Валерий Комаров

ОПАСНАЯ ПРОФЕССИЯ

Будни работы в сфере информационных технологий

Валерий Комаров

Опасная профессия. Будни работы в сфере информационных технологий

«Издательские решения»

Комаров В.

Опасная профессия. Будни работы в сфере информационных технологий / В. Комаров — «Издательские решения»,

ISBN 978-5-00-678929-6

Издание адресовано широкому кругу читателей.В первой части вы найдете примеры жизненных ситуаций, приведших к возбуждению уголовных дел по компьютерным преступлениям. Во второй части рассмотрены примеры участия гражданина в следственных действиях (свидетель, потерпевший, понятой, обвиняемый и т.д.). Описаны следственные мероприятия и меры пресечения. В третьей части — примеры уголовного наказания за компьютерным преступлениям.Книга публикуется в авторской орфографии и пунктуации.

ISBN 978-5-00-678929-6

Содержание

Опасная профессия
Будни работы в сфере информационных технологий

Валерий Комаров

ISBN 978-5-0067-8929-6
Создано в интеллектуальной издательской системе Ridero

Предисловие

С правоохранительными и судебными органами мы сталкиваемся повсеместно и вне зависимости от нашего какого-то особого желания: нарушения правил дорожного движения, общественного порядка и т. д.

Не обязательно для этого быть хулиганом или аморальным типом.

Но, что очень странно, мало кто готов к прямому общению с представителями органов: не отличают осмотр от обыска, протокол от постановления, задержание от ареста, правонарушение от преступления….

На помощь приходит огромное количество статей, заметок, видеороликов с консультациями для водителей (общение с инспектором ДПС), охотникам (общение с инспектором охотнадзора или полиции), рыбакам (общение с инспектором рыбнадзор, ГИМС) и т. д.

Подобные ресурсы вполне могут дать общую базу по правилам общения с представителями надзорных органов, но отражают в основном вопросы административных правонарушений.

Юридические общедоступные ресурсы в большинстве разбирают отношения с правоохранительной системой в рамках экономических или бытовых уголовных преступлений, а вот выбор публичных ресурсов, посвященных ИТ отрасли и компьютерным преступлениям очень беден.

Работая специалистом по защите информации, а затем и руководителем подразделения информационной безопасности, я получил определенный жизненный опыт по взаимодействию с правоохранительной и судебной системой при расследованиях компьютерных преступлений, который уже заставлял задуматься о существовании определенного «правового нигилизма» среди работников ИТ сферы.

Но осознание глубины проблемы и масштабы последствий наступило во время ведения авторского блога «Рупор бумажной безопасности» и «Клуб любителей КИИ» в период с 2018 по 2022 года. Сначала просто собирая и изучая судебные дела по компьютерным правонарушениям и преступлениям, а затем и получая в личном общении от своих читателей информацию из первых рук. Накапливался опыт неформального общения с представителями стороны обвинения (оперативные работники, следователи, прокуроры, эксперты), с судьями и адвокатами.

Столкнувшись с десятками случаев обвинения специалистов информационных технологий, в том числе специалистов информационной безопасности (далее в книге – ИТ/ИБ специалисты), за поступки, которые они не осознавали в качестве незаконных и/или преступных.

С ситуациями, когда специалисты ИТ/ИБ своими необдуманными действиями в ходе оперативно-розыскных, следственных и судебных мероприятий, усугубляли свое положение и тяжесть наступивших последствий. Возникло понимание, что именно отсутствие должной правой грамотности среди ИТ/ИБ специалистов способствует формированию такой негативной практики, так родилась идея написания этой книги.

Можно сказать, что автором этой книги является жизнь. Моя роль была лишь обработать и систематизировать правоприменительную практику по компьютерным преступлениям – в основе книги сотни судебных решений, за каждым их них стоит жизнь и судьба человека.

Автор не ставит под сомнение справедливость вынесенных судебных решений, приведенных в книге, и не оценивает эффективность работы правоохранительных и судебных органов.

Цель книги – профилактика уголовных преступлений среди специалистов ИТ сферы.

Глава 1 «ДО»

Введение

Это не учебное пособие по уголовному праву или расследованию компьютерных преступлений и тем более не наставление по противодействию следствию или уходу от наказания за совершенные правонарушения и преступления.

Нет, автор резко отрицательно относится к любой незаконной деятельности и компьютерные преступления не являются исключением.

Книгу формируют три главы:

– Описание жизненных ситуаций, характерных для сферы информационных технологий, которые приводят к уголовной ответственности.

Рассматриваются все этапы карьерного роста специалиста ИТ: от обучения в школе до руководства крупной компанией.

– Описание жизненных ситуаций, характерных для участников расследования уголовных дел (свидетель, обвиняемый, подозреваемый, эксперт) по компьютерным преступлениям.

– Описание жизненных ситуаций после обвинительного решения суда по компьютерным преступлениям.

При написании книги использовались общедоступные источники в сети Интернет: официальные сайты судебных и правоохранительных органов, ГАС «Правосудие», справочно-правовые системы «Консультант» и «Гарант». Автор стремился иллюстрировать материал актуальными судебными решениями (с датами принятия за последние пять лет).

Издержки профессии

Судьба ИТ/ ИБ специалист ВСЕГДА отягощена по Уголовному кодексу (далее – УК РФ) в следствии:

– Образование, стаж, устойчивые навыки в информационных технологиях – обвиняемые всегда означает, что «предвидели, осознавали и имели возможность избежать наступление общественно опасных последствий» при совершении компьютерных преступлений. И чем больше учился и чем выше оценки, тем хуже перспективы с наказанием.

«*обладая достаточными знаниями в области пользования компьютерной техникой и имея практический опыт работы в сети Интернет*»

(Приговор от 20.04.2020 №1—40/2020)

«*В указанное время в указанном месте В. с целью реализации своего преступного умысла, обладая знаниями в области пользования компьютерной техникой, имея практический опыт работы с программным обеспечением, используя служебный персональный компьютер, осознавая общественную опасность своих действий, предвидя возможность модификации компьютерной информации, содержащейся в базе программы*»

(Постановление от 24.04.2023 №1—32/2023)

«*обладая познаниями в области компьютерной техники, имея навыки и опыт работы на персональных ЭВМ, пользования всемирной информационно-телекоммуникационной сетью „Интернет“ и различными Интернет-ресурсами*»

(Приговор от 27.02.2025 №1—150/2025)

«*имеющего высшее техническое образование по специальности „Информационные системы и технологии“, осуществляющего трудовую деятельность в должности ведущего технолога ПАО.., с целью выявления последствий воздействия вредоносной компьютерной программы на веб-сервис ООО…*»

(Приговор от 28.11.2024 №1—504/2024)

«*обладая достаточными познаниями и практическими навыками, полученными в процессе своей служебной деятельности на различных должностях, связанных с компьютерной информацией и работы с компьютерным обеспечением, преследуя корыстную цель, осознавая, что такими действиями им будут нарушены правила эксплуатации средств хранения и передачи охраняемой компьютерной информации*»

(Приговор от 31.01.2025 №1—23/2025)

И даже без диплома об образовании, достаточно быть «самоучкой»:

«*самостоятельно обучался в сети Интернет работе с компьютерными сетями и сетью Интернет, основам построения сайтов и работе социальных сетей. С. получал доход от сборки персональных компьютеров из комплектующих, бывших в употреблении, а также от продажи таких компьютеров. С. на достаточном уровне разбирается в компьютерной сфере, хорошо знает компьютерную терминологию. Помимо этого, С. имеет опыт в создании интернет-сайтов, в том числе онлайн-кинотеатров, с помощью которых зарабатывал денежные средства. Построение сайтов осуществлял на „движке“ „DLE“. Так же знает принцип работы анонимайзеров - VPN, имел опыт работы в „Даркнете“, а также является активным пользователем хакерских ресурсов и форумов.*»

(Приговор от 07.10.2020 №1—366/2020)

«*Свидетели ФИО73., ФИО74., ФИО75., ФИО76., ФИО77., ФИО78 подтвердили высокий уровень знаний Д.А. в области компьютерных технологий, его интерес к ним*»

(Апелляционное определение от 18.12.2023 №22—4622/2023)

– Организация рабочего места и процесса с ОБЯЗАТЕЛЬНЫМ использованием компьютера – обвиняемые всегда «совершали компьютерное преступление с использованием СЛУЖЕБНОГО положения».

«*Квалифицирующий признак „совершенное с использованием своего служебного положения“ нашел свое подтверждение в ходе судебного следствия, так как А. являясь работником.., действовал при помощи служебного компьютера, с использованием персонального логина и пароля, во исполнение своих должностных обязанностей, предусмотренных трудовым договором, должностной инструкцией*»

(Приговор от 13.02.2025 №1—41/2025)

Специалистов, обслуживающих контрольно-измерительные приборы (КИПовцев), это тоже касается.

«*Квалифицирующий признак «с использованием служебного положения» по каждому эпизоду подтвержден исследованными доказательствами о том, что Б. на дату совершения преступления являлся инженером КИПиА ООО «К..», в его должностные обязанности входили организация работы по технической эксплуатации и ремонту контрольно-измерительных приборов, средств связи, электронного оборудования и обеспечение их бесперебойной работы, и осуществлял работы по техническому обслуживанию, настройке систем измерения, в связи с чем обладал паролем для входа с уровнем доступа «Администратор» в автоматизированную систему измерения «С..», установленную на и автоматизированную систему измерения «Д..»*

(Приговор от 04.03.2024 №1—7/2024*)*

А исполнение рабочих обязанностей с должным усердием будет трактоваться

«*из иной личной заинтересованности, обусловленной ложно понимаемыми интересами службы в виде желания любыми способами реализовать служебные полномочия, с использованием служебного положения*»

(Приговор от 25.08.2023 №1—204/2023)

И даже, если компьютер личный, то достаточно использование в работе служебных учетных записей.

«*указанные действия Г. совершил, используя свое служебное положение, поскольку согласно трудовым договорам, локальным нормативным актам и должностной инструкции, он совершил вышеуказанное преступление в должности.., при выполнении своих служебных полномочий с использованием учетной записи и личного пароля для доступа в информационные системы, предоставленному ему работодателем для выполнения своих служебных обязанностей*»

(Приговор от 04.09.2024 №1—419/2024)

Иногда достаточно просто находится в момент преступлений на рабочем месте.

«*Исследованными доказательствами подтвержден квалифицирующий признак „с использованием своего служебного положения“. Из показаний А. установлено, что когда совершал неправомерные действия 13.04.2023, 18.04.2023, 22.06.2023, 10.07.2023, 18.08.2023, 08.09.2023, 19.09.2023, 21.09.2023 он находился на своем рабочем месте*»

(Приговор от 26.12.2024 №1—462/2024)

– Субъективность оценки действия/ бездействия и, используемых в работе программ и программно-аппаратных комплексов – обвинение будет строится на компьютерно-технических экспертизах, доверие к которым у судьи будет априори выше, чем к показаниям обвиняемого или к результатам экспертизы со стороны защиты.

Приводит это к снижению шансов на оправдательный приговор суда и к более серьезному (строгому) наказанию.

Для сравнения:

Неправомерный доступ к информации по ч.1 ст.272 УК РФ наказывается до 2 лет лишения свободы максимально, а при использовании служебного положения по ч.3 ст.272 УК РФ до 5 лет лишения свободы. Срок лишения свободы в 2,5 раза больше, просто за наличие трудовых отношений!

Или

Само по себе «нарушение правил эксплуатации» по ч.3 ст.274.1 УК РФ наказывается лишением свободы до 6 лет. Заметим, что нижней границы наказания не установлено, только верхняя.

А «нарушение правил эксплуатации с использованием служебного положения» наказывается уже по ч.4 ст.274.1 УК РФ и лишением свободы от трех до восьми лет. То есть, меньше трех лет суд не может назначить, а вот больше 6 лет может.

Аналогично и с формой наказания по ст.274.1 УК РФ.

«Обычное» нарушение по усмотрению суда может караться на выбор: принудительные работы, лишение свободы, а «служебное» нарушение только одна форма: лишение свободы.

Но это не повод для грусти и печали, подобные профессиональные риски характерны для множества других видов деятельности, причем с намного более высокими вероятностями получения наказания с реальным лишением свободы (врачи, энергетики, водители, машинисты и т.д.).

Школьный гений

Подростки старшего школьного возраста вполне уверенно владеют компьютерной техникой, обладают навыками программирования и не всегда оттачивают эти знания только на хакатонах и олимпиадах.

Уголовная ответственность за компьютерные преступления наступает с 16 лет.

«*вступил в преступный сговор с ранее знакомым ему Ю., <…> года рождения (в отношении которого 18 апреля 2024 г. вынесено постановление об отказе в возбуждении уголовного дела в связи с не достижением возраста уголовной ответственности)*»

(Приговор от 02.06.2025 №1—578/2025)

Виды наказаний, назначаемых судом несовершеннолетним, не сильно отличается от стандартных «взрослых» (штраф, лишение права заниматься определенной деятельностью, обязательные работы, исправительные работы, ограничение свободы, лишение свободы на определенный срок).

При назначении наказания несовершеннолетнему учитываются в том числе условия его жизни и воспитания, уровень психического развития, иные особенности личности, а также влияние на него старших по возрасту лиц.

Несовершеннолетний возраст учитывается судом как смягчающее обстоятельство.

«*В период с 2022 года до ДД. ММ. ГГГГ (точная дата и время следствием не установлены) несовершеннолетний А., ДД. ММ. ГГГГ года рождения, обладая достаточными специальными познаниями в области программирования и информационных сетевых технологий, находясь по месту своего жительства в <адрес>, секция 17 комната 3, имея в своем распоряжении сотовый телефон марки «iPhone 12 pro» (IMEI 1: N, IMEI 2: N), на котором установлен мессенджер «Telegram», посредствам которого он приобрел у неизвестного лица «Исходный код» вредоносной программы «Стиллер» для дальнейшего внесения в него изменений с целью продажи полученной программы и получения денежных средств. После чего при помощи вышеуказанного сотового телефона с возможностью выхода в глобальную информационно-телекоммуникационную сеть Интернет, скопировал на него с неустановленного сетевого ресурса компьютерную программу «Стиллер», которая несанкционированно, в скрытом от пользователя персонального компьютера режиме, осуществляет сбор и пересылку на канал программного продукта «Telegram» пользовательских данных (логинов и паролей), сохраненных в браузерах «Opera» и «Mozilla Firefox», в том числе в почтовых сервисах, социальных сетях, данные о банковских картах, информацию о криптокошельках, и, в соответствии с п. 2.6.5 «ГОСТ Р 50922—2006. Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие Приказом Ростехрегулирования от ДД. ММ. ГГГГ N-ст), является вредоносной программой. Полученную, таким образом, компьютерную программу «Стиллер» А. впоследствии перезаписал на «виртуальную память» сотового телефона под названием "<данные изъяты>" для последующего использования в личных целях.*

В силу ст. 61 УК РФ обстоятельствами, смягчающими наказание А. суд признает: полное признание своей вины и раскаяние в содеянном; активное способствование раскрытию и расследованию преступления, выраженное в даче показаний об обстоятельствах совершенного преступления на предварительном следствии при допросе, что способствовало установлению обстоятельств дела; условия жизни и воспитания; совершение преступления в несовершеннолетнем возрасте.»

(Приговор от 08.05.2024 №1—104/2024)

А еще есть приятный бонус: сокращение срока давности привлечения к уголовной ответственности в два раза.

«Приговором установлено, что два преступления, квалифицированные судом первой инстанции по ч. 1 ст. 273 УК РФ (в период Дата изъята и Дата изъята), были совершены Д.А. в несовершеннолетнем возрасте.

Данные преступления отнесены законом к категории средней тяжести (ч. 3 ст. 15 УК РФ).

Предусмотренный п. «б» ч. 1 ст. 78 УК РФ срок давности привлечения к уголовной ответственности за совершение указанных преступлений (шесть лет после совершения преступлений), согласно ст. 94 УК РФ подлежит сокращению наполовину и составляет для несовершеннолетнего осужденного три года.

С учетом вышеизложенных особенностей уголовной ответственности несовершеннолетних, срок давности по двум преступлениям, совершенным в период с Дата изъята года и с Дата изъята года, истек до постановления приговора. От следствия и суда в Д.А. не уклонялся, течение сроков давности не приостанавливалось.»

(Апелляционное определение от 18.12.2023 №22—4622/2023)

Есть важный нюанс с отсчетом возраста совершеннолетия, он наступает не в день рождения подростка.

«*Лицо считается достигшим возраста, с которого наступает уголовная ответственность, не в день рождения, а по его истечении, то есть с ноля часов следующих суток. При установлении возраста несовершеннолетнего днем его рождения считается последний день того года, который определен экспертами, а при установлении возраста, исчисляемого числом лет, суду следует исходить из предлагаемого экспертами минимального возраста такого лица.»*

«Постановление Пленума Верховного Суда РФ от 01.02.2011 №1

«О судебной практике применения законодательства, регламентирующего особенности уголовной ответственности и наказания несовершеннолетних»

И несовершеннолетнему надо очень постараться, чтобы попасть в следственный изолятор: заключение под стражу до судебного разбирательства может применяться к несовершеннолетнему лишь в качестве крайней меры и в течение кратчайшего периода времени. Такое возможно только в случаях продолжения хакерских атак в период запрета судом на использования сети в интернет и/или атак в отношении КИИ РФ (тяжкие преступления).

К сожалению, не каждый подросток правильно оценивает последствия от своих поступков, особенно когда государство дает второй шанс.

Так, молодой человек сначала попался на «лже-минировании учебного заведения» (телефонном терроризме) и вроде бы одумался. Увлекся компьютерными играми и программированием, но полученные знания направил по преступному пути. В итоге, судимость в несовершеннолетнем возрасте

«*Родители несовершеннолетнего ФИО1 видели, что их сын много времени проводил за компьютером, в том числе за компьютерными играми, и активно интересовался программированием, но интереса в его действиях не проявляли. Чем именно занимается их несовершеннолетний ребенок не интересовались. Знаниями в создании и распространении вредоносного программного обеспечения не обладают.*

Доводы адвоката ФИО8 о применении к ФИО1 принудительной меры воспитательного воздействия в виде передачи последнего под надзор родителей судом не принимаются во внимание, так как в ходе рассмотрения уголовного дела, с учетом данных, характеризующих личность несовершеннолетнего установлено отсутствие надлежащего воспитания и недостаточного контроля со стороны родителей несовершеннолетнего ФИО1, который ранее привлекался к уголовной ответственности за преступление против общественной безопасности.

