредоносных компьютерных программ, предназначенных для несанкционированного блокирования, модификации, копирования компьютерной информации, используя свой ноутбук «Apple MacBook», Serial № C02NQS96G085», подключенный к ОТКС Интернет через провайдера АО «ЭР-Телеком Холдинг», предоставляющего услуги доступа в ОТКС Интернет, с использованием ранее созданной им при неустановленных следствием обстоятельствах своей учетной записи «<данные изъяты>» коммуникационного сервиса Jabber, предназначенного для общения в ОТКС Интернет, обратился к пользователям указанного коммуникационного сервиса с псевдонимами «<данные изъяты>», «<данные изъяты>», данные которых предварительным следствием не установлены, с просьбой предоставить и настроить ему в пользование экземпляры вредоносных программ, так называемых лоадера и бота для мобильных устройств, работающих под ОС Android.

ДД.ММ.ГГГГ в 12 часов 29 минут Кузнецов В.В., имея вышеуказанный умысел, в целях использование и распространение вредоносных компьютерных программ, предназначенных для несанкционированного блокирования, модификации, копирования компьютерной информации на устройствах, работающих на ОС Android, приобрел лоадер «CryptoShield» у пользователя с псевдонимом «googleplay@exploit.im» путем перечисления со своего Bitcoin-кошелька на Bitcoin-кошелек <данные изъяты> используемый пользователем «<данные изъяты>», № единицы **криптовалюты** Bitcoin, которая на тот момент была эквивалента 1500.12 долларов США.

ДД.ММ.ГГГГ Кузнецов В.В. в этих же целях при аналогичных обстоятельствах, приобрел бот под условным наименованием mazar у пользователя «gm_project@exploit.im» путем перечисления ему 1.32103886 единиц **криптовалюты** Bitcoin (эквивалент на тот момент составлял 994.52 долларам США) в качестве оплаты со свого Bitcoin-кошелька на его электронный Bitcoin-кошелёк <данные изъяты>, после чего загрузил себе его на накопитель информации своего ноутбука. При этом достоверно зная, что указанная вредоносная компьютерная программа с наименованием mazar классифицируется антивирусным программным обеспечением как «HEUR:Trojan-Banker.AndroidOS.Razam.a», способна скрытно от пользователей устройств, работающих под операционной системой Android, и помимо их воли выполнять следующие действия:

отправлять на управляющий сервер http<данные изъяты>» IMEI (уникальный идентификатор мобильного оборудования), MSISDN (номер мобильного абонента цифровой сети), MCC и MNC (уникальный идентификатор сотового оператора), версию ОС Android, модель устройства, список процессов, установленных несистемных программ, содержимое сохраненных входящих SMS-сообщений, имена адресатов, дату/время получения, свой идентификатор установки («№»);

по команде с управляющего сервера скрытно выполнять следующие действия:

изменять свои настройки, включая содержащиеся HTML-сценарии;

контролировать функциональные возможности программы, включая перехват входящих SMS-сообщений;

отправлять SMS-сообщение, номер и адресат которого указаны в команде;

удалять все данные пользователя путем сброса устройства до заводских настроек;

осуществлять телефонный вызов/USSD - запрос на номер, указанный в команде;

отображать/прекращать отображение своего окна;

исполнять/завершать исполнение Javascript-сценариев, полученных в команде.

собирать текст, а также номера адресантов входящих SMS-сообщений;

перехватывать входящие SMS-сообщения или те номера адресантов, которых содержатся в настройках программы, либо содержание которых удовлетворяет определенным установщиком «вируса» условиям. Данные SMS-сообщения могут не сохраняться и не отображаться пользователю.

В указанный период времени Кузнецов В.В., продолжая реализовывать свои вышеуказанные преступные намерения, через электронные биржи трафика, расположенные в ОТКС Интернет, организовал перенаправление неустановленных пользователей сети Интернет на страницу приложения «CryptoShield» сервиса «Google Play» с предложением установки данного приложения в целях обхода средств защиты пользователей устройств, работающих под управлением ОС Android, в целях привлечения как можно большего количества этих пользователей для внедрения в их устройства вредоносной компьютерной программы.

После установки лоадер «CryptoShield» на устройства «жертв» он загрузил вредоносную компьютерную программу бот mazar на их устройства, работающие под управлением операционной системы Android. Статистику установок бота mazar («HEUR<данные изъяты>Кузнецов В.В. отслеживал в панели администрирования на сервере с IP-адресом №.