Преступления по ч. 2 ст. 273 УК РФ несовершеннолетним ФИО1 были совершенны без физического или психического принуждения либо иных фактов, связанных с материальной, служебной или иной зависимостью несовершеннолетнего.

Учитывая характер и степень общественной опасности трех преступлений, личность несовершеннолетнего ФИО1, условия его жизни и воспитания, уровень психического развития, влияние на него старших по возрасту лиц, все смягчающие обстоятельства при отсутствии отягчающих, влияние назначенного наказания на исправление ФИО1 и на условия жизни его семьи суд считает, что применение принудительных мер воспитательного воздействия не целесообразным. Сфера, в которой совершены преступления несовершеннолетним ФИО1 не может контролироваться со стороны родителей, не имеющих соответствующих познаний в сфере компьютерной информации.

приговорил:

ФИО1 признать виновным в совершении трех преступлений, предусмотренных ч. 2 ст. 273 УК РФ, и назначить ему наказание с применением ч. 5 ст. 88 УК РФ:

– по ч. 2 ст. 273 УК РФ в виде ограничения свободы на срок 1 (один) год,

– по ч. 2 ст. 273 УК РФ в виде ограничения свободы на срок 1 (один) год,

– по ч. 2 ст. 273 УК РФ в виде ограничения свободы на срок 1 (один) год.

На основании ч. 2 ст. 69 УК РФ по совокупности преступлений путем частичного сложения наказаний назначить ФИО1окончательное наказание в виде ограничения свободы на срок 1 (один) год 6 (шесть) месяцев.»

(Приговор от 05.02.2024 №1—21/2024)

Учиться надо честно

Мы учимся в школе, учимся в ВУЗе, повышаем квалификацию и проходим переподготовку в учебных центрах по время рабочей деятельности, а еще сдаем множество тестов и экзаменов по охране труда, информационной безопасности и т. д.

Развитие информационных технологий привело к широкому применению компьютерной технике при сдаче экзаменов и тестировании.

И, к сожалению, если за списывание на очном экзамене или разнообразные студенческие шалости для гарантированного положительного решения преподавателя грозит максимум отчисление, то аналогичные действия в отношении электронного экзаменатора расцениваются государством как неправомерный доступ и модификация компьютерной информации.

Пример с электронным дневником в школе:

«*В соответствии с п. 4 Инструкции для реализации региональных мероприятий по сокращению и (или) отмене отчетности учителей» (направлена письмом Минобразнауки России № НТ-664/08 Общеобразовательного Профсоюза образования №269 от 16.05.2016) ведение электронного журнала и дневников входит в должностные обязанности учителя в рамках осуществляемой им контрольно-оценочной деятельности. На основании Приказа Минобрнауки России от 06.10.2009 г. №373), Письма Министерства образования и науки Российской Федерации от 15.02.2012 № А11—147/07 «О методических рекомендациях по внедрению систем ведения журналов успеваемости в электронном виде», Письма Минобрнауки России от 21.11.2014 № АК-3358/08 «Об уточнениях в методические рекомендации по внедрению систем ведения журналов успеваемости электронном виде» каждое образовательное учреждение разрабатывает Положение о ведении электронного журнала и электронного дневника, соответствии с которым, электронный дневник наряду с электронным журналом является государственным нормативно-финансовым документом.*

Поддержание информации, хранящейся в базе данных электронного дневника, в актуальном состоянии является обязательным для учителя. Категорически запрещается допускать учащихся к работе (только просмотр) электронного дневника. С помощью электронного дневника фиксируется и регламентируются этапы и уровень фактического усвоения учебных программ, хранение данных об успеваемости учащихся.

В соответствии с ч. 1 ст. 272 Уголовного кодекса Российской Федерации, взлом электронного дневника – это факт неправомерного доступа к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации»

(Решение №2А-403/2020 2А-403/2020~М-219/2020 М-219/2020 от 22 мая 2020 г. по делу №2А-403/2020).

Пример с ВУЗ.

«*Согласно материалам дела, студент ФГБОУ ВО «СамГУПС» (в настоящее время «ПривГУПС») С., незаконно получив доступ к логину и паролю, оформленным на бывшего сотрудника филиала университета, находясь в помещении указанного образовательного учреждения, при помощи служебного компьютера осуществил неправомерный доступ к содержимому программного обеспечения «1С Университет» и в аттестационной ведомости другого студента (его знакомой) исправил оценку «удовлетворительно» на оценку «хорошо», чем изменил свойства охраняемой законом компьютерной информации (достоверность), что повлекло ее модификацию.*

Признан виновным в совершении преступления, предусмотренного ч. 1 ст. 272 УК РФ (неправомерный доступ к охраняемой законом компьютерной информации, повлекший уничто-

жение, модификацию компьютерной информации), ему назначено наказание в виде 6 месяцев исправительных работ с удержанием 10% из его заработка ежемесячно в доход государства .»

(Приговор от 27.03.2025 №1—31/2025)

На работе при сдаче тестов для допуска на маршрут

«*Примененное П. на служебной ПЭВМ указанное нештатное программное обеспечение в виде исполняемых файлов, неправомерно модифицировало компьютерную информацию в программном комплексе «АСУТ», сформировав положительный результат тестирования в модуле «АС ГРАТ».*

Таким образом, П. предъявлено обвинение в совершении преступления, предусмотренного ч. 1 ст. 274.1 УК РФ – использование компьютерной программы, заведомо предназначенной для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, в том числе для модификации информации, содержащейся в ней.»

(Постановление от 07.04.2025 г. по делу №1—215/2025)

«*В конце дата (более точное время не установлено), но не позднее дата, П., осознавая необходимость прохождения в силу занимаемой должности процедуры тестирования знаний технико-распорядительных актов железнодорожных станций, без которой невозможно получение (продление) допуска к выезду на участок обслуживания, стремясь получить гарантированный положительный результат тестирования, решил воспользоваться сторонним нештатным программным обеспечением, предоставляющим тестируемому в модуле „АС ГРАТ“ программного комплекса „АСУТ“ ОАО „РЖД“ получение такого результата независимо от правильности ответов на вопросы теста.*»

(Постановление от 07.04.2025 г. по делу №1—217/2025)

Лабораторная работа к судимости привела

Знания и практические навыки, которые даются студентам и слушателям курсов повышения квалификации, могут быть применимы как с благой целью – повышение защищенности информации, так и с преступной целью. Часто учебные заведения даже специально акцентируют внимание, что обучают специалиста думать, как нарушитель (хакер). Пока практические навыки (выявление уязвимостей, пентест) отрабатываются на лабораторных стендах – нет проблем, попробовали применить вне стенда – судимость.

«*01.03.2023 в период с 12:18 часов до 13:17 часов (время московское) М.С., находясь у себя дома по адресу: <адрес>, умышленно, с целью проверки своих навыков по использованию программного обеспечения, зная, что ресурс Университета входит в информационно-телекоммуникационную сеть Университета, и относится к объектам критической информационной инфраструктуры, на мобильном телефоне марки <данные изъяты> IMEI1: N (IP-адрес N) открыл цифровое окно свободно распространяемого в сети <данные изъяты> программного обеспечения <данные изъяты>, предназначенного для проведения сетевого аудита безопасности информационных ресурсов, в том числе в открытых телекоммуникационных сетях, внес в него данные электронного адреса Университета <данные изъяты> (IP-адрес N) и запустил указанное программное обеспечение, то есть осуществил использование программного обеспечения <данные изъяты> с целью проверки наличия уязвимостей на сайте <данные изъяты>.*

Согласно заключению специалиста УФСБ России по <адрес> от 10.04.2023, неправомерные воздействия 01.03.2023 в период с 12:18:19 часов до 13:17:06 часов на информационный ресурс Университета представляли собой сканирование сервера (IP-адрес N) на выявление уязвимостей и проблем безопасности информационного ресурса с помощью программного обеспечения <данные изъяты>.

Подсудимый М. С. в судебном заседании фактические обстоятельства не оспаривал, показал, что, являясь студентом <данные изъяты> технического факультета <данные изъяты>, о программе <данные изъяты> он узнал при выполнении лабораторной работы в университете по предмету <данные изъяты>

(Приговор от 19.01.2024 по делу №1—21/2024)

Легкомысленность и небрежность на работе уголовно наказуема!

«1. Преступлением, совершенным по неосторожности, признается деяние, совершенное по легкомыслию или небрежности.

(«Уголовный кодекс Российской Федерации» от 13.06.1996 №63-ФЗ)

Большим заблуждением будет позиция, что для совершения преступления обязательно наличие прямого умысла. И думать, что, если следствие не доказало прямого преступного умысла, то никакого компьютерного преступления не произошло.

Собственно, нам об этом же и методические документы по защите информации говорят, так при оценке угроз должны рассматриваться «*Непреднамеренные, неосторожные или неквалифицированные действия персонала*»

(Методический документ. «Методика оценки угроз безопасности информации» (утв. ФСТЭК России 05.02.2021)

Уголовный кодекс различает между собой деяния по легкомыслию и по небрежности. Не следует их путать между собой.

«Не виноватая я, он сам пришёл!» (к/ф «Бриллиантовая рука»)

2. Преступление признается совершенным по легкомыслию, если лицо предвидело возможность наступления общественно опасных последствий своих действий (бездействия), но без достаточных к тому оснований самонадеянно рассчитывало на предотвращение этих последствий.»

(«Уголовный кодекс Российской Федерации» от 13.06.1996 №63-ФЗ)

Генеральная прокуратура дает такой пример:

«*программист, работающий в больнице, поставил полученную им по сетям программу без предварительной проверки ее на наличие в ней компьютерного вируса, в результате чего произошел отказ в работе систем жизнеобеспечения реанимационного отделения больницы* ».

В судебных документах это описывается таким образом:

«Ссылаясь на показания обвиняемых, отмечает, что они при проведении работ на сети осознавали общественную опасность своих действий в виде сбоев в ее функционировании, предвидели и сознательно допускали такие последствия. *Обращает внимание на осведомленность обвиняемых о функциональном назначении оборудования, обеспечивающего управленческие, технологические, производственные, финансово-экономические и (или) иные процессы в рамках выполнения функций (полномочий) и осуществления видов деятельности субъекта КИИ – ПАО «МТС» в области связи… находясь на рабочем месте по адресу: <адрес>, в период времени с 8—00 до 10—00 часов ДД. ММ. ГГГГ провели несанкционированные работы по демонтажу действующего сетевого оборудования в категорированном помещении (Автозал №1), что повлекло причинение вреда критической информационной инфраструктуре Российской Федерации, в виде прекращения функционирования сетей связи по технологии 2G//3G.*

(Постановление от 02.08.2022 №22—1382)

«Не откладывай на завтра то, что можешь отложить на послезавтра» (Марк Твен)

«3. Преступление признается совершенным по небрежности, если лицо не предвидело возможности наступления общественно опасных последствий своих действий (бездействия), хотя при необходимой внимательности и предусмотрительности должно было и могло предвидеть эти последствия.»

(«Уголовный кодекс Российской Федерации» от 13.06.1996 №63-ФЗ)

Как это выглядит на практике:

«не предвидя возможности наступления общественно опасных последствий в виде причинения вреда информационной системе « <данные изъяты>» являющейся объектом критической информационной инфраструктуры 3 категории значимости, хотя при необходимой внимательности и предусмотрительности должен был и мог предвидеть эти последствия, имея на то реальную возможность, не исполнил свои обязанности в качестве <данные изъяты> <данные изъяты>» по мониторингу (просмотру и анализу) записей регистрации (аудита) в журнале регистрации событий информационной панели АО « <данные изъяты>» как минимум два раза за весь период с 22 часов 25 минут ДД. ММ. ГГГГ по 12 часов 20 минут ДД. ММ. ГГГГ для всех событий, подлежащих регистрации и обеспечению своевременного выявления признаков инцидентов безопасности в информационных системах, а также реагированию на компьютерные инциденты, тем самым недобросовестно и небрежно относясь к своим должностным обязанностям.

Тем самым, установлено, что между наступившими последствиями в виде причинения вреда объекту критической информационной инфраструктуры 3 категории значимости и преступной небрежностью <данные изъяты> <данные изъяты>» ФИО2 имеется прямая причинно-следственная связь.

Признать ФИО2 виновным в совершении преступления, предусмотренного ч.3 ст. 274.1 УК РФ, и назначить ему наказание в виде лишения свободы на срок 1 год с лишением права заниматься деятельностью, связанной с доступом к критической информационной инфраструктуре Российской Федерации на срок 2 года.»

(Приговор от 23.08.2024 №1—1309/2024)

Даже, если центр мониторинга событий информационной безопасности (SOC) не оказывает услуг субъектам КИИ, то его работники «первой линии» имеют шансы попасть под уголовную ответственность по ст.274 УК РФ (не путать с ст.274.1 УК РФ), если в результате их преступной небрежности пропущена компьютерная атака и ущерб при ликвидации ее последствий превысил 1 миллион рублей, что при современных ценах на компьютерную технику и программное обеспечение не такая уж и редкость. Даже если информационная инфраструктура не пострадала, то в ущерб традиционно засчитывают время простоя организации и стоимость трудозатрат (зарплаты) на дополнительные проверки и контрольные мероприятия.

А, если центр мониторинга событий информационной безопасности (SOC) развернут на базе бюджетного или казенного учреждения, то еще и по ст. 293 УК РФ «Халатность».

«С.Т.В., в нарушение приведенных выше нормативно-правовых актов, относясь к службе недобросовестно и небрежно, не предвидя наступления общественно опасных последствий в виде …, хотя при необходимой внимательности и предусмотрительности должна была и могла предвидеть эти последствия, в период с 11.33 часов до 12.31 часов ДД. ММ. ГГГГ безосновательно отвлекалась от исполнения своих должностных обязанностей, не обеспечила постоянный просмотр и контроль за мониторами …. Однако С. Т. В., проявляя небрежное отношение к службе, имея при этом достаточные опыт работы и профессиональную подготовку, обладая необходимыми знаниями в области работы оператора группы надзора отдела безопасности, зная алгоритм проведения необходимых мероприятий …, не находясь в беспомощном, болезненном состоянии, будучи трудоспособной, при наличии реальной возможности надлежащего исполнения своих обязанностей, не пресекла действия …..

При рассмотрении дела установлено, что С. Т. В. в период, относящийся.. неоднократно отвлекалась от несения службы – вставала с кресла, отходила от мониторов, отдалялась от них, на мониторы не смотрела.

Судом установлено, что перед заступлением в дежурную смену ДД. ММ. ГГГГ на качество изображения камер, на иные технические неполадки С. Т. В. не указывала, по состоянию здоровья нести службу могла.

Признать С. Т. В. виновной в совершении преступления, предусмотренного ч. 2 ст. 293 УК РФ, и назначить ей наказание в виде 1 (одного) года 6 (шести) месяцев лишения свободы.»

(Приговор от 18.11.2024 по делу №1—132/2024)

Думай, что отправляешь

Иногда даже опытные и квалифицированные ИТ специалисты устраивают эксперименты над системами защиты информации своих прежних работодателей, стоимость подобного эксперимента для них – уголовная ответственность.

«С., имеющего высшее техническое образование по специальности «Информационные системы и технологии», осуществляющего трудовую деятельность в должности ведущего технолога Информационно-технологического кластера ПАО «МТС-Банк», с целью выявления последствий воздействия вредоносной компьютерной программы на веб-сервис ООО «Башкирэнерго», где он ранее осуществлял трудовую деятельность, возник преступный умысел, направленный на распространение вредоносной компьютерной программы, заведомо предназначенной для несанкционированного блокирования компьютерной информации.

Во исполнение указанного умысла, направленного на распространение вредоносной компьютерной программы, С., находясь по месту своего проживания по адресу: <адрес>, используя принадлежащий ему персональный компьютер с накопителем информации «SAMSUNG» с серийным номером № (mac-адрес шлюза №), имеющий выход в информационно-телекоммуникационную сеть «Интернет» (по тексту – сеть «Интернет), с IP-адресом №, предоставленным АО „ЭР-Телеком Холдинг“, достоверно зная, что вредоносный архивный файл « <данные изъяты>» предназначен для несанкционированного блокирования компьютерной информации, скачал его с сайта « <данные изъяты>» по ссылке « <данные изъяты>».

Реализуя преступный умысел, направленный на распространение вредоносной компьютерной программы, С., находясь по месту своего проживания по адресу: <адрес>, действуя умышленно в нарушение Федерального закона от 27 июля 2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации», осознавая, что вредоносный архивный файл « <данные изъяты>» предназначен для несанкционированного блокирования компьютерной информации, используя принадлежащий ему персональный компьютер, с накопителем информации «SAMSUNG» с серийным номером № (mac-адрес шлюза №), имеющий выход в сеть «Интернет», с IP-адресом №, предоставленным АО «ЭР-Телеком Холдинг», разместил на веб-сервисе ООО «Башкирэнерго», имеющим возможность удаленного обмена файлами, вредоносный архивный файл « <данные изъяты>», сформированный таким образом, что при попытке программы-архиватора извлечь содержащиеся в нем данные, происходит перегрузка вычислительных мощностей системы без предварительного информирования пользователя о запуске и получении его согласия, что может спровоцировать блокирование или существенное замедление работы компьютера за счет заполнения оперативной памяти и чрезмерной нагрузки на центральный процессор.

С. признать виновным в совершении преступления, предусмотренного ч.1 ст.273 УК РФ, и назначить наказание в виде ограничения свободы сроком на ДВА ГОДА».

(Приговор от 28.11.2024 №1—504/2024)

Под аналогичные обвинения можно попасть: при пересылке в мессенджерах, почте, ссылки на облачный ресурс и т.д., файлов с вредоносным программным обеспечением, полученным ранее при исполнении рабочих обязанностей в фишинговом письме, выявленном антивирусной системой и т. д.

Переслали файл с вредоносным программным обеспечением (ВПО) на форум исследователей, скинули в телеграм-канал студентов ВУЗа – для отправителя риски уголовного преследования серьезно возросли.

Опасные связи

В России серьезно развит выставочный бизнес – проводятся конференции, форумы и выставки достижений в ИТ и ИБ индустрии. Сотни отечественных компаний и предпринимателей выставляет свою высокотехнологичную продукция на стендах участников.

Ну какие здесь опасности и компьютерные преступления?

Вот одна российская ведущая компания, разработчик технологий для организации и мониторинга цифрового телевидения, тоже испытывала подобные иллюзии.

Компания развернула собственный стенд, демонстрирующий возможности продукции. В составе стенда был Wi-Fi роутер. При настройке и подготовке стенда к выставке не были реализованы меры защиты от несанкционированного доступа – стояли пароли по умолчанию и т. д.

Результат не самый тяжелый, можно сказать – легко отделались.

Всего то штраф и конфискация оборудования. Всего-лишь за подмену имени Wi-Fi сети стенда на выставке.

«24 апреля 2024 года в 12 час. 40 мин. по адресу: адрес, на территории адрес, во время проведения выставки «Связь-2024», с количеством участников до 685 экспонентов, в нарушении требований Федерального закона №144-ФЗ от 25.07.2002 года «О противодействии экстремисткой деятельности», а также Федеральный закон от 19.05.1995 года №80-ФЗ «Об увековечивании Победы советского народа в Великой отечественной войне 1941—1945 г.г.», распоряжения Министерства юстиции Российской Федерации от 17.01.2024 №38-р «О включении организации, ее атрибутики и символики в перечень организаций, указанных в частях третьей и четвертой статьи 6 Федерального закона «Об увековечивании Победы советского народа в Великой отечественной войне 1941—1945 годов», а также атрибутики и символики этих организаций» … допустило, с целью пропаганды, лозунга украинских националистов, публичное распространение лозунга: «SLAVA UKRAINE» и «SLAVA UKRAINE_5G», путем демонстрации названия Wi-Fi сети и отображения указанного лозунга при подключении к интернет сети неограниченного числа пользователей в пределах доступа Wi-Fi сигнала

постановлением о представлении результатов оперативно-розыскной деятельности заместителя начальника управления «П» 4 Службы ФСБ России от 24.04.2024г., из которого усматривается, что в результате проведенных оперативно-розыскных мероприятий получены материалы, свидетельствующие о совершении неустановленным лицом, либо группой лиц из числа сотрудников… административного правонарушения, в частности 24.04.2024г. на территории адрес проводилось выставочное мероприятие «Связь-2024», в ходе которого неустановленные лица из числа сотрудников… установили wi-fi роутер, на котором были установлены точки доступа с названиями «SLAVA UKRAINE» и «SLAVA UKRAINE_5G». Данное обстоятельство было зафиксировано сотрудниками Управления безопасности адрес путем использования технических средств и составлен соответствующий акт, в связи с чем, постановил направить в ОМВД России по пресненскому району адрес справку о проведении оперативно-розыскного мероприятия «наведение справок» №8/П/6/1535 от 24.04.2024г.;

актом от 24.04.2024 года о выявлении на стенде 23С40 компании …, работающего wi-fi -роутера, марки ASUS, серийный номер F81OR4001582, на котором включена точка доступа, с названием «SLAVA UKRAINE» и «SLAVA UKRAINE_5G», в котором также содержатся сведения, данные представителем… о том, что роутер был взят уже настроенный из офиса компании, самостоятельно его не настраивали, роутер не изымался, настройки его сброшены, с фотоматериалом;

договором №д/181—2300367 на участие в выставке «Связь-2024» от 16.11.2023 года, заключенный между адрес и… с 23.04.2024 по 26.04.2024 г. с 08.00—20.00 час.;»

(Постановление от 20.06.2024 № №5—322/24)

Иногда, особенно в молодых неокрепших умах, возникают шальные мысли «просто пошутить». Вот только последствия такого чувства юмора – арест, штрафы, потерянная техника и испорченная репутация.

«06 марта 2024 года в 10 ч. 00 мин. по адресу: адрес оперуполномоченными УПЭ ГУ МВД России по адрес выявлен факт массовой демонстрации в названии Wi-Fi сети SSID с целью пропаганды лозунга фио!» (Slava Ukraine!) неограниченному кругу лиц из числа пользователей в пределах доступа Wi-Fi сигнала идеологии Организации украинских националистов, в нарушение требований ФЗ №114-ФЗ от 25.07.2002 года «О противодействии экстремистской деятельности», а также ФЗ №80-ФЗ от 19.05:1995 «Об увековечивании Победы, советского народа в Великой отечественной войне 1941—1945 г.г.», распоряжения Министерства юстиции Российской Федерации от 17.01.2024 №29-р «О включении организации, ее атрибутики и символики в перечень организаций, указанных в частях третьей и четвертой статьи 6 Федерального закона „Об увековечивании Победы советского народа в Великой отечественной войне 1941—1945 годов“, а также атрибутики и символики этих организаций».

06.03.2024 г. в период времени с 10 часов 09 минут до 10 часов 26 минут в ходе осмотра комнаты В218 по адресу: адрес, на столе был выявлен персональный компьютер и ноутбук, а под столом на полу Wi-Fi роутер TP-Link, модель TI.-WR841N (RU), при подключении к Wi-Fi сети на мониторе в окне выбора сети отображается название в виде лозунга «Slava Ukraine!» (фио!).

Установлено, что пользователем персонального компьютера, ноутбука, Wi-Fi роутера TP-Link, модель TL-WR841N (RU) является Т., …паспортные данные, который находясь по адресу: адрес, осознавая доступность наименования Wi-Fi сети для неограниченного числа пользователей в пределах доступа Wi-Fi сигнала, изменил название Wi-Fi сети с предустановленного на название в виде лозунга «Slava Ukraine!» (фио!), с целью пропаганды лозунга украинских националистов.»

(Постановление от 07.03.2024 №5—141\24)

Защищайте свои средства беспроводного доступа, не используйте провокационные наименования сетей, устройств в сети, логины и адреса электронной почты, никнеймы и аккаунты в соцсетях/мессенджерах.

И помните о рисках при сдаче жилья в аренду. Если квартиросъемщик совершит компьютерное преступление, то провайдер сообщит оперативным работникам о лице, заключившим договор на услуги интернет. Минимум получением статуса «свидетель» грозит и это не самый плохой вариант развития событий.

*«Свидетель Б. П. С. показал, что в ** году он приобрел жилье по адресу: …, …, …, которое арендовала впоследствии семья Ч., на момент ** года она также проживала по вышеуказанному адресу. В квартире имелся интернет-провайдер АО "<данные изъяты>», договор по которому заключен на его имя. Таким образом, по указанному адресу имелся доступ в сеть "<данные изъяты>" посредством использования указанного провайдера»*

(Приговор от 16.05.2025 №1—208/2025)

Друг ты мне или нет. Или как взаимовыручка до судимости довела

Существуют мнение, что специалисты ИТ это люди, избегающие социума и предпочитающие проводить время исключительно с «железками», но ничто человеческое им не чуждо и крепкие личные рабочие отношения во многом определяют совершаемые поступки.

«*Подсудимым Ч. А. ВА. и С. И. ИА., учитывая установленные по делу фактические обстоятельства, связанные с доступом к объекту КИИ РФ в силу должностного положения, занимаемого в ООО «Шахта Листвяжная», мотивы С. И. ИА. в виде желания угодить инспекторам Ростехнадзора В. С. АА. и лицу N 2, Ч.А.ВА. чувства ложно понятого товарищества, и как следствие возможности избежать по отношению к ним неблагоприятных последствий, характер их действий, на основании ч. 1 ст. 47 УК РФ суд приводят суд к убеждению о необходимости значить им дополнительное наказание в виде лишения права заниматься деятельностью, связанной с автоматизацией технологических процессов и информационных технологий.*

Признать Ч. А. ВА. виновным в совершении преступления, предусмотренного ч. 4 ст. 274.1 УК РФ и назначить ему наказание в виде лишения свободы на срок 4 года, с лишением права заниматься деятельностью, связанной с автоматизацией технологических процессов и информационных технологий на срок 1 год.»

(Приговор от 31.01.2024 по делу №1—69/2024)

«*После регистрации сим-карты банк отказал в кредитном лимите на карту, они сообщили ему, после чего он покинул офис продаж, оставив ей данную сим-кару с абонентским номером N, при этом он разрешил ей пользоваться, пояснив, что он проживает в другом регионе и пользоваться номером не собирается. Она взяла данную сим-карту абонентского номера N для личного пользования, после чего передала данную сим-карту своему малолетнему сыну. После пользования какое-то время данной сим-картой на этот абонентский номер начали поступать спам-звонки и доставать семью, а так как сотовый телефон с сим-картой абонентского номера находился у малолетнего ребенка, она решила, что нужно переоформить данный абонентский номер на себя. Вышеуказанные противоправные действия она совершила по личной просьбе своей коллеги по работе Свидетель N 2, так как она лежала в больнице, и она хотела ей помочь. При этом она также понимала, что изменения в действующем абонентском договоре она могла совершить только с согласия собственника данного абонентского номера Свидетель N 1, который должен был находиться непосредственно в офисе продаж с документом, удостоверяющим личность (паспортом), либо же зайти в любой офис продаж „Билайн“, оставить свою доверенность на изменение данных. Она понимает, что неправомерное изменение данных клиентов в информационной системе ПАО „ВымпелКом“ подпадает под действие ч. 4 ст. 274.1 УК РФ „неправомерное воздействие на критическую инфраструктуру Российской Федерации с использованием своего служебного положения“ и была с этим ознакомлена в ПАО „Вымпелком“ при ее трудоустройстве. По данному факту вину свою полностью признает, в содеянном раскаивается*»

(Приговор от 11.04.2025 по делу №1—26/2025)

«*Ему знаком Б. Ю. ВА., он познакомился с ним в 2010 году, тот в тот момент работал также, как и он, в РЭО ОГИБДД У МВД России по <адрес>, они с ним были в дружеских отношениях, виделись в основном на работе, но хорошо общались.*

Периодически он созванивался с Б. Ю. ВА., просто общался. В 2021 году он стал обращаться к Б. Ю. ВА. с просьбами о предоставлении информации из базы данных ГИБДД.

Б.Ю.ВА. он денег за предоставляемую им информацию из баз данных ГИБДД не давал, подарков не дарил, услуг не оказывал, всю информацию из баз данных ГИБДД зафиксированную в их с ним переписке в мессенджере «Whats app» тот предоставлял ему по дружбе.

Б.Ю.ВА. действовал не в связи с исполнением служебных обязанностей, а из личной заинтересованности – по просьбе Свидетель N 1. Обращение к подсудимому Б. Ю. ВА. свидетеля Свидетель N 1 было неофициальным, следовательно, предоставление ему конфиденциальной информации было незаконным.

Б.Ю.ВА. признать виновным в совершении шести преступлений, предусмотренных частью 3 статьи 272 УК РФ, и назначить ему наказание за каждое из шести преступлений в виде штрафа в размере 80000 (восемьдесят тысяч) рублей, с лишением права заниматься деятельностью, связанной с обработкой, хранением и распоряжением охраняемой законом информацией, на срок 1 год.»

(Приговор от 15.10.2024 по делу №1—111/2024)

Это не твоя почта, если уволился

«Это не твой зуб. Это даже не мой зуб. Это ихний зуб» (к/ф «Не бойся, я с тобой!»)

Достаточно распространенная ситуация, когда по рабочей необходимости в организации создается электронный почтовый ящик, файловое хранилище на публичных ресурсах, с использованием личной sim-карты специалиста ИТ/ИБ или создаются веб-ресурсы (сайты, каналы и группы в мессенджерах, чат-боты, страницы организаций в соцсетях), привязанные к его личным аккаунтам или электронной почте.

Определенные проблемы возникают при увольнении специалиста. Но мы не о технологических проблемах организации, в рамках данной книги нас интересует исключительно вопрос потенциальных уголовных последствий для уволенного работника, чей личный ресурс используется в служебных целях организации.

Что будет, если такой специалист зайдет после увольнения на такой ресурс, владельцем которого он формально является?

Что будет, если он, как формальный владелец, его заблокирует или удалит информацию с него?

«*Эта электронная почта …..*b@mail.ru *была создана для отдела ветеринарного контроля, заместителем начальника которого ранее являлась А.*

С ДД. ММ. ГГГГ по ДД. ММ. ГГГГ А. работала заместителем начальником отдела ветеринарного контроля. В настоящее время она там не работает.

Указанная электронная почта была несанкционированно привязана к телефону 89……

Главным лицом, ответственным за администрирование данной электронной почты ранее являлась А.

После того как заблокировали электронный почтовый ящик, вся информация, которая там имелась, была утеряна. ФИО6 (Свидетель №1) пытался ее восстановить, ему приходили сообщения со службы поддержки, что даже если и удастся его восстановить сам почтовый ящик, то информация, хранившаяся на нем, не восстановится. Поэтому прекратили попытки восстановить почтовый ящик и просто стали пользоваться другой электронной почтой.

Вред имуществу Управления не причинен. Вместе с тем, нанесен непоправимый вред деловой репутации Управления как федерального органа исполнительной власти, поскольку неправомерное изменение пароля к учетной записи повлекло блокирование и аннулирование электронной почты Управления под логином «…b@mail.ru». Взаимосвязь между Управлением и контролируемыми лицами на длительное время прервалась, пока доводилась до сведения всем необходимая информация об изменении логина электронной почты, чем были нарушены права граждан, закрепленные за ними Конституцией РФ, на обращение в государственные органы. В данный период времени в адрес Управления поступало значительное количество телефонных звонков с возмущениями граждан об отсутствии электронной связи для направления обращений и заявлений.

Непоправимый вред Управлению как федеральному органу нанесен и утратой служебной необходимой информации, накопленной за годы деятельности.

Кроме того, электронная почта была установлена на рабочем компьютере Управления для использования специалистами в своей служебной деятельности, ограничивающей законодательством доступ к этой переписке, имеющей конфиденциальные, служебные сведения и персональные данные.

Следовательно, изменение пароля и привязки номера телефона аккаунта электронной почты, а также удаление секретного слова, являющегося способом защиты компьютерной информации, также являются модификацией и блокированием компьютерной информации.

Суд квалифицирует деяние А. по ч. 1 ст. 272 УК РФ – неправомерный доступ к охраняемой законом компьютерной информации, повлекший копирование, модификацию и блокирование компьютерной информации.»

(Приговор от 21.06.2024 №1—76/2024).

Айтишник, помоги с регистрацией личного кабинета

Частенько мы сталкиваемся с просьбами коллег, родственников и знакомых о помощи при совершении каких-либо действий на интернет порталах или в информационных системах в целях регистрации пользователя. А в таких случаях нам становятся известны учетные данные (логин, пароль и т.д.), что уже нехорошо.

Но хуже, когда нас просят еще и совершать какие-либо действия в системах под этой учетной записью:

– коллега попросил поставить отметку о согласовании в системе электронного документооборота, что бы не задерживать подписание важного документа в свое отсутствие;

– родственники попросили внести данные в декларации налоговой, ЖКХ и т. д.

Варианты жизненных ситуаций могут быть разнообразными.

Самое печальное, если вы не сможете подтвердить правомочность своего доступа под чужой «учеткой», то есть – что вы действовали по поручению и в интересах владельца учетной записи.

«*М. совершил неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло копирование компьютерной информации, при следующих обстоятельствах.*

Так он 26.04.2024, находясь в офисе ООО «Расчетно-информационный центр ЖКХ», расположенного по адресу: <…>, работая в должности бухгалтера, имея в пользовании служебный компьютер, обеспечивающий соединение с сетью «Интернет», с использованием N, обладая навыками и знаниями работы в сферах компьютерных и информационных технологий, включая навыки работы с сайтом https://www.nalog.gov.ru, имея в распоряжении учетно-регистрационные данные в виде логина и пароля личного кабинета налогоплательщика – физического лица С. В. С., которые последний сообщил ему (М.) ранее, умышленно, незаконно, осуществил неправомерный доступ к охраняемой законом информации, и ее копирование, содержащийся на сайте https://www.nalog.gov.ru, без ведома и против воли С. В. С., осуществив вход в «личный кабинет» последнего, не осведомленного о его (М.) преступных намерениях, путем ввода имеющегося у него (М.), логина и пароля. Затем М., действуя в продолжение своего преступного умысла, в нарушение требований Федерального закона от 27.06.2003 №152-ФЗ «О персональных данных» осуществил формирование справок по форме 2-НДФЛ в формате PDF: NN 8016, 12, 7136, 6680028, которые без ведома и против воли С. В. С., действуя умышленно, осознавая противоправный характер своих действий, скопировал с указанного сайта на служебный компьютер и ознакомился с охраняемой законом информацией, содержащейся в отмеченных справках.

Подсудимый М. в судебном заседании свою вину в совершении указанного преступления при обстоятельствах, изложенных судом выше, фактически не признал, при этом пояснил, что его просил С. В. С. открыть для него личный кабинет в налоговой в 2021 году. Пароль и логин были у М., при этом считает, что С. В. С. не запрещал заходить в личный кабинет в дальнейшем. Когда заходил 26.04.2024 на сайт, то руководствовался разрешением С. В. С., которое получил зимой при встрече в квартире, где проживали его дочь и потерпевший, поэтому не согласен с тем, что в его действиях есть противоправное деяние. Также показал, что декларации скопировались на компьютер, так как программа на указанном сайте налоговой службы настроена таким образом, что просмотреть полное содержание справки 2-НДФЛ возможно только после ее формирования и скачивания на компьютер, с которого просматриваются данные, то есть справки автоматически копируются на компьютер.

Признать М. виновным в совершении преступления, предусмотренного ч. 1 ст. 272 УК РФ»

(Приговор от 19.02.2025 №1—102/2025)

Не надо проверять систему защиты информации, тем более чужую

Иногда странные желания посещают голову специалистов ИТ, в народе такое обычно называют «бес попутал». Кто-то проверяет зажигалкой датчики противопожарной сигнализации, а кто-то сознательно отправляет вредоносное программное обеспечение в чужую организацию – просто посмотреть, как сработает антивирусная система защиты информации в ней.