Таким образом, Кузнецов В.В. в указанный период времени, осуществил использование и распространение вредоносной компьютерной программы mazar, которая заведомо для него предназначена для несанкционированной блокировки, модификации, копирования компьютерной информации и нейтрализации средств защиты компьютерной информации и внедрил её без ведома и помимо воли 54 владельцев устройств под управлением ОС Android со следующими IMEI: №; №

Подсудимый Кузнецов В.В. в судебном заседании с предъявленным ему по ч. 2 ст.273, ч.1 ст.273 УК РФ обвинением согласился в полном объеме и подтвердил, что он выполнил все условия досудебного соглашения, оказал органу предварительного следствия активное содействие в раскрытии и расследовании преступления, просит рассмотреть дело в отношении него в порядке ст.317.7 УПК РФ, пояснил, что ходатайство о заключении досудебного соглашения о сотрудничестве им было заявлено добровольно, после консультации с защитником и в присутствии защитника, осознает последствия постановления приговора в особом порядке при заключении досудебного соглашения о сотрудничестве, в содеянном раскаивается, с чем также согласился защитник подсудимого – адвокат Демяшкин И.К.

Кроме того, подсудимый и его защитник заявили суду ходатайство о прекращении производства по делу на основании ст.25.1 Уголовно-процессуального кодекса Российской Федерации (далее – УПК РФ) с назначением подсудимому судебного штрафа.

Государственный обвинитель возразил на прекращение уголовного дела.

Выслушав участников процесса, исследовав материалы дела в объеме, необходимом для принятия решения по делу, суд приходит к следующему.

Уголовное дело в отношении Кузнецова В.В. поступило в суд с представлением заместителя прокурора Чувашской Республики и ходатайством подсудимого и его защитника о применении по уголовному делу особого порядка проведения судебного заседания и вынесения судебного решения, поскольку в ходе предварительного следствия с Кузнецовым В.В. заключено досудебное соглашение о сотрудничестве.

В судебном заседании государственный обвинитель Михайлов Ю.П. представление заместителя прокурора Чувашской Республики поддержал и подтвердил, что в ходе расследования уголовного дела Кузнецов В.В. активно способствовал расследованию совершенных им преступлений, дал подробные, правдивые показания по факту совершенных им преступления, сообщил данные лица, с которым совместно совершал преступление, согласился с обвинением, которое было ему предъявлено, не отказывался от показаний, которые были даны им на предварительном следствии после заключения досудебного соглашения. В результате сотрудничества с Кузнецовым В.В. следственным отделом УФСБ России по Чувашской Республике привлечен к уголовной ответственности соучастник преступления - ФИОЗ, уголовное дел по которому Новочебоксарским городским судом Чувашской Республики рассмотрено с постановлением обвинительного приговора, в связи с чем просит рассмотреть уголовное дело в особом порядке, поскольку подсудимый выполнил взятые на себя досудебным соглашением о сотрудничестве обязательства.

Выслушав участников процесса и исследовав материалы уголовного дела, касающиеся выполнения подсудимым Кузнецовым В.В. условий досудебного соглашения, суд приходит к выводу, что подсудимым выполнены все условия и обязательства, предусмотренные досудебным соглашением о сотрудничестве.

Как установлено судом, подсудимый активно способствовал расследованию совершенных им преступлений, дал подробные, правдивые показания по факту совершенных им преступлений, сообщил данные соучастника преступления, добровольно участвовал в следственных действиях, не возражал против обвинения, которое было ему предъявлено, не отказывался от показаний, которые были даны им на предварительном следствии после заключения досудебного соглашения. В результате сотрудничества с Кузнецовым В.В. следственным отделом УФСБ России по Чувашии привлечено к уголовной ответственности другое лицо – ФИОЗ, участвовавший в совершении преступления группой лиц по предварительному сговору с Кузнецовым В.В. (ч.2 ст. 273 УК РФ).

Обвинение, с которым согласился подсудимый в судебном заседании, является обоснованным и подтверждается доказательствами, собранными по делу. Ходатайство о заключении досудебного соглашения о сотрудничестве подсудимым было заявлено добровольно, после консультации с защитником и в присутствии защитника, Кузнецов В.В. осознает последствия постановления приговора в особом порядке при заключении досудебного соглашения о сотрудничестве.

При таких обстоятельствах суд приходит к выводу, подсудимым соблюдены все условия и выполнены все обстоятельства, предусмотренные заключенным с ним досудебным соглашением о сотрудничестве, в связи с чем уголовное дело в отношении него подлежит рассмотрению в порядке, установленной главой 40.1 УПК РФ.

Таким образом, суд признает Кузнецова В.В. виновным с совершении указанных в описательной части преступлений и квалифицирует его действия по совокупности преступлений:

- по ч.2 ст. 273 УК РФ - как распространение и использование компьютерных программ и компьютерной информации, заведомо предназначенных для несанкционированной модификации, копирования компьютерной информации и нейтрализации средств защиты компьютерной информации, совершенные группой лиц по предварительному сговору, из корыстной заинтересованности

- по ч.1 ст. 273 УК РФ - как распространение и использование компьютерных программы и компьютерной информации, заведомо предназначенных для несанкционированного блокирования, модификации, копирования компьютерной информации.

Вместе с тем, в соответствии со ст.76.2 УК РФ лицо, впервые совершившее преступление небольшой или средней тяжести, может быть освобождено судом от уголовной ответственности с назначением судебного штрафа в случае, если оно возместило ущерб или иным образом загладило причиненный преступлением вред.

Совершенные подсудимым Кузнецовым В.В. преступления относятся к категории небольшой и средней тяжести.

Подсудимый ранее не судим, совершил преступления впервые, трудоустроен, женат, имеет на иждивении двух малолетних детей, по месту жительства и работы характеризуется исключительно с положительной стороны.

Подсудимый свою вину в совершенных преступлениях признал полностью, раскаялся, заключил досудебное соглашение, требования которого исполнил в полном объеме, тяжких последствий по рассматриваемому делу судом не установлено.

В соответствии с ч.1 ст.25.1 УПК РФ суд, в случаях, предусмотренных статьей 76.2 УК РФ, вправе прекратить уголовное дело или уголовное преследование в отношении лица, подозреваемого или обвиняемого в совершении преступления небольшой или средней тяжести, если это лицо возместило ущерб или иным образом загладило причиненный преступлением вред, и назначить данному лицу меру уголовно-правового характера в виде судебного штрафа.

Учитывая изложенные выше обстоятельства, суд считает возможным освободить подсудимого на основании ст.76.2 УК РФ от уголовной ответственности за совершенное преступление и производство по делу прекратить на основании ст.25.1 УПК РФ с назначением подсудимому меры уголовно-правового характера в виде судебного штрафа.

При определении размера судебного штрафа, суд учитывает положения ст.104.5 УК РФ, а также нахождение подсудимого в период с 08.12.2016 по 13.01.2017 – под стражей, а с 13.01.2017 по 21.04.2017 - под домашним арестом.

Срок оплаты судебного штрафа суд определяет не позднее 60 дней со дня вступления настоящего постановления в законную силу.

Гражданский иск по делу не заявлен.

По делу имеются вещественные доказательства, вопрос о которых суд разрешает в соответствии с требованиями ч.3 ст.81 УПК РФ.

Руководствуясь ст. 76.2 УК РФ, ст. ст. 25.1, 254, 256, 317.6, 317.7 УПК РФ, суд

п о с т а н о в и л :

КУЗНЕЦОВА Валерия Валерьевича на основании ст.76.2 Уголовного кодекса Российской Федерации освободить от уголовной ответственности за совершение преступлений, предусмотренных ч.2 ст. 273, ч.1 ст. 273 Уголовного кодекса Российской Федерации и производство по уголовному делу прекратить на основании ст.25.1 Уголовно-процессуального кодекса Российской Федерации с назначением Кузнецову В.В. меры уголовно-правового характера в виде судебного штрафа в размере 30 000 (тридцать тысяч) рублей в доход государства. Штраф подлежит реальному исполнению.

Меру пресечения в виде подписки о невыезде и надлежащем поведении в отношении Кузнецова В.В. – отменить.

Срок уплаты судебного штрафа Кузнецову В.В. установить не позднее 60 дней со дня вступления настоящего постановления в законную силу.

Сведения об уплате судебного штрафа представить судебному приставу-исполнителю в течение 10 дней после истечения срока, установленного для уплаты судебного штрафа.

В случае неуплаты судебного штрафа в установленный судом срок судебный штраф отменяется и лицо привлекается к уголовной ответственности по соответствующей статье Особенной части настоящего Кодекса.

По вступлению постановления в законную силу вещественные доказательства по делу:

- <данные изъяты> – хранить в материалах дела;

- ноутбук «MacBook», Serial C02NQS96G085», накопитель информации «My Passport», S № (хранящиеся в УФСБ России по Чувашии), после уничтожения вредоносных программ специалистами УФСБ России по Чувашии, возвратить по принадлежности Кузнецову В.В.;

- ноутбук «MacBook Pro», Serial C1MMC0RTDTY3»; накопитель информации «Fujitsu», серийный номер « № »; накопитель информации с надписями «8GB», «SmartBuy»; накопитель информации «Transcend», серийный номер « № » (хранящиеся в УФСБ России по Чувашии), после уничтожения вредоносных программ специалистами УФСБ России по Чувашии, возвратить по принадлежности ФИО3;

- накопитель информации «Seagate Expansion», серийный номер « № », (собственность УФСБ России по Чувашии), содержащий в себе запись криптоконтейнера www с ноутбука ФИО3 «MacBook Pro» Serial №» - хранить в УФСБ России по Чувашии.

Постановление может быть обжаловано путем подачи апелляционных жалоб, представления через Новочебоксарский городской суд Чувашской Республики в Судебную коллегию по уголовным делам Верховного Суда Чувашской Республики в течение 10 (десяти) суток со дня вынесения данного постановления.

Председательствующий судья Д.Е. Ефимов