И последствий то никаких для информации, все штатно срабатывает и ничего страшного не происходит.

Не понимают такие экспериментаторы, что сам факт отправки вредоносного программного обеспечения подлежит уголовному преследованию. И для получения уголовного наказания наступление каких-либо последствий по ст.273 УК РФ не требуется.

«*лицом с использованием IP-адреса № была загружена вредоносная компьютерная программа с именем файла « <данные изъяты>», а вредоносная компьютерная программа была обнаружена в автоматическом режиме средствами системой антивирусной защиты ООО «Башкирэнерго» и удалена. По результатам анализа журналов Веб-сервера определен IP адрес, с которого выполнялась отправка файла, и адрес электронной почты, указанный в обращении. К тяжким последствиям, либо созданию угроз их наступления не привело, так как штатно сработала система антивирусной защиты.*

Подсудимый А. вину в совершении инкриминированного ему преступления признал полностью и показал, что он году он работал в «МТС – Банк» на должности, которая подразумевала разработку и проектирование информационной системы. Решил провести эксперимент, с точки зрения клиента, как потребителя системы посмотреть, как отреагирует система ООО «Башкирэнерго», если он загрузит зараженный документ. Тогда он скачал из открытых источников готовый вредоносный архив, который определялся антивирусом как вредоносный и находясь дома по адресу: <адрес>, со своего компьютера осуществил загрузку этого самого архива в сервис ООО «Башкирэнерго» по приему документов. После этого к нему пришли сотрудники ФСБ, он содействовал следствию по установлению обстоятельств, все рассказал и показал, в содеянном раскаивается.

Вместе с тем, состав преступления, предусмотренный ч.1 ст.273 УК РФ, является формальным и не требует наступления тех или иных последствий. То есть состав преступления считается оконченным с момента совершения любого из указанных в статье действий

Учитывая совершение подсудимым преступления с прямым умыслом, принимая во внимание последовательность и целенаправленность действий при совершении преступления, обстоятельства его совершения, суд не находит оснований для изменения категории преступления в отношении подсудимого на менее тяжкую в соответствии с ч.6 ст.15 УК РФ.»

(Приговор от 28.11.2024 №1—504/2024)

Снявши голову, по волосам не плачут

После увольнения может возникнуть соблазн подключится к информационным системам бывшего работодателя с использованием ранее выданных учетных данных (пароль и логин). В нормальной ситуации, учетные записи уволенных работников должны блокироваться, но в силу безалаберности ИТ/ИБ подразделений, либо по техническим причинам (сбои), возможность доступа сохраняется.

С точки зрения законодательства, это – неправомерный доступ к защищаемой информации.

Как только получили запись в трудовую книжку об увольнении – забудьте о доступе к информации в этой организации.

«*Т.., имевший прямой доступ к информационной системе «Р…» ПАО «С…», умышлено, осознавая противоправный характер своих действий и предвидя возможность наступления последствий в виде незаконного сбора сведений, составляющих <данные изъяты>, воспользовался, известными ему ранее, учетной записью «timu…» и паролем..*

Заключением по служебной проверке ПАО «С….», согласно которому у Т.. после расторжения договора не был ограничен доступ к информационной системе «Р» из-за технической ошибки, в связи с чем он продолжил пользоваться рабочим доступом к системе…»

(Приговор от 29.03.2022 №1—341/2021)

Средство защиты информации или вредоносное программное обеспечение?

Казалось бы, какая опасность может угрожать ИТ/ИБ специалисту при установке по указанию руководителя специализированного программного обеспечения? К тому же, производитель данного программного обеспечения заявил его, как средство защиты информации? Ан, нет. Все сложно.

Обычная бытовая ситуация: сложные взаимоотношения между коммерческими компаниями, руководитель одной из компаний подозревает нескольких своих подчиненных в «работе на конкурентов», ставит задачу системному администратору установить на их служебные ноутбуки систему контроля утечек информации (DLP). Системный администратор выполнил задачу и оказался на скамье подсудимых.

«*Фио лично после увольнения Фио1 вызвал его и дал устное распоряжение найти компьютерные программы, которые могли бы контролировать действия сотрудников за их рабочими компьютерами и сказал, что слышал от кого-то о подобных программах. Он по поручению Фио провел анализ рынка таких лицензионных программ, подобрал две лицензионные легальные программы «Лан агент стандарт» и «Секьюрити Куратор» от известных российских производителей, которые имели представительства в каждом регионе страны, участвовали в выставках, их программы признавались лучшими компетентными рейтингами, отмечались в профессиональных изданиях, были известны на рынке и были правомочно введены в гражданский оборот, ими пользовались многие компании по стране. Программа «Лан агент стандарт» с 2009 года зарегистрирована Федеральной службой по интеллектуальной собственности, патентам и товарным знакам*.

Согласно официальным сведениям, представленным на веб-сайтах производителей программного обеспечения «Security Curator» и «LanAgent», Security Curator – это система обеспечения информационной безопасности нового поколения, объединяющая в себе возможность наблюдения за деятельностью сотрудников, контроля их действий и блокировки потенциально опасных путей утечки информации

Антивирусная защита, установленная на компьютерах пользователей сети сотрудников офиса, на данные части программы «Лан Агент» и «Секьюрити Куратор» не среагировала, что говорит о том, что программы не были вредоносными. В целом обе программы помогают руководству предприятия обеспечить эффективность работы сотрудников, обеспечивают его информацией, предупреждают утечку информации с компьютеров, принадлежащих компании.».

«*В ходе служебной проверки, а впоследствии в ходе проведения судебной компьютерной экспертизы на компьютерах выявлены активированные и установленные компьютерные программы, заведомо предназначенные для несанкционированного копирования компьютерной информации принадлежащей „наименование организации“ и охраняемой законом, являющейся информацией ограниченного доступа, поскольку руководители не давали распоряжения на установку, активацию и использование данных программ, не были поставлены в известность об их активации, установке и использовании, о чем категорично утверждали как в ходе предварительного расследования, так и в ходе судебного разбирательства, пользователи компьютеров также не были осведомлены об активации, установке и функционировании на их рабочих компьютерах указанных компьютерных программ .*»

И даже наличие экспертного заключения, сделанного по запросу адвоката обвиняемого не всегда поможет.

«*Стороной защиты представлено заключение №226/ИЗ специалистов Фио Фио и Фио, согласно выводов которого: компьютерная программа «LanAgent» не является заведомо*

предназначенной для несанкционированных действий, перечисленных в ч. 1 ст. 273 УК РФ, поскольку исходя из документации на программу, она не предназначена производителем программы для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, а предназначена для защиты конфиденциальной информации от утечек, что является элементом защиты компьютерной информации. Компьютерная программа «Security Curator Agent» не является заведомо предназначенной для несанкционированных действий, перечисленных в ч. 1 ст. 273 УК РФ, поскольку исходя из документации на программу, она не предназначена производителем программы для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, а предназначена для обеспечения информационной безопасности и блокировки потенциально опасных путей утечки информации, что является элементом защиты компьютерной информации. Допрошенный специалист Фио подтвердил изложенные в заключении специалиста выводы в полном объеме.

Оценивая представленные заключения и показания Фио, суд не может принять их во внимание, поскольку лицами, составившими данное заключение, компьютерное оборудование непосредственно не осматривалось и его исследование не проводилось.»

А суд принимает во внимание, только заключение экспертизы со стороны обвинения.

«*Указанные компьютерные программы – „Time Machine“, „Security Curator Agent“ и „LanAgent“ считаются вредоносными в том случае, если пользователи исследованных компьютеров и ноутбуков (макбуков) не ставились в известность об установке и активации (включении, работе) данных программ на их компьютерах и ноутбуках. Указанные компьютерные программы „Time Machine“, „Security Curator Agent“ и „LanAgent“ заведомо предназначены, в силу своих особенностей для скрытого и без ведома пользователя функционирования для уничтожения, блокирования, модификации, копирования компьютерной информации и нейтрализации средств защиты компьютерной информации, а именно – „Security Curator Agent“ и „LanAgent“, и скрытого копирования компьютерной информации, а именно- „Time Machine“. Также в ходе производства экспертизы было установлено, что настройки всех трех программ „Time Machine“, „Security Curator Agent“ и „LanAgent“ были таковы, чтобы не отображать на экране их работу, то есть данные программы на исследуемых носителях информации функционировали скрытно и без ведома пользователя;*»

Системный администратор считал, что его задача только установить программное обеспечение на служебные компьютеры, а остальные действия вне зоны его трудовых обязанностей и ответственности.

«*Постановка в известность работников – пользователей компьютеров о данных программах, в целях исключения возможностей раскрытия информации в рамках локальной сети, касающейся их частной жизни, которую они могут разместить на компьютере – это прерогатива работодателя после установки программ, регулируется трудовыми договорами* .»

Он ошибся и был привлечен к уголовной ответственности.

(Приговор от 07.06.2016 №01—0006/2016)

Достаточно экспертного заключения и разработка или использование общедоступной программы нагрузочного тестирования сайта приводит к судимости программиста.

«*Согласно заключению компьютерной судебной экспертизы №80/Н/6—759т от 26.03.2019, сайт «l…» содержал исполняемый код (скрипт) с функциями программного обеспечения «L..», предназначенного для нагрузочного тестирования Интернет-ресурсов путем отправки большого количества HTTP-запросов.*

Действия ФИО1 квалифицированы по ч. 1 ст. 274.1 УК РФ – использование компьютерной программы заведомо предназначенной для неправомерного воздействия на критиче-

скую информационную инфраструктуру Российской Федерации, в том числе для блокирования информации, содержащейся в ней.»

(Постановление от 31.05.2019 №1—345/2019)

Не знал, что программное обеспечение для проведение нагрузочного тестирования заведомо предназначены для неправомерного воздействия на объекты КИИ? Никто не поверит…

«с использованием предназначенных для мониторинга отказоустойчивости доменов и сетевого оборудования легальных иностранных сайтов StresserUS, имеющего URL-адрес: https://stresser.us/, и Anonboot.com, имеющего URL-адрес: https://rankchart.org/site/anonboot.com/

действуя умышленно, из любопытства, в период с ДД. ММ. ГГГГ по ДД. ММ. ГГГГ, включительно, через небольшие интервалы во времени, находясь по месту своего жительства, используя браузер, установленный на своем мобильном телефоне «Redminote 7», осуществил вход под учетной записью «М..» на сайт «StresserUS», а затем на сайт «Anonboot» под учетной записью с аналогичным наименованием, заведомо зная, что указанные сайты предназначены для неправомерного воздействия на информационную инфраструктуру путем использования компьютерной программы, в том числе для блокирования содержащейся в ней информации»

(Постановление от 21.06.2022 №1—442/2022)

А еще есть отдельная статья уголовного кодекса – незаконное производство специальных технических средств, предназначенных для негласного получения информации (Ст. 138.1 УК РФ).

Для получения судимости достаточно заклеить светодиод – индикатор работы.

«После чего, 01.07.2024, более точное время следствием не установлено, находясь по месту своего жительства по адресу: адрес, действуя в продолжение своего преступного умысла, осознавая противоправность деяния и желая наступления общественно-опасных последствий, действуя с целью пресечения обнаружения указанного устройства посторонними лицами, фио закамуфлировал видеорегистратор путём наклеивания полимерной клейкой ленты и клейкой ленты из тканого материалы на элементы индикации на корпусе видеорегистратора, и таким образом, произвёл из него устройство, отнесённое согласно заключению эксперта №221э/20 от 29.11.2024 к категории специальных технических средств, предназначенных для негласного получения информации, по функциональной возможности и конструктивной приспособленности пригоден для использования по своему функциональному назначению и подпадает под пункт 2 Перечня видов специальных технических средств (разработанных, приспособленных, запрограммированных) для негласного получения информации в процессе осуществления оперативно-розыскной деятельности, утверждённого Постановлением Правительства Российской Федерации от 01.07.1996 №770.»

(Приговор от 08.04.2025 №1—146/2025)

Прокачка профессиональных навыков до судимости довела!

Сфера информационных технологий настолько динамично развивается, что без самообразования очень быстро перестанешь быть специалистом в своей профессии.

Интернет позволяет получить доступ к огромному массиву знаний, обучающим курсам и библиотекам прикладного программного обеспечения.

Скачал общедоступную программу для аудита защищенности сайта, посмотрел учебный видеокурс и решил провести практическую работу по закреплению полученных знаний. Только вот сайт чужой. И уже не важно, что не было умысла на что плохое, что никаких негативных последствий не наступило.

«*используя персональную электронно-вычислительную машину (далее – ПЭВМ) «Компьютер №1» с доступом в информационно-телекоммуникационную сеть «Интернет», зашел на сайт видеохостинга « <данные изъяты>», электронный адрес « <данные изъяты>», где открыл соответствующую ссылку, после чего сохранил на жесткий диск данной ПЭВМ (<данные изъяты>), в папку «Programm Files» специальное программное обеспечение (далее – СПО) « <данные изъяты>», позволяющее проводить аудит безопасности информационного ресурса посредством загрузки и запуска данного СПО на сторонних (удаленных) ПЭВМ. Далее Р. установил на ПЭВМ указанное СПО. В этот же день в период с 10.27 по 10.30 часов (время московское) Р., действуя умышленно, с целью проверки своих навыков по использованию СПО, достоверно зная, что веб-сайт <адрес> <адрес> – « <данные изъяты>», расположенный по электронному адресу: « <данные изъяты>» (<данные изъяты> 228) относится к объектам критической информационной инфраструктуры, открыл цифровое окно СПО « <данные изъяты>», внёс в него данные электронного адреса: « <данные изъяты>» (<данные изъяты>) после чего запустил указанное СПО. Таким образом, Р. осуществил использование компьютерной программы « <данные изъяты>» с целью проверки наличия на указанном сайте уязвимостей RCE, которая представляет собой возможность удаленного внедрения кода в серверный скрипт <адрес> <адрес>, главным администратором информационно-телекоммуникационной сети которой является «Казенное учреждение г. Омска « <данные изъяты>».*

(Приговор от 18.01.2021 №1—398/2021)

Пример с тестированием на работе:

«*В., осознавая в силу занимаемой должности необходимость прохождения процедуры тестирования знаний технико-распорядительных актов и стремясь получить гарантированный положительный результат тестирования, В., решил воспользоваться сторонним нештатным программным обеспечением, предоставляющим тестируемому в модуле «АС…» программного комплекса «АС…» ОАО «….» получение такого результата независимо от правильности ответов на вопросы теста.*

В этих целях В., обладая навыками работы с персональным компьютером и программным обеспечением, в вечернее время, около 20:57 часов, находясь по месту своего жительства по адресу: адрес, с использованием своего личного персонального компьютера – ноутбука марки «Lenovo» (s\n номер) в информационно-телекоммуникационной сети «Интернет» отыскал информационный ресурс «иные данные», на котором-обнаружил компьютерную программу «Бот…», заведомо предназначенную для неправомерного воздействия на модуль «АС…» программного комплекса «АС..» ОАО «….». Указанную компьютерную программу. В. скопировал на собственный внешний накопитель (флэш-карту), оплатив ее стоимость в размере 520 руб., посредством сервиса «Яндекс деньги».

В рабочее время В., имея при себе указанную флэш-карту прибыл в учебный класс, расположенный по адресу: адрес, р. адрес, где около 09:24 часов на служебном персональном ком-

пьютере, имеющем подключение к сети передачи данных ОАО»..» с IP-адресом …., приступил в модуле «АС…» программного комплекса «АС… – ОАО «…» к прохождению тестирования знаний технически-распорядительных актов.

Реализуя свой преступный умысел, направленный на использование компьютерной программы, заведомо предназначенной для неправомерного воздействия, осознавая общественную опасность и противоправность своих действий, предвидя возможность наступления общественно опасных последствий в виде модификации содержащейся в ней компьютерной информации, В. в этот же день в период с 09:10:48 часов по 16:20:24 часов при прохождении тестирования подключил собственный внешний накопитель (флэш-карту) к служебному персональному компьютеру и в период с 09:11:11 часов по 16:22:55 часов запустил стороннее программное обеспечение – компьютерную программу «Бот..», тем самым совершил умышленные целенаправленные действия, направленные на использование компьютерной программы, заведомо предназначенной для неправомерного воздействия на модуль «АС…» программного обеспечения «АС..».

Примененное В. на служебной ПЭВМ указанное нештатное программное обеспечение в виде исполняемых файлов, неправомерно модифицировало компьютерную информацию в программном комплексе «АС…», сформировав положительный результат его тестирования в модуле «АС».

(Приговор от 15.09.2020 №1—315/2020).

Или

«Н., являясь инженером электросвязи предприятия, решил в нарушение установленного законодательством РФ порядка, умышленно, незаконно, с рабочего персонального компьютера отправил на адрес электронной почты письмо, содержащее закрытую информацию.

Н., данных им в ходе предварительного следствия, следует, что <…> на рабочей ЭВМ он обнаружил каталог, содержащий видеофайлы с лекциями в области связи, а также каталог, содержащий техническую документацию и схемы сетей связи предприятия. В целях саморазвития он начал просмотр указанных лекций. <…>

Затем он решил продолжить саморазвитие и подготовку в свободное время, дома, используя обнаруженные им схемы и лекции. При этом он знал, что передача служебной информации за пределы предприятия запрещена, но не придал этому значения.

Для обхода системы защиты предприятия, а также для доступа к этим файлам с любого устройства, имеющего доступ в сеть Интернет, в не рабочее время, он использовал публичную почту.

Обвиняемый незаконно с рабочего компьютера ПАО «Ростелеком» скопировал и направил электронным письмом на личный компьютер информацию, относящуюся к охраняемой компьютерной информации ПАО «Ростелеком», создав опасность нанесения ущерба национальным интересам в информационной сфере, угрозу нарушения целостности сети связи»

(Приговор от 07.12.2020 №1—1317/2020)

«Участвуя на вышеназванных сайтах в веб-форумах, посвященных созданию вредоносных компьютерных программ, удаленному несанкционированному управлению ПК с помощью данных компьютерных программ, хищению и обналичиванию похищенных денежных средств и переписываясь на jabber-серверах, в тех же целях В.А. в период с 2009 г. по 2015 г. изучил:

– языки программирования: Assembly (ассамблер), Delphi (делфи),

PHP (Пи-Эйч-Пи) и другие, алгоритмы создания и изменения исходного кода вредоносного программного обеспечения, предназначенного для получения несанкционированного доступа к ПК, их удаленного и скрытного управления и получения с их помощью конфиденциальной информации пользователей ПК;

– возможности распространения вредоносного программного обеспечения на ПК неопределенного количества пользователей (юридических лиц), посредством массовой рассылки элек-

тронных писем и создания поддельных сайтов, в том числе, с бухгалтерскими бланками, содержащими файл загрузки вредоносного программного обеспечения, в также внедрение (инжектирование) вредоносного программного кода в легальные компьютерные программы;

– возможности управления посредством использования вредоносных компьютерных программ, банковскими счетами юридических и физических лиц через их системы дистанционного банковского обслуживания (ДБО), в том числе дистанционного перевода денежных средств с банковских счетов коммерческих организаций и других юридических лиц на подконтрольные счета юридических и физических лиц;

– возможности хищения хранящихся на банковских счетах безналичных денежных средств с помощью вредоносных компьютерных программ.

При этом В.А. в тот же период, но не позднее 2015 г., точное время не установлено, проживая по адресу: <адрес>, посредством переписки на jabber-серверах под сетевыми именами forecast@xmpp.jp, twotish@jabber.de, bsod@jabber.de, познакомился с неустановленным лицом под псевдонимом «kutuzov», использовавшим сетевые имена kutuzov@afera.li и kutuzov_money@default.rs, по договоренности с которым, за денежное вознаграждение последнего, согласился создать уникальную вредоносную компьютерную программу с модульной структурой, заведомо предназначенную для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации и нейтрализации средств защиты компьютерной информации.

После этого, В.А., проживая по адресу: <адрес>, обладая специальными познаниями в области компьютерной техники и программирования, из корыстной заинтересованности, при неустановленных обстоятельствах создал (разработал) основные модули вредоносного программного обеспечения (вредоносные компьютерные программы), которые им условно обозначались как «RTM»

(Приговор от 26.10.2023 №1—36/2023)

Посещение хакерских форумов к беде приводит

Хотя и утверждается, что «врага надо знать в лицо и изучать его возможности», но в случаях с темной стороной компьютерного профессионального сообщества (хакерами) такая исследовательская деятельность специалиста ИТ требует очень серьезной осмотрительности.

Правоохранительные органы фиксируют следы такого профессионального любопытства и это отягощает дальнейшую судьбу специалиста ИТ.

«*Примерно с 2017 года он начал изучать сферу информационных технологий, узнал про браузер «Tor». В нем он начал изучение вопросов информационной безопасности на специализированных форумах, названия которых не помнит, их очень много, и все они посвящены компьютерным атакам. У него было много свободного времени, и он решил этим заняться.*

На указанных форумах он скачал компьютерную программу <…> для неправомерного доступа к информационным системам путем перебора паролей по заданному диапазону IP-адресов с указанием порта с целью получения логин/парольных пар. Все это происходило примерно с 1 января 2021 года по ноябрь 2023 года, он скачивал все дома со своего IP-адреса, с помощью одного из двух ноутбуков (какого именно, он уже не помнит, так как прошло много времени). В квартире у него имеется несколько электронных устройств, а именно два ноутбука <…>; они изъяты в ходе ОРМ «обследование помещений, зданий, сооружений, участков местности и транспортных средств». Соответственно, используя один из вышеуказанных ноутбуков, он и скачал программу. В сети Интернет он детально изучал способы получения неправомерного доступа к веб-камерам и ftp-серверам при помощи компьютерной программы <…> ему это было интересно, для этого в 2021 году он зарегистрировался на хакерском ресурсе <…> для изучения вопросов получения неправомерного доступа к информационным системам, осуществления компьютерных атак и использования для этих целей специализированных программ. Изучив данные о компьютерных атаках, он пришел к выводу, исходя из найденных в сети Интернет материалов, что перебор необходимо осуществлять по портам 3777, 8000 и 21. Выбор IP-адресов для атаки он осуществлял при помощи сайта, название которого вспомнить уже не может, так как последний раз заходил на него в конце ноября 2023 года. В конце ноября 2023 года он выбрал диапазон российских IP-адресов ради интереса.»

(Приговор от 25.03.2025 №1—113/2025)

«*В.А., проживая по адресу: <адрес>, используя находящиеся в его распоряжении персональные компьютеры (далее – ПК) и мобильные средства связи, подключенные к информационно-телекоммуникационной сети «Интернет» (далее – Интернет), из корыстных побуждений, в целях незаконного обогащения, имея умысел на создание, распространение и использование компьютерных программ, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации и нейтрализации средств защиты компьютерной информации, то есть вредоносных компьютерных программ, получение с их помощью неправомерного доступа в локальные сети различных коммерческих организаций и ПК их работников и систематических хищений денежных средств с банковских счетов коммерческих организаций, зарегистрировался на специализированных сайтах «exploit.in» и «wasm.in», посвященных, в том числе, созданию вредоносных компьютерных программ, удаленному несанкционированному управлению ПК пользователей с помощью данных компьютерных программ, хищению и обналичиванию похищенных денежных средств, под сетевым именем «reverse» и «K10», создав при этом одноименные учётные записи. Кроме этого, в этих же целях В.А. с 2009 г. создавал на обеспечивающих анонимность jabber-серверах различные учетные записи, в том числе forecast@xmpp.jp, twotish@jabber.de и bsod@jabber.de, которые в целях конспирации, систематически менял.*»

(Приговор от 26.102023 №1—36/2023)

«ФИО1 начал активно изучать программирование. Для своего обучения он выбрал открытые интернет источники, а именно различные форумы компьютерной направленности, в том числе и интернет ресурсы «Хабре» и «Лолзтим». Благодаря статьям на указанных форумах ФИО1 освоил языки программирования «C++» и «C#». Поскольку ФИО1 нужны были денежные средства на карманные расходы, он решил заработать на своих навыках программирования. Примерно в это же время на одном из открытых форумов в сети интернет он узнал о т.н. услугах «криптование». Насколько ему известно, «криптование» – это обход средств антивирусной защиты путем модификации вредоносного программного обеспечения. Чтобы разобраться в «криптовании» он начал изучать работу средств антивирусной защиты на основе статей из интернета.

Изначально у ФИО1 не получалось создать программу для «криптования», поэтому он часто откладывал ее разработку и больше изучал принцы ее работы и способы написания исходного кода. Так, примерно с конца января 2023 года по лето 2023 года ему удалось на своем компьютере посредством программного обеспечения «VisualStudio» создать вредоносную программу «CLRegAsm. exe», которую он хранил в папке «clregasm-master» на «рабочем столе» своего компьютера. Данная программа предназначена для обхода средств антивирусной защиты путем модификации вредоносного программного обеспечения. В связи с постоянным обновлением средств антивирусной защиты ФИО1 примерно раз в 10 дней актуализировал ее с учетом новых обновлений.»

(Приговор от 05.02.2024 №1—21/2024)

Наказывается даже неудачная попытка использования программного обеспечения, отнесенного экспертизой к вредоносной.

«А.К., обладая навыками работы с персональным компьютером, находясь по <адрес>, используя личный ноутбук фирмы « <данные изъяты>», s/n: <данные изъяты>, пришкал в информационно-телекоммуникационной сети «Интернет» архив с названием « <данные изъяты>», содержащий компьютерную программу « <данные изъяты>», заведомо предназначенную для нейтрализации средств защиты компьютерной информации, после чего скопировал её в память принадлежащего ему твердотельного накопителя серого цвета производства фирмы « <данные изъяты>».

С целью получения навыков работы с компьютерной программой « <данные изъяты>» А.К. в информационно-телекоммуникационной сети «Интернет», доступ к которому ему был предоставлен провайдером ООО Телекоммуникационная группа « <данные изъяты>», изучил порядок установки и использования указанной компьютерной программы.

Кроме того, А.К. изучил описание и инструкции по использованию компьютерной программы « <данные изъяты>» путем прочтения их в текстовом файле, содержащемся в скаченном им архиве с названием « <данные изъяты>», в результате чего получил достоверную информацию о принципах функционирования компьютерной программы и убедился в предназначении программы « <данные изъяты>» для получения доступа к компьютерной информации и нейтрализации средств защиты компьютерной информации без согласия владельца.

Далее, А.К., находясь по <адрес>, используя личный ноутбук фирмы « <данные изъяты>», s/n: <данные изъяты> (IP-адрес: <данные изъяты>), подключенный к информационно-телекоммуникационной сети «Интернет», а также принадлежащий ему твердотельный накопитель серого цвета производства фирмы « <данные изъяты>», в целях проверки собственных навыков владения компьютерными программами, осознавая противоправность и общественную опасность своих действий, предвидя возможность наступления общественно опасных последствий, связанных с несанкционированным уничтожением, блокированием, модификацией, копированием компьютерной информации или нейтрализацией средств защиты компьютерной информации использовал компьютерную программу « <данные изъ-

яты>» заведомо предназначенную для нейтрализации средств защиты компьютерной информации.

В результате использования компьютерной программы « <данные изъяты>» на сайт МБУ ДО «ФИО8» были осуществлены компьютерные атаки (более 600 воздействий), заключающиеся в попытке получения несанкционированного доступа к компьютерной информации путём подбора аутентификационной информации (пара – «логин-пароль») к системе управления контентом « <данные изъяты>» по протоколу «HTTP».

Получить доступ к компьютерной информации сайта « <данные изъяты>» (IP-адрес: <данные изъяты>) А.К. не смог по причине его высокой технической защищенности. »

(Постановление от 10.09.2020 №1—414/2020)

«При допросе в качестве подозреваемого и обвиняемого В. пояснил, что в 2021 году во время просмотра различных информационных ресурсов в сети «Интернет», связанных с компьютерными технологиями, он обнаружил утилит «…» для сканирования интернет-сети по диапазонам ip-адресов с последующим брутфорсом (т.е. подбором аутентификационных данных (логин и пароль) от ранее отсканированных различных интернет-ресурсов, что является само по себе совершением компьютерных атак методом подбора аутентификационных данных. Ему показалось это очень интересным, и он решил изучить данный утилит в целях дальнейшего использования полученных знаний на практике, т.е. осуществлять неправомерный доступ к различным устройствам и информационным ресурсам.

Находясь по адресу: Адрес, используя свой компьютер, подключенный к сети интернет провайдер от ПАО «Ростелеком», на информационном портале обнаружил вредоносную программу «…», после чего, осуществил ее загрузку и установку на свой компьютер. Он осознавал, что программа «…» – является вредоносной. Далее в период с 2021 года по 2023 год, используя вредоносную компьютерную программу «…» осуществлял многочисленные компьютерные атаки (неправомерное воздействие) в отношении различных ip-адресов, принадлежащих различным источникам, расположенным по разным городам России, уязвимости которых выдавала программа «…», что в последующем позволяло нейтрализовать средства защиты компьютерной информации содержащейся на различных ip-адресах. Каждая компьютерная атака была совершена им индивидуально, в разный промежуток времени и направлена на конкретный результат.

Он показал, что вредоносная программа «…» осуществляла попытку доступа к информационным ресурсам, а так же к защищаемой компьютерной информации, которая содержится на различных интернет-ресурсах, при этом он не исключал, что на различных ip-адресах, к которым он пытался получить доступ, могут содержаться как объекты, так и субъекты критической информационной инфраструктуры Российской Федерации. Также пояснил, что ip-адреса: №№ ему знакомы, поскольку являлись объектами совершенных им компьютерных атак. Данные ip-адреса получил после того, как в 2022 году в поисковике интернет – браузера вбил ip – диапазоны, после чего скопировал выбранный им ip диапазон и вставил в поле программы «…».

Далее, он собственноручно запустил программу «…». В процессе работы, данная программа начала сканировать ip-диапазоны, среди которых находились ip-адрес: №№ В процессе сканирования указанных ip-адресов, программа осуществляла попытку подбора аутентификационных данных (логин и пароль) по встроенным в ней списком логинов и паролей, но безуспешно. Кроме того показал, что он не исключал, что ip-адреса: №№, могут быть объектом либо субъектом критической информационной инфраструктурой Российской Федерации, но его это не остановило и в конечном итоге результат работы программы „…“ в отношении ip-адресов: №, был безуспешен, в случае успешного доступа (компьютерной атаки) к вышеуказанному ресурсу, он бы имел возможность, в том числе модифицировать, блокировать или копировать какую-либо информацию, хранящуюся на них»

(Приговор от 14.11.2024 №1—534/2024)

Машина виртуальная, а срок условный

Специалист ИТ получил задачу от своего руководителя, но не учел, что произошли изменения в статусе обслуживаемой им информационной инфраструктуры (стала объектом КИИ). Выполнил задачу как обычно. К качеству выполненной работы претензий нет, а уголовная ответственность есть. И предпринятые меры по защите информации в ходе выполнения рабочей задачи поставлены в вину самому работнику!

«Согласно рапорту об обнаружении признаков преступления от ДД. ММ. ГГГГ, в результате осуществления комплекса оперативно-розыскных мероприятий получены материалы, из которых следует, что инженер – электроник отдела информационно-телекоммуникационных сетей и инфраструктуры <адрес>» А.Е., с целью доступа в ИТКС «Интернет», в нарушении правил эксплуатации информационно-вычислительной сети предприятия, установленных положением «О порядке работы в ИВС» от ДД. ММ. ГГГГ №, осуществил несанкционированную установку в ИВС предприятия маршрутизатора «Mikrotik», а также его подключение и настройку для выхода в Интернет, после чего, находясь на рабочем месте, модифицировал сетевые настройки виртуального рабочего места «CentOS8-CA-RADIUS» (изменил сетевые настройки интернет – браузера Mozilla Firefox, в которые внес proxy-сервер с ip-адресом ДД. ММ. ГГГГ.5, одновременно внеся разрешающее правило для данного адреса на Mikrotik), тем самым организовал связь виртуальной машины и маршрутизатора «Mikrotik» и подключил виртуальную машину к ИТКС «Интернет», создав несанкционированный неконтролируемый канал доступа объекта КИИ РФ (ЦОД предприятия) к ИТКС «Интернет»

В 2021 году проводилась проверка в отношении инженера – электроника А.Е. на основании сведений ФСБ об организации им канала доступа в ИВС предприятия, в одной из виртуальных машин, располагающейся в системе, относящейся к КИИ. Было нарушено Положение об ИВС предприятия и должностная инструкция в части безопасности информации. Когда он работал в составе комиссии по проверки данного инцидента, то поднимали указанные документы и установили, что А.Е. с Положением об ИВС предприятия и своей должностной инструкцией был ознакомлен. Было также установлено, что он допустил изменение технических средств ИВС, а также создал дополнительный канал связи, самовольно переустановил программное обеспечение.

В частности, была создана виртуальная машина на серверах, находящихся в ЦОДе, входящем в состав КИИ. А.Е. действовал в служебных целях по указанию его начальника для установления программного обеспечения на оборудовании, входящем в состав ЦОД, однако для удобства скачивания и обновления программного обеспечения на указанное оборудование, относящееся к КИИ, А.Е. создал канал связи в сети Интернет, чем был причинен ущерб КИИ.

Прямого вреда не было, то есть никакое оборудование из строя не вышло, проникновения в сеть ИВС из вне не было, но создание канала связи создало угрозу такого проникновения. На предприятии имеется официальный способ доступа к сети Интернет – посредством переноса программного обеспечения через внешний носитель, что регламентировано отдельными документами предприятия, таким способом пользуется большинство сотрудников. То есть в <адрес> практически в каждом отделе имеются пункты доступа к сети Интернет в виде отдельных компьютеров, посредством которых можно выйти в сеть Интернет, скачать оттуда информацию, в том числе программное обеспечение путем переноса на отдельный съемный носитель. Однако А. Е. подключился к сети Интернет напрямую посредством подключения и настройки Mikrotik

Под словом «инцидент», употребляемым им в пояснениях относительно А.Е. он подразумевал то, что в отношении А.Е. проводилась проверка по поводу подключения им виртуальной машины к сети Интернет. Ранее виртуальные машины к сети Интернет подключали,

но это было до КИИ, то есть до начала 2020 года, точную дату назвать не может. В таком случае, то есть подключения к сети Интернет до 2020 года, за это было наказание в виде замечания, даже выговор не объявлялся. После внесения объектов в КИИ, случай подключения к сети Интернет А. Е. был первым.

В обязанности А.Е.. входила установка и настройка сетевого оборудования, поддержка пользователей, подключение рабочих мест к автоматизированной системе предприятия, работа с серверами – мониторинга, доступа и других, их конфигурирование. К ним в бюро поступило письмо из Роскосмоса с требованием усиления безопасности, в связи с чем он получил задание от руководства решить вопрос с контролем доступа к сети предприятия. У них на предприятии существует сервер доступа – программное обеспечение «Cisco ACS», который может выполнять такие функции контроля. Однако данный сервис платный и его продление после 2014 года было проблемным. Кроме того, у данного сервиса был бак (дефект), который мешал в работе, что могло привести к тому, что все компьютеры пользователей не смогут подключаться к сети. В связи с этим они, зная о наличии доступного открытого программного обеспечения «Freeradius», способного осуществлять аналогичные функции контроля, то решили заменить «Cisco ACS» на «Freeradius». В связи с этим он дал А.Е. задание установить программное обеспечение «Freeradius» и попробовать его в работе, что также входило в обязанности А.Е. и он с задачей справился, установил данную программу, виртуальная машина, созданная А.Е. в настоящее время клонирована и функционирует на предприятии более года без каких-либо изменений.

С целью выполнения указанной задачи было принято решение произвести тестирование программного обеспечения «free-RADIUS». Данное программное обеспечение является свободно распространяемым и не требует лицензии на инсталляцию («open sourse»). Для контроля доступа пользователей к сети предприятия А.Е. было поручено установить и протестировать «free-RADIUS» серверы, как серверы доступа к ИВС предприятия на замену сервера-доступа «Cisco ACS», который приобретен по лицензии. Однако, в работе «Cisco ACS» имелись неполадки в работе т.н. «баги», которые указанной программой предлагалось устранить путём покупки нового лицензионного продукта по более дорогой цене. Для выполнения указанной задачи, А.Е. должен был установить сервер «free-RADIUS» и подключать к нему устройства, входящие в ИВС предприятия, после чего аутентифицировать пользователей или устройства.

Программное обеспечение «Freeradius» осуществляет контроль подключений, что обеспечивает при попытках подключения к сети идентифицировать пользователя и, в зависимости от ответа сервера, допустить пользователя к сети либо ограничить доступ. Программное обеспечение «Freeradius» и «Cisco ACS», в целом, выполняют одни функции, но каждое из них имеет свои преимущества. Проблема программного обеспечения «Cisco ACS» в том, что все обновления и поддержка платные, причем по стоимости изначальной закупки самого программного обеспечения, стоимость на момент приобретения (примерно в 2012—2014 гг.) «Cisco ACS» составляла порядка 7 000 долларов. Покупка обновления и поддержки «Cisco ACS» после 2014 года стала проблемной из-за санкций. Установка «Freeradius» непосредственно из сети Интернет из официального репозитория, путем введения команды безопасно, поскольку производятся с применением публичного ключа шифрования, что позволяет убедиться, что скачанная программа из официального репозитория и аутенцифитировать репозиторий.

То есть А.Е..в ходе выполнения порученных ему задач был нарушен периметр ИВС, а именно осуществлен удаленный доступ к периметру предприятия из дома.

Со слов А.Е.. следовало, что перед ним была поставлена задача, а как ее выполнить ему не сказали, поэтому он ее выполнял так, как сам решил.

Было установлено, что имело место неправомерное подключение периметра внутренней сети предприятия к сети Интернет, что категорически запрещено. Также было установлено, что А.Е. вносил изменения в программное обеспечение на автоматизированном рабочем месте, подключил внешнее устройство к рабочему месту, находящемуся во внутренней сети предприятия. Есин пояснил, что все действия проводил в рамках своих должностных обязанностей во исполнение поручения руководителя. Все действия выполнил с целью скорейшего выполнения задания… однако уточнил, что удаленный доступ из дома организовал для того, чтобы работать из дома удаленно в нерабочее время, то есть сверхурочно.

Для того, чтобы наиболее полно оценить каналы утечки информации, а также причиненный ущерб, было принято решение привлечь к проверке стороннюю специализированную организацию <адрес>. По результатам проверки сотрудниками указанной организации был предоставлен отчет, исходя из которого, факт указанных выше нарушений подтвердился, также указано, что объекту КИИ был нанесен вред в плане создания канала возможного воздействия на объект КИИ – ЦОД. В результате организации канала могло быть выведено из строя оборудование ЦОД путем внешнего внесения через канал вредоносных программ.

Ущерб предприятию выражен в том, что пришлось оплачивать услуги компании <адрес>.

действиями А.Е. объекту КИИ РФ (ЦОД РКЦ) нанесен организационный (технологически-эксплуатационный) вред, выразившийся в нарушении безопасности доступа и эксплуатации обрабатываемой и хранящейся компьютерной информации оборонного предприятия, находящейся в КИИ РФ третьей категории значимости, в результате чего создана возможность проникновения внешних злоумышленников в периметр объектов КИИ РФ и нанесения им критического ущерба вплоть до выведения из строя, потери данных и отказа критических для функционирования предприятия процессов.

Доводы защиты о принятых А.Е. при организации канала средствах защиты от проникновения в ИВС предприятия, суд не принимает во внимание, поскольку как установлено в судебном заседании, данные средства не исключают возможность проникновения в закрытую сеть предприятия при наличии канала связи, организованного напрямую через сеть Интернет

При этом, суд отмечает, что доводы подсудимого относительно применения им всех известных ему технических мер (аппаратных и программных) с целью исключения возможных угроз безопасности информационно-телекоммуникационной сети предприятия, прямо свидетельствуют о том, что подсудимый осознавал, что своими действиями нарушает безопасность доступа и эксплуатации обрабатываемой и хранящейся в ЦОД информации и понимал последствия этого в виде возможности проникновения внешних злоумышленников в периметр объектов КИИ РФ.

Аналогичным образом, об осведомленности А.Е. относительно возможных последствий в виде причинения вреда объектам ЦОД, относящимся к КИИ РФ, свидетельствуют его доводы о том, что устройство «Mikrotik» не работало непрерывно, а включалось им только по необходимости.

Как установлено судом, А.Е. нарушая правила эксплуатации информационно-телекоммуникационных сетей, а также правила доступа к информационно-телекоммуникационным сетям, будучи квалифицированным специалистом в области информационных технологий, являясь сетевым администратором, будучи осведомленным о правилах работы в ИВС предприятия и установленных запретах, а также об отнесении объектов ЦОД предприятия к КИИ РФ, осознавал общественную опасность своих действий, предвидел возможность наступления общественно опасных последствий в виде причинения вреда, выразившегося в нарушении безопасности доступа и эксплуатации обрабатываемой и хранящейся компьютерной информации оборонного предприятия, находящейся в КИИ РФ, создании воз-

можности проникновения внешних злоумышленников в периметр объектов КИИ РФ и нанесения им критического ущерба вплоть до выведения из строя, потери данных и отказа критических для функционирования предприятия процессов, то есть создании угрозы наступления тяжких последствий для ИВС и технологических процессов завода, в том числе срыва сроков исполнения государственного оборонного заказа, не желал, но сознательно допускал эти последствия.

ПРИГОВОРИЛ:

Признать А. Е. виновным в совершении преступления, предусмотренного ч. 3 ст. 274.1 УК РФ, и назначить ему наказание в виде лишения свободы сроком в 1 (один) год 6 (шесть) месяцев»

(Приговор от 28.02.2023 №1—11/2023)

Зарубежные ресурсы не для использования в работе

Достаточно часто возникает необходимость переслать на зарубежную почту типа gmail или воспользоваться иностранными мессенджерами в рабочих целях. Причем отправка может проводиться на свой же личный почтовый ящик, а в мессенджере сохраняться в папке «Избранное». Просто что бы нужная информация всегда была доступна при необходимости.

Но именно для ИТ специалистов это несет наибольшую опасность – документация о сетевой архитектуре, настройках, протоколах маршрутизации относиться государством к чувствительной для безопасности страны, так как ее наличие у хакера повышает разрушительные последствия от потенциальных компьютерных атак.

«..которая после отправки на личный почтовый ящик сохранилась в памяти облачного хранилища компании „Google“ зарегистрированной в США, тем самым О.В. причинил вред критической информационной инфраструктуре Российской Федерации в виде раскрытия информации о моделях, серийных номерах, количестве используемых портов и территориальном расположении телекоммуникационного оборудования применяемого на сети связи Амурского филиала ПАО „Ростелеком“, нарушив правила эксплуатации информационных систем, информационно-телекоммуникационных систем, автоматизированных систем управления, сетей электросвязи, относящихся к критической информационной инфраструктуре Российской Федерации, осуществив копирование электронных сведений, содержащих подробные данные о топологии сети Амурского филиала ПАО „Ростелеком“, и передав их постороннему лицу, не имеющему допуска к указанным сведениям, путем отправки их на адрес электронной почты бесплатного электронного сервиса компании „Google“ зарегистрированной в США. Нарушение правил доступа к сведениям о топологии сети Амурского филиала ПАО „Ростелеком“ или нарушение правил передачи посторонним лицам указанной информации, содержащейся в информационных системах, информационно-телекоммуникационных сетях, автоматизированных системах управления, сетях электросвязи, относящихся к критической информационной инфраструктуре Российской Федерации, причинило вред в виде угрозы нарушения целостности сети связи ПАО „Ростелеком“, вследствие прекращения функционирования телекоммуникационного оборудования в результате разрушающих функционирование телекоммуникационного оборудования в результате разрушающих физических или информационных воздействий.»

(Приговор от 26.06.2020 №1—536/2020)

Аналогичные ситуации возникают при пересылке информации ограниченного доступа, например, персональных данных, через иностранные мессенджеры.

Правоохранительные органы трактуют, как передачу охраняемой законом информации по средствам связи, контролируемых специальными службами иностранных государств.

«*Судом установлено, что осужденный, используя служебный персональный компьютер и персональные учетные записи сотрудников одного из областных медицинских учреждений, зарегистрированных в государственной информационной системе здравоохранения Оренбургской области, незаконно копировал персональные данные пациентов. После чего с помощью программы анонимной электронной переписки в одном из мессенджеров по каналу связи, находящемуся под управлением Бюро разведки и исследований Государственного департамента США, а также Федерального бюро расследований…*

Направленные Пикаловым Д. А. в адрес разведывательных органов США персональные данные наших граждан могли быть использованы против безопасности Российской Федерации.

.. виновным в совершении преступлений, предусмотренных ч. 5 ст. 274.1 и ст. 275 УК РФ и осужден по совокупности преступлений к 19 годам лишения свободы с отбыванием

наказания в исправительной колонии строгого режима со штрафом в размере 300 000 рублей и иными дополнительными видами наказания.»

(Приговор от 16.12.2024 №2—19/2024)

Пентест

Тема проведения пентестов сейчас очень модная, активно внедряется в нормативные требования по защите информации, специалисты по пентесту востребованы рынком и высокооплачиваемые. Все это привлекает как молодых и начинающих специалистов ИБ, так и уже опытных из других специализаций ИБ.

При этом, пентесты одно из самых слабо урегулированных специализаций ИБ с точки зрения уголовного преследования. Уж очень тонкая грань между «этичным хакингом» и криминальным хакингом, особенно с учетом использования однотипных инструментов взлома/пентеста.

«Программное обеспечение использовалось исключительно в познавательных целях, доступ к сетевому оборудованию потерпевших не осуществлял, ее использованием не желал и не причинил никому вреда. Он скачал на свой компьютер программу « <данные изъяты>» и хотел использовать ее для проверки компьютерной сети организации, в которой работает. Он запускал программу « <данные изъяты>» и она в автоматическом режиме попыталась сканировать сетевое оборудование. Программу он использовал в ознакомительных целях, то есть у него не было никакого намеренного умысла причинить вред и никакого вреда потерпевшим он не причинил.

Программа « <данные изъяты>» не является вредоносной, у программы « <данные изъяты>» есть собственный сайт в сети интернет, на ней указаны разработчики данного программного обеспечения. Сайт не заблокирован Роскомнадзором.

Кроме того, та программа, которой он пользовался, не позиционирует себя как вредоносная, сообщений о незаконном использовании при запуске не выдает, что подтверждается проведенной экспертизой, сайт программы находится в свободном (общем) доступе в сети «Интернет», активная аудитория пользователей данной программы составляет не менее 3300 человек, которые не скрывают факт, использование данной программы и открыто общаются друг с другом в сети «Интернет». Полагает, что вывод о вредоносности программного обеспечения сделан экспертом ФИО10 на основе личного опыта, игнорируя четкие понятия и терминологию, указанные в закрепленных ГОСТах..Обращает внимание на то, что на сайте «Роскомнадзора», информации о вредоносности или запрета к использованию данной программы не содержится, антивирусные программы, данное программное обеспечение, как вредоносное не определяют, официальный сайт программы в сети «Интернет» не заблокирован.

Согласно выводам эксперта, «Router Skan» – это программа для поиска в сети интернет веб-интерфейсов сетевого оборудования, с целью дальнейшего получения несанкционированного доступа к нему. Несанкционированный доступ достигается путем нейтрализации средств защиты веб-интерфейса сетевого оборудования с помощью подбора пары логин/пароль либо эксплуатации программных уязвимостей указанного оборудования. Программа «Router Skan» предоставляет возможность пользователю нейтрализовать средства защиты компьютерной информации, то есть является вредоносной компьютерной программой. Иного предназначения данное программное обеспечение не имеет

— показаниями эксперта ЭКЦ ГУ МВД России по Воронежской области ФИО3 о том, что для экспертизы был предоставлен системный блок, было несколько вопросов, его были вопросы 1, 2, 4, 7. Первый вопрос – имеется ли электронное программное обеспечение с определенным наименованием? Второй вопрос – детектируется ли антивирусными программными обеспечениями с определенным наименованием? Четвертый вопрос – имеются следы использования данного программного обеспечения? Седьмой вопрос – имеется ли следы выхода в сеть интернет, или использовались какие-либо учетные данные пользователя компьютера?

Он на эти вопросы ответил. На первый вопрос – программное обеспечение было обнаружено. На второй вопрос – программа «Router Scan» антивирусным программным обеспечением не детектировалось, как вредоносная.»

(Постановление от 02.03.2021 №1—40/2021)

«УСТАНОВИЛ:

В.Ю. для установления уязвимостей удаленного ресурса информационно-телекоммуникационной сети «Интернет» (далее Интернет-ресурс) решил использовать со своей персональной электронной вычислительной машины (далее ПЭВМ) вредоносную компьютерную программу «SQLi Dumper», предназначенную заведомо для него для получения неправомерного доступа к компьютерной информации методом SQL-инъекций, несанкционированного уничтожения, блокирования, модификации и копирования компьютерной информации на сервере, в случае подставки вредоносными SQL-запросами некорректных значений в параметры, применяемые веб-сервером.

Признать В. Ю. виновным в совершении преступления, предусмотренного ч. 1 ст. 273 УК РФ и назначить ему наказание в виде ограничения свободы сроком 1 (один) год.»

(Приговор от 02.07.2020 №1—183/2020)

«А. вину полностью не признал и пояснил, что он проживает в <адрес>, работает <данные изъяты> он скачал на свой компьютер программу « <данные изъяты>» и хотел использовать ее для проверки компьютерной сети организации, в которой работает. Он запускал программу « <данные изъяты>» и она в автоматическом режиме попыталась сканировать сетевое оборудование. Программу он использовал в ознакомительных целях, то есть у него не было никакого намеренного умысла причинить вред. Никакого вреда потерпевшим он не причинил. Программа « <данные изъяты>» не является вредоносной, у программы « <данные изъяты>» есть собственный сайт в сети интернет, на ней указаны разработчики данного программного обеспечения. Сайт не заблокирован Роскомнадзором .

Действия А. суд квалифицирует по ч. 1 ст. 273 УК РФ, так как он совершил использование программы, заведомо предназначенной для нейтрализации средств защиты компьютерной информации.

А. обладает знаниями в области информационных технологий и использования компьютерной техники, поскольку имеет высшее образование по специальности информационные системы и технологии и стаж работы по специальности.

Доводы защиты о том, что действиями А. потерпевшим не причинено никакого вреда, суд находит не состоятельными, поскольку состав, предусмотренный ч. 1 ст. 273 УК РФ является формальным и не требует наступления каких-либо последствий, уголовная ответственность возникает уже в результате использования компьютерных программ, заведомо предназначенных для нейтрализации средств защиты компьютерной информации, независимо от того, наступили ли в результате этого какие-либо общественно опасные последствия.»

(Приговор от 25.11.2020 г. по делу №1—40/2020)

«подсудимый является студентом КГУ ИФМЭН «Информационная безопасность», изучает теорию информации и кодирования, обладает навыками и знаниями в области программирования.

В 2022 году он заинтересовался технологиями поиска по открытым источникам. Поиск по открытым источникам – это размещенная на открытых сайтах, площадках информация, которая ранее была похищена неустановленными лицами у организаций, физических лиц, после чего размещена на вышеуказанных площадках. В процессе изучения его заинтересовала сфера «Penetration Testing» – тестирование систем на уязвимость. Он изучал различ-

ные площадки, связанные с этой сферой, например «Наск The Box» и его заинтересовало, каким образом можно получать доступ к данным на каком-либо носителе – персональном компьютере, облаке, сервере. Зимой 2023 года он зашел на ресурс «…» https://… com. На одной из форумных веток площадки он нашел пост, размещенный пользователем «Эссентри Тим». В данном посте содержался код вредоносной программы, которая по факту является стиллером, с названием»..». Стиллер – это файл формата «exe», который попадая на компьютер какого-либо пользователя, собирает всю возможную информацию, в том числе, пароли, логины, файлы, техническую информацию об устройстве, после чего отправляет ее на сервер человека, который полностью настроил работу кода в соответствии с заданными стандартами конкретного стиллера. «Скомпилировать код» значит собрать воедино весь массив кода, чтобы все его файлы могли между собой правильно взаимодействовать. Под кодом он подразумевает несколько файлов, имеющих различные расширения и форматы. Так, там имелась панель, предназначенная для получения данных, билдер, который собирает вирус воедино с целью взаимодействия всех заданных команд. Вирус, собранный билдером отправляет на вышеописанную панель полученные в результате заражения программой сведения и информацию. Он протестировал данный стиллер на принадлежащем ему компьютере. В ходе неоднократного тестирования он установил, что половина команд кода, которые он тестировал, не работает так, как должны. На тот момент он уже придумал название для стиллера – «Phoenix».

На момент тестирования им данной вредоносной программы, тот мог собирать данные об устройстве, версию операционной системы, размер оперативной памяти, IP-адрес, наличие видеокарты. Он понимал и осознавал, что данная программа является вредоносной, поскольку обладал навыками и знаниями в этой сфере. Его не устраивало, что стиллер не работает в полном объеме, в результате чего, он решил обратиться к людям, понимающим в данной сфере, чтобы постараться починить код.

В тот момент он состоял в сообществе людей, интересовавшихся кодировкой, хакингом – «Phoenix», а также был подписан в телеграмме на канал «…», посвященный тематике специальной военной операции и публикующий информацию о различных атаках хак-группировок на серверы и сайты страны, где в настоящий момент проходит специальная военная операция. В сообществе он познакомился с человеком с никнеймом в «Телеграме» – «…». С ним он лично никогда не виделся, только общался посредством мессенджера «Телеграмм». Знал, что этот человек обладает знаниями, достаточными для того, чтобы поправить код его стиллера, чтобы тот работал. Он связался с ним, отправил ему скомпилированный исходный код стиллера, заархивированный в формате «RAR», попросив помочь настроить неработающие команды. «…» ему помогать не стал, так как не захотел разбираться в данном софте. Переписку с указанным лицом подтверждает. Также зимой 2023 года он отправлял стиллер посредством «Телеграмм» людям с никнеймами «3», «5» с целью того, чтобы те также посмотрели и проверили скомпилированный исходный код. Отправлял стиллер также в формате файла с расширением «RAR».

Стиллер на тот момент был в таком же состоянии, в нем также не работала часть команд. Тестирование удовлетворяющих его результатов не достигало, и у него начал пропадать интерес к данной сфере, в результате чего, код он так и не усовершенствовал, после чего, больше не использовал. Признает, что распространил среди нескольких его знакомых исходный код вредоносной программы – стиллер, но делал он это, не имея корыстных намерений, а только в целях изучения работы данной сферы кодинга.

Никому не отправлял файл с расширением «exe», а отправлял именно исходный код. Сам исходный код в своем исходном состоянии не наносил вреда человеку, который его запускал, так как тот, сам по себе, не является вирусом. Данный код может использоваться и в полезных целях, для облегчения аутентификации пользователей сайтов. В содеянном раскаивается

Тот факт, что ФИО1 отправлялся не исполняемый файл с расширением». exe», а часть кода, с учетом вышеуказанных разъяснений Постановления Пленума ВС РФ значения для квалификации содеянного подсудимым значения не имеет.

ФИО11 не являлся лицом, использовавшим указанную программу правомерно для установленных законом целей.

Таким образом, действия ФИО1 суд квалифицирует по ч. 1 ст. 273 УК РФ как использование и распространение вредоносных компьютерных программ, то есть распространение и использование компьютерных программ, заведомо предназначенных для несанкционированного копирования компьютерной информации и нейтрализации средств защиты компьютерной информации.»

(Приговор от 22.10.2024 №1—333/2024)

Самая большая опасность для пентестеров – это обвинение по ст.273 УК РФ, просто за разработку собственных программных инструментов, используемых при проведении пентеста.

Для наступления уголовной ответственности достаточно заключение эксперта, что разработанная программа имеет признаки вредоносного программного обеспечения. Просто наличие на компьютере, можно даже не применять.

«С.П. создал и распространил компьютерную программу, заведомо предназначенную для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации и нейтрализации средств защиты компьютерной информации, совершенные из корыстной заинтересованности, при следующих обстоятельствах.

Так, С.П. действуя с возникшим умыслом на создание и распространение вредоносной компьютерной программы, из корыстной заинтересованности, ввиду обладания достаточными, самостоятельно приобретенными познаниями и практическими навыками в области компьютерной информации, и работы с компьютерным обеспечением, с помощью принадлежащей ему персональной электронно-вычислительной машины, находясь по месту своего жительства, по адресу, пришкал на интернет – ресурсе пришкал утилиты программного обеспечения «Arachni scanner», осуществляющие поиск уязвимости на WEB-ресурсах, и действуя в указанный период времени во исполнение своего преступного умысла, находясь по указанному адресу, используя вышеуказанные утилиты программного обеспечения «SQLMap» и «Arachni scanner», при помощи языка программирования "<данные изъяты>», создал вредоносную компьютерную программу, предназначенную для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации и нейтрализации средств защиты компьютерной информации, заведомо зная о ее вредоносности, наименовав ее "<данные изъяты> 0», которая в соответствии с заключением эксперта N от ДД. ММ. ГГГГ, может быть использована для неправомерного доступа к компьютерной информации, ее уничтожения, блокирования, модификации либо копирования и нейтрализации средств защиты компьютерной информации.

С.П. признать виновным в совершении преступления, предусмотренного ч. 2 ст. 273 Уголовного кодекса Российской Федерации и назначить наказание в виде лишения свободы на срок два года со штрафом в размере 100 000 (сто тысяч) рублей, с отбыванием наказания в исправительной колонии строгого режима.»

(Приговор от 19.09.2022 №1—207/2022)

А вот так это выглядело глазами обвиняемого

«данная программа не является вредоносной программой, а является программой для тестирования сайтов с помощью которой можно выявить уязвимость сайтов. Пояснил, что им была создана оболочка вокруг данной программы, позволяющая полностью автоматизировать процесс, поскольку сама по себе программа является консольной, поэтому ей пользоваться не удобно, в связи с чем он сделал интерфейс к этой программе для удобства. Сама

программа предназначена для автоматизирования тестирования сайтов на проникновение. Данная программа не является заведомо для уничтожения, копирования и тому подобное, она заведомо предназначена для тестирования, что подтверждается ее официальным сайтом и входит во все операционные системы линокс и поставляется вместе с ними. С заключением эксперта он не согласен, поскольку у данной программы есть официальный сайт, торговый знак и официальное лицензионное соглашение, которым разрешено право на ее распространение и использование при определенных условиях. В справке специалист О. дал описание команд полностью исказив все справки. Атакующего режима у программы не имеется. При работе с данной программой сайт как работал, так и работает, даже никто и не заметит, что работает данная программа, то есть она блокирует и не модифицирует. Программа дает полную информацию, при этом если программа находит какой-то адрес, который подтвержден SQL-инъекцией, то она дает полную характеристику, описание, методы проникновения и методы исправления этой ошибки. Вместе с тем, если это злоумышленник, то он, используя эту информацию, может ей воспользоваться, но если тестировщик, то он естественно исправляет. Сам он данную программу не использовал, а лишь тестировал на сайтах "<данные изъяты>», где дается разрешение на тестирование. После тестирования результат всегда был положительный и данные сайты не блокировались после использования данного программного обеспечения, поскольку сайты ее даже не замечали, но программа показывал свою работоспособность. В программу встроен браузер, при этом сама программа не вредоносная, а вредоносными являются действия человека при использовании данной программы, но он таких действий не совершал.

Функционал данной программы заключался в том, что с помощью графической оболочки запускается перечень сайтов, необходимый для тестирования, а созданная им (С.П.) оболочка передает адреса данных сайтов сначала "<данные изъяты>», который сканирует их, определяет все адреса, выявляет среди них то, которые имеют уязвимость, и ссылку с уязвимостью передает в <данные изъяты>», которая проводит полный анализ этой уязвимости и делает полный отчет проведенной работы.»

Но суд посчитал, что «*Доводы подсудимого и стороны защиты о том, что созданное С.П. программное обеспечение „WASP 1.0“, не является вредоносными, опровергаются исследованными судом доказательствами, в том числе и заключением эксперта*.» и пентестер получил очень серьезное наказание – несколько лет колонии строго режима. Попытки обжаловать приговор безуспешны.

«*Подсудимый Ж. виновным себя не признал, пояснив, что работает программистом, имеет высшее профессиональное образование в области информатизации, с 2016 г. работал в компании «…», по заданию которой с целью проведения тестирования на проникновение разрабатывал ПО «…», включающий в себя программы «BeaconDNS», «beacon_dns-admin», «dns-bot-js», предназначенные для удаленного управления, этот комплекс не может несанкционированно производить какие-либо действия, а программа «dns-bot-js» запускается открыто через командную строку, что может быть осуществлено только продвинутым пользователем; файлы tinymet. x64.dll, tinymet. x86.dll не создавал, они были переданы ему работодателем, скачал из сети Интернет, их функциональное назначение состоит в скачивании и запуске программы, им был создан файл «питон», а файлы tinymet. x64.dll, tinymet. x86.dll не изменялись им. Полагает, что выводы эксперта несостоятельны. Оказал содействие оперативному сотруднику, добровольно предоставив коды от компьютерной техники «…", давал объяснения.*

Согласно заключению специалиста от 21.08.2020 г.

Программы из папок «…» и «…» являются модифицированными программными комплексами «…», предназначенными для разработки и применения эксплойтов, содержит большой набор готовых вспомогательных утилит, эксплойтов и «полезных нагрузок», позво-

ляющих находить и эксплуатировать уязвимости в вычислительных системах. Несмотря на предназначение комплекса для использования в рамках тестирования защищенности, в частности, в тестах на проникновение, данный комплекс пользуется популярностью у злоумышленников для получения несанкционированного доступа.

Утверждения защитника о том, что созданные Ж. программы «BeaconDNS», «beacon_dns_admin», «dns-bot-js» не являются вредоносными, а представляют собой аналог легальных программ для тестирования на проникновение «…», «…», созданы по заданию работодателя, оказывающего услуги в сфере разработки программного обеспечения по защите информации, а потому эти программы не могут нейтрализовать средства защиты, несанкционированно копировать информацию с удаленного компьютера, не могут быть установлены на нем без ведома пользователя, поскольку для этого требуется создание дополнительной программы, чего не делал Ж., проверены в ходе судебного следствия и не нашли своего подтверждения.

Факты принадлежности Ж. ноутбука «…» с N… и создания им программного обеспечения «BeaconDNS», «beacon_dns_admin», «dns-bot-js» сторона защиты не отрицает.

приговорил:

Ж. признать виновным в совершении преступления, предусмотренного ч. 1 ст. 273 УК РФ, и назначить наказание с применением ст. 64 УК РФ в виде лишения свободы на срок 1 год.»

(Приговор от 29.10.2021 по делу №1—23/2021)

Да, сейчас есть разъяснения Пленума Верховного суда, которые направлены на снижение такого риска, но ими еще необходимо суметь воспользоваться

«*Следует иметь в виду, что не образует состава преступления использование такой программы или информации лицом на принадлежащих ему компьютерных устройствах либо с согласия собственника компьютерного устройства, не преследующее цели неправомерного доступа к охраняемой законом компьютерной информации и не повлекшее несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств ее защиты (например, в образовательных целях либо в ходе тестирования компьютерных систем для проверки уязвимости средств защиты компьютерной информации, к которым у данного лица имеется правомерный доступ), равно как и создание подобных программ для указанных целей.*»

(Постановление Пленума Верховного Суда РФ от 15.12.2022 №37

«О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»)

Сканирование уязвимостей

Сфера деятельности, обязательная по нормативным документам ИБ, активно развивается, профессионально интересная. Основная проблема при уголовном преследовании – хакеры и специалисты ИБ используют одни и те же инструменты, что и порождает высокие риски наступления уголовной ответственности для специалистов ИБ и студентов.

«*Установлено, что 01.03.2023 в период с 12:18 часов до 13:17 часов (по Московскому времени) М.С., находясь у себя дома по адресу: <адрес>, действуя умышленно, с целью проверки своих навыков по использованию программного обеспечения, достоверно зная, что ресурс <данные изъяты>, имеющий доменное имя "<данные изъяты>" с IP-адресом N, входит в информационно-телекоммуникационную сеть Университета, то есть относится к объектам критической информационной инфраструктуры, на мобильном телефоне марки "<данные изъяты>" открыл цифровое окно свободно распространяемого в сети "<данные изъяты> «ПО» <данные изъяты>», предназначенного для проведения сетевого аудита безопасности информационных ресурсов, в том числе в открытых телекоммуникационных сетях, ранее установленного на указанный мобильный телефон, и внес в него данные электронного адреса Университета "<данные изъяты>». После чего М.С. запустил указанное программное обеспечение с применением дополнительных скриптов (» <данные изъяты>»), осуществив использование данного программного обеспечения с целью проверки наличия на сайте "<данные изъяты>" уязвимостей.*

Согласно заключению специалиста УФСБ России по <адрес> от 19.05.2023 на мобильном телефоне марки "<данные изъяты>" IMEI1: N, обнаружены следы размещения программного обеспечения "<данные изъяты>"; согласно сведениям, представленным в дампе трафика, установлено применение программного обеспечения "<данные изъяты>" для сканирования информационного ресурса "<данные изъяты>" Университета.»

(Приговор от 19.01.2024 по делу №1—21/2024)

С государственного IT особый спрос

Важный момент, состав преступления в форме подлога документов (внесение информации в ГИС), превышении должностных полномочий, нецелевое расходование бюджетных средств, халатности приведены в УК РФ в главе Глава 30. «Преступления против государственной власти, интересов государственной службы и службы в органах местного самоуправления» – это означает, что работники коммерческих организаций не привлекаются по ней.

А вот руководители ИТ-подразделений, цифровой трансформации, защиты информации (информационной безопасности/ безопасности КИИ) и аналогичных должны учитывать высокий риск привлечения к уголовной ответственности именно по этим статьям УК РФ.

Сейчас опишем потенциально опасные ситуации для государственного (бюджетного) ИТ специалиста при выполнении требований информационной безопасности, чтобы остаться в канве повествования о компьютерных преступлениях. То есть, какие обвинения можно получить при выполнении работ по защите информации.

Сначала разберемся кому это угрожает:

«*Должностными лицами в статьях настоящей главы признаются лица, постоянно, временно или по специальному полномочию осуществляющие функции представителя власти либо выполняющие организационно-распорядительные, административно-хозяйственные функции в государственных органах, органах местного самоуправления, государственных и муниципальных учреждениях, государственных внебюджетных фондах, государственных корпорациях, государственных компаниях, публично-правовых компаниях, на государственных и муниципальных унитарных предприятиях, в хозяйственных обществах, в высшем органе управления которых Российская Федерация, субъект Российской Федерации или муниципальное образование имеет право прямо или косвенно (через подконтрольных им лиц) распоряжаться более чем пятьюдесятью процентами голосов либо в которых Российская Федерация, субъект Российской Федерации или муниципальное образование имеет право назначать (избирать) единоличный исполнительный орган и (или) более пятидесяти процентов состава коллегиального органа управления, в акционерных обществах, в отношении которых используется специальное право на участие Российской Федерации, субъектов Российской Федерации или муниципальных образований в управлении такими акционерными обществами („золотая акция“), а также в Вооруженных Силах Российской Федерации, других войсках и воинских формированиях Российской Федерации.* »

Начнем с халатности, как наиболее характерного преступления именно по смыслу нашего исследования – не имел преступных намерений и оказался на скамье подсудимых.

Описание состава преступления «Халатность» очень похоже на «злоупотребление» и «превышение». А главное отличие при квалификации по халатности – небрежность в работе, то есть, халатно – это когда не осторожно.

Самонадеянно рассчитывал на то, что последствия от его действий не наступят либо им или иными лицами последствия будут предотвращены, либо не предвидел последствий, хотя должно было и могло их предвидеть.

Подозреваемый не имел умысла, он не хотел наступления последствий.

А вот превысить или злоупотребить своими полномочиями можно только умышленно и осознанно.

Или, по простому, халатность = и так сойдет! = авось!

Ст.293 УК РФ

«*Халатность, то есть неисполнение или ненадлежащее исполнение должностным лицом своих обязанностей вследствие недобросовестного или небрежного отношения к службе либо обязанностей по должности, если это повлекло причинение крупного ущерба*

или существенное нарушение прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства

Крупным ущербом в настоящей статье признается ущерб, сумма которого превышает один миллион пятьсот тысяч рублей, а особо крупным – семь миллионов пятьсот тысяч рублей.»

Создал информационную систему и не провел ее аттестацию – наказан.

«З*., являясь должностным лицом – руководителем Агентства связи и массовых коммуникаций Астраханской области, на которую в силу должностного регламента возложена персональная ответственность за реализацию программы «Внедрение спутниковых навигационных технологий с использованием системы ФИО9 и других результатов космической деятельности в интересах социально-экономического и инновационного развития Астраханской области в 2012—2016 годах», а также эффективное использование финансовых средств, в период с 18 августа 2011 г. по 31 декабря 2014 г. не проконтролировала деятельность исполнителей государственной программы, ввиду чего не обеспечила реализацию тех мероприятий, которые бы обеспечили возможность использования и эксплуатацию РНИС в соответствии с ее целями и задачами, ввиду чего надлежащим образом права на использование и эксплуатацию РНИС Астраханской области не оформлены, требования о защите информации, включая проведение аттестации РНИС Астраханской области в соответствии с программой и методиками аттестационных испытаний, заключение о соответствии с программой и методиками аттестационных испытаний, заключение о соответствии указанной информационной системы требованиям о защите информации, аттестат соответствия не получен..*

признана виновной в совершении преступления, предусмотренного частью 1 статьи 293 Уголовного кодекса Российской Федерации – халатность, то есть ненадлежащее исполнение должностным лицом своих обязанностей вследствие недобросовестного отношения к службе, если это повлекло причинение крупного ущерба и существенное нарушение прав и законных интересов граждан и охраняемых законом интересов общества и государства. »

(Решение от 09.09.2024 по делу №2—4236/2024)

Достаточно широкая практика квалификации «превышение служебных полномочий». Иногда самостоятельное обвинение, иногда в дополнение к классическим компьютерным преступлениям.

«*Признавая вину фио установленной в полном объеме и подтвержденной собранными по делу доказательствами, суд квалифицирует его действия по ч.3 ст.272 УК РФ, как неправомерный доступ к компьютерной информации, то есть неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло копирование компьютерной информации, совершенное из корыстной заинтересованности, с использованием своего служебного положения.*

Его же (фио) действия суд квалифицирует по ч.1 ст.286 УК РФ как превышение должностных полномочий, то есть совершение должностным лицом действий, явно выходящих за пределы его полномочий и повлекших существенное нарушение прав и законных интересов граждан и охраняемых законом интересов общества или государства. »

(Приговор от 14.04.2022 №1—363/22)

Для государственного ИТ характерны возможные последствия от нарушения работы информационных систем с серьезным масштабом и социально отягощенные, а так же высокий уровень стоимости госконтрактов.

«*Под тяжкими последствиями как квалифицирующим признаком преступления, предусмотренным частью 3 статьи 285, пунктом „б“ части 2 статьи 285.4 и пунктом „в“ части 3 статьи 286 УК РФ, следует понимать последствия совершения преступления в виде крупных аварий и длительной остановки транспорта или производственного процесса, иного нарушения деятельности организации, причинение значительного материального ущерба, причине-*

ние смерти по неосторожности, самоубийство или покушение на самоубийство потерпевшего и т.п.»

(Постановление Пленума Верховного Суда РФ от 16.10.2009 №19 «О судебной практике по делам о злоупотреблении должностными полномочиями и о превышении должностных полномочий»)

Принял работы по аттестации информационной системы, выполненные «для получения бумажки», – наказан.

«*В период времени с ДД. ММ. ГГГГ по ДД. ММ. ГГГГ, более точная дата и время в ходе предварительного следствия не установлены, у ФИО1, находящегося в неустановленном месте на территории Республики Потерпевший N 1, возник преступный умысел, направленный на превышение должностных полномочий в рамках государственного Контракта, то есть совершение должностным лицом действий, явно выходящих за пределы его полномочий и влекущих существенное нарушение прав и законных интересов граждан, охраняемых законом интересов общества и государства, с причинением тяжких последствий.*

ДД. ММ. ГГГГ, более точное время органом предварительного следствия не установлено, ФИО1, находясь по адресу: <адрес>, реализуя указанный преступный умысел, осознавая общественную опасность своих действий, предвидя возможность наступления общественно опасных последствий, а именно существенного нарушения прав и законных интересов граждан в виде незащищенности персональных данных работников исполнительных органов государственной власти Республики Крым, охраняемых законом интересов общества и государства в виде неработоспособности системы защиты конфиденциальной информации исполнительных органов государственной власти Республики Крым, безразлично относясь к заданным результатам обеспечения государственных и муниципальных нужд, выполнению условий Контракта и расходованию бюджетных денежных средств, допуская наступление тяжких последствий в виде значительного материального ущерба.

достоверно зная, что по состоянию на ДД. ММ. ГГГГ ЦОД РК не аттестован по требованиям безопасности информации, работы по 5 этапу Контракта не выполнены, в связи с чем аттестовать систему защиты информации государственной информационной системы ЕЦСВБУ по требованиям защиты информации невозможно, подготовил экспертное заключение по результатам проведения экспертизы оказанных услуг, предусмотренных Контрактом по 6 этапу, согласно которому установил факт соответствия проведенных работ по аттестации системы по требованиям защиты информации техническому заданию, а также нормативным и методическим документам ФСТЭК России, которое представил в приемочную комиссию Министерства финансов Республики

При указанных обстоятельствах, заместитель заведующего отделом информационных технологий Министерства финансов Республики Крым ФИО1, являясь должностным лицом Министерства, на которое были возложены дополнительные обязанности по проведению экспертизы отдельных этапов исполнения Контракта, совершил действия, явно выходящие за пределы его полномочий, повлекшие существенное нарушение прав и законных интересов граждан в виде незащищенности персональных данных работников исполнительных органов государственной власти Республики Крым, охраняемых законом интересов общества и государства в виде неработоспособности системы защиты конфиденциальной информации исполнительных органов государственной власти Республики Крым, неэффективности осуществления государственной закупки, повлекшей существенное нарушение основных принципов контрактной системы в сфере закупок, предусмотренных ст. 6 ФЗ N, подрыва авторитета государственного органа в виду нарушений

приговорил:

ФИО1 признать виновным в совершении преступления, предусмотренного п. «в» ч. 3 ст. 286 УК Российской Федерации.

Назначить ФИО1 наказание по п. «в» ч. 3 ст. 286 УК Российской Федерации – 4 года лишения свободы с лишением права занимать на государственной гражданской службе должности, связанные с выполнением организационно-распорядительных функций, сроком на 2 года.»

(Приговор от 12.09.2024 №1—18/2024)

Необходимо помнить, что обвинения по статьям о злоупотреблении должностными полномочиями может коснуться руководителей ИТ подразделений и не в бюджетных организациях.

«*Подсудимый Г. Д. А. совершил злоупотребление должностными полномочиями, то есть использование должностным лицом своих служебных полномочий вопреки интересам службы, если это деяние совершено из корыстной заинтересованности и повлекло существенное нарушение прав и законных интересов организаций и охраняемых законом интересов государства, повлекшее тяжкие последствия.*

Г.Д.А., в период с 24 апреля 2020 года по 10 января 2022 года, являлся на основании приказа генерального директора ООО «РТ-Капитал» N 30-лс от 24 апреля 2020 года руководителем направления информационных технологий Административного департамента ООО «РТ-Капитал» ИНН <…>, учредителем которого с долей в размере 85.7786% является Государственная корпорация по содействию разработке, производству и экспорту высокотехнологичной промышленной продукции «Ростех» желая избежать наступления негативных последствий в виде возможных дисциплинарных взысканий вследствие неоконченной реализации по договору № РТК-151-21, а также желая повысить уровень KPI (Кипиай – ключевые показатели эффективности), за соответствующий уровень которого полагается годовая премия в размере 40% от суммы окладов за год, сформировал преступный умысел, направленный на злоупотребление должностными полномочиями, то есть использование должностным лицом своих служебных полномочий вопреки интересам службы, если это деяние совершено из корыстной заинтересованности и повлекло существенное нарушение прав и законных интересов организаций и охраняемых законом интересов государства, повлекшее тяжкие последствия.

В результате совершения Г. Д. А. злоупотребления должностными полномочиями, существенно нарушены права и интересы ООО «РТ-Капитал» и государства, выражающиеся в отсутствии возможности введения в организации системы электронного документооборота и долгосрочного хранения данных, что в свою очередь, позволило бы государственной организации укрепить уровень безопасности информационного модуля и поддерживать его на надлежащем уровне с иными государственными структурами, а также его действия повлекли тяжкие последствия, выразившиеся, кроме вышеуказанного, также в причинении ООО «РТ-Капитал» материального ущерба в размере сумма со стороны ООО «Авинтел»..

Признать Г. … виновным в совершении преступления, предусмотренного ч. 3 ст. 285 УК РФ, и назначить ему наказание в виде лишения свободы сроком на 4 (четыре) года, с лишением права заниматься деятельностью, связанной с выполнением организационно-распорядительных функций в государственных корпорациях и в хозяйственных обществах, в высшем органе управления которых Российская Федерация имеет право прямо или косвенно (через подконтрольных лиц) распоряжаться более чем пятьюдесятью процентами голосов, сроком на 2 (два) года, с отбыванием наказания в виде лишения свободы в исправительной колонии общего режима.»

(Приговор от 28.08.2024 №01—0057/2024)

Нарушил процедуру приемки в эксплуатацию информационной системы, включая проверку подсистемы защиты информации, – наказан.

«Таким образом, Ш., в соответствии с занимаемой должностью заместителя директора – начальника отдела обеспечения цифровой трансформации

Ш. совершил действия, которые никто и ни при каких обстоятельствах не вправе совершать. Между <данные изъяты> и ООО "<данные изъяты> был заключен контракт по внедрению и сопровождению медицинской информационной подсистемы Регионального фрагмента Единой государственной информационной системы в сфере здравоохранения Ульяновской области, предназначенной для автоматизации контроля движения лекарственных препаратов и медицинских изделий в медицинских организациях, подведомственных Министерству здравоохранения Ульяновской области.

Ш. совершил действия, которые никто и ни при каких обстоятельствах не вправе совершать. Между <данные изъяты> и ООО <данные изъяты> был заключен контракт по внедрению и сопровождению медицинской информационной подсистемы Регионального фрагмента Единой государственной информационной системы в сфере здравоохранения Ульяновской области, предназначенной для автоматизации контроля движения лекарственных препаратов и медицинских изделий в медицинских организациях, подведомственных Министерству здравоохранения Ульяновской области.

Ш., достоверно зная, что приемка результатов исполнения контракта должна осуществляться приемочной комиссией, с проведением экспертизы результатов исполнения в части их соответствия условиям контракта, превысив свои должностные полномочия, не созвал приемочную комиссию, не провел экспертизу на предмет соответствия результатов исполнения контракта. Без созыва приемочной комиссии, принял участие посредством ВКС в совещании с ООО <данные изъяты> в ходе которого без проведения проверки соответствия результатов оказанных услуг, осуществил визуальный поверхностный осмотр демонстрации 3 этапа по контракту. Не убедившись, что работы по 3 этапу контракта выполнены в полном объеме, осознавая, что его действия выходят за пределы его должностных полномочий, превышая свои должностные полномочия по приемке работ и распоряжению бюджетными денежными средствами, единолично подписал акт приемки-передачи оказанных услуг, необоснованно указав, что работы по 3 этапу выполнены.

Не убедившись, что работы по 3 этапу контракта выполнены в полном объеме, осознавая, что его действия выходят за пределы его должностных полномочий, превышая свои должностные полномочия по приемке работ и распоряжению бюджетными денежными средствами, единолично подписал акт приемки-передачи оказанных услуг, необоснованно указав, что работы по 3 этапу выполнены.

Действия Ш. способствовали совершению хищения бюджетных денежных средств, принадлежащих <данные изъяты> учрежденному Министерством здравоохранения Ульяновской области в размере 1 450 000 рублей и существенно нарушили охраняемые законом интересы общества и государства в сфере отношений, направленных на обеспечение государственных и муниципальных нужд в целях повышения эффективности, результативности закупок товаров, работ, услуг.

приговорил:

Признать Ш. ФИО66 виновным в совершении преступления, предусмотренного ч. 1 ст. 286 УК РФ и назначить ему наказание в виде штрафа в размере 50 000 рублей.»

(Приговор от 18.09.2024 по делу №1—189/2024)

Но самое распространенное обвинение для «цифровых спецназовцев» -это либо нецелевое использование бюджетных средств, либо мошенничество.

Завысили категорию значимости значимого объекта КИИ/класса ГИС/уровня защищенности ИСПДн и как следствие создали более сложную и дорогую систему защиты информации, хотя могли обеспечить соответствие требованиям законодательства с меньшим расходом бюджетных средств?

Закупили более дорогие средства криптографической защиты информации, чем обоснованы в модели угроз?

Закупили избыточные средства защиты информации, не направленных на нейтрализацию актуальных угроз, описанных в модели угроз?

Тратите бюджетные деньги на текущую эксплуатацию ГИС без аттестата соответствия требованиям по защите информации?

Это все повышает риски привлечения к уголовной ответственности по статьям УК РФ Статья 160. «Присвоение или растрата» и Статья 285.1. «Нецелевое расходование бюджетных средств».

Под статью 159. «Мошенничество» УК РФ попасть еще легче, она фактически «народная» для ГосИТ.

Обвинения в «завышенной стоимости», «завышенных объемов работ», «несоответствие требованиям госконтракта разработанного программного обеспечения» и т. д. К сожалению, сфера информационных технологий во многом носит виртуальный характер и для обоснования любого обвинения достаточно получить заключение экспертизы, носящего сугубо субъективный характер.

На низовом уровне, самый распространенный преступный сценарий – выполнение части работ по госконтракту силами заказчика на подряде у исполнителя.

Для примера, по госконтракту подрядчик должен проложить слаботочную сеть, установить и настроить сетевое оборудование – создать СКУД, противопожарную сигнализацию, локально-вычислительную сеть и тому подобное. Распространенная ситуация, когда на монтажные работы по договору ГПХ подрядчик нанимает местных связистов и сисадминов (работников заказчика).

Все довольны – подрядчику не пришлось искать квалифицированных работников, связисты получили дополнительные деньги к зарплате и качество работ на высоте – исполнители делали для себя, им дальше эксплуатировать созданное.

Но вот как раз круговорот денег: заказчик-подрядчик-работник заказчика и приводит к массе уголовных дел, в которых осуждают: и руководителя подрядчика и руководителя заказчика и работяг.

Пиратское ПО: экономия со сроком

Программы с торрентов – классика «офисного фольклора».

Вроде бы – мелочь. На деле – уголовно наказуемое деяние.

По ст. 146 УК РФ (нарушение авторских прав) можно получить до 2 лет лишения свободы, если доказан ущерб правообладателю. А, если использовать специальные программы-активаторы, то формируется дополнительный состав компьютерного преступления по ст. 273 УК РФ.

И тогда размер ущерба или отсутствие претензий от правообладателей программного обеспечения уже не важны. Достаточно самого факта использования таких программ.

«у ФИО1 работающего ведущим инженером в <данные изъяты>», возник преступный умысел, направленный на незаконное использование объектов авторского права, а именно программного продукта «Microsoft Office Enterprise 2007» путем использования полезных свойств данного программного продукта в своей трудовой деятельности в ООО ВСЗ «Техника». При этом ФИО1, обладая познаниями в области компьютерной техники и компьютерных программ, навыками работы на персональных электронно-вычислительных машинах, был лично заинтересован в незаконном использовании контрафактного программного обеспечения в целях достижения положительных результатов в своей трудовой деятельности в ООО ВСЗ «Техника».

В целях реализации своего преступного умысла ФИО1 планировал использовать компьютерную информацию, содержащуюся в файле «Ключ. txt», заведомо предназначенную для перевода программного продукта «Microsoft Office Enterprise 2007» в полнофункциональный режим способом, не предусмотренным правообладателем. »

(Постановление от 29.07.2020 г. по делу №1—277/2020)

К сожалению, практика привлечения по данному составу преступления довольна обширна. Отсутствие корыстного умысла и какого-либо ущерба никак не влияет на судьбу специалиста ИТ.

«суду показал, что он работает инженером по эксплуатации и учету средств информационных технологий на ФКП «…», в связи с занимаемой должностью он был под роспись ознакомлен со своей должностной инструкцией и со Стандартом предприятия «Система…», также ему известно, что сеть ФКП «…» прокатегорирована и является объектом критической информационной инфраструктуры. В середине апреля 2020 года к нему обратилась сотрудница предприятия М., которая попросила его найти программу «Microsoft Office Word» для другой сотрудницы М.1. в целях использования и работы дома в период «удаленки» (карантина). Для скорейшего исполнения просьбы, он на своем рабочем компьютере в сети «Интернет» с неизвестного ему источника скачал программу «Microsoft Office Word» с программой-активатором, которые находились в одной папке. Признает, что, скачивая программу активатор, он знал, что эта программа предназначена для преодоления защиты продуктов компании «Microsoft» от несанкционированного использования, что любой активатор является программой для преодоления защиты, понимал, что он для не лицензионного использования. Открыв программу, он узнал, что программа-активатор – «…». Затем он запустил указанный активатор на рабочем компьютере для того, чтобы в случае возникновения вопросов от М.1. или М., он мог им ответить на них. После этого он скопировал папку с программой «Microsoft Office Word» и программой-активатором «…» на флешнакопитель, который передал М. Откуда появился флеш-накопитель он не помнит. При скачивании и открытии программы «Microsoft Office Word» совместно с программой-активатором «…» каких-либо уведомлений, сообщений от антивируса «…», установленного на его служебном компьютере,

не поступало. Сам он антивирус «…» не отключал, в исключение скаченные им программы не вносил.

– заключением программно-технической судебной экспертизы от ДД. ММ. ГГГГ, согласно выводам которого на носителе N в явном виде и на носителе N в удаленном виде обнаружена программа…, предназначенная для обхода системы защиты от несанкционированного копирования и распространения операционных систем производства компании «Microsoft» и пакета MS Office, широко известная в сети «Интернет» и имеющая много версий. Обнаруженная версия… относится к 2018 году. Назначение программы: произвести активацию вышеуказанных программных продуктов производства компании «Microsoft» без оплаты стоимости лицензии. На представленных носителях информации следов запуска программы… обнаружить не удалось

В судебном заседании установлено, что А.А., имея доступ к информационно-телекоммуникационной сети «Интернет» на ФКП «…», из неустановленного Интернет-ресурса на закрепленный за ним компьютер скачал программу «…», заведомо предназначенную для нейтрализации средств защиты компьютерной информации – операционных систем компании «Microsoft» и пакета «MS Office», которую в целях проверки работоспособности использовал путем запуска на компьютере, после чего скопировал на твердотельный накопитель, который передал через М.М.1., тем самым распространив вредоносную компьютерную программу.

Об умысле А.А. на совершение данного преступления свидетельствуют все обстоятельства дела, в том числе тот факт, что А.А., имеющий высшее профессиональное образование по направлению «Информатика и вычислительная техника», зная, что для использования программы «Microsoft» и пакета «MS Office» необходимо лицензионное разрешение, в целях нейтрализации средств защиты информации от несанкционированного доступа, скачал на компьютер программу-активатор «…», которую запустил и, скопировав на флеш-накопитель, передал его для М.1.

Оценив в совокупности собранные по делу доказательства, суд считает вину подсудимого доказанной полностью и квалифицирует его действия по ч. 1 ст. 273 УК РФ как распространение и использование компьютерной программы, заведомо предназначенной для нейтрализации средств защиты компьютерной информации.»

(Приговор от 07.07.2021 по делу №1—181/2021)

Бывают ситуации и хуже, специалисты ИТ устанавливают официально программы и/или программно-аппаратные комплексы, но по различным причинам нарушают лицензионные требования и даже не подозревает, что программа-активатор будет отнесена к вредоносному программному обеспечению, а он получит обвинения в совершении компьютерного преступления.

«В.А., будучи официальным партнером ООО «1С» и ООО «1С-СОФТ» на территории г. Новый Уренгой ЯНАО, был наделен согласно договору коммерческой концессии №58146—71 от 12.03.2020 г. и лицензионному договору №58146—71 от 12.03.2020 г., заключенными с ООО «СОФТЕХНО» – дочерней компанией ООО «1ССОФТ», правомочиями по участию в работе сети «1С: Франчайзинг» по предоставлению комплексных услуг по автоматизации учетных и управленческих задач на основе системы программ «1С: «Предприятие» путем осуществления помощи в выборе программного обеспечения, установке, настройке, внедрения, обслуживания, консультации, обучения пользователей программных продуктов, а также реализации программных продуктов системы «1С: Предприятие», распространения продуктов системы программ «1С: Предприятие», включая продукты, снабженные в прайс-листе пометкой «франчайзинговый ассортимент», за исключением продуктов особых компетенций, имея преступный, направленный на использование вредоносной компьютерной программы, заведомо предназначенной для несанкционированной нейтрализации технических

средств защиты компьютерной информации, с целью беспрепятственного запуска и использования программных продуктов ООО «1С-СОФТ».

Своими преступными действиями В.А. в период времени с 03.01.2021 г. По 05.04.2022 г. на ЭВМ, находящейся в ООО «Арт Групп», незаконно использовал вредоносную компьютерную программу «techsys. dll» с хеш-суммой SHA-1 9F06A9AFD400EB [суммы изъяты] B4131BF4F, с целью нейтрализации установленных правообладателем средств индивидуальной защиты компьютерной информации программного обеспечения «1С: Предприятие 8.3 Технологическая поставка, версия 8.3.19.1399», 1 экземпляр, «1С: Бухгалтерия 8. Проф, версия 3.0.106.60», 1 экземпляр, «1С: Зарплата и управление персоналом 8, версия 3.1.21.36», 1 экземпляр, правообладателя – ООО «1С-СОФТ». Действия В. А. по каждому из четырех преступлений квалифицированы по

ч. 1 ст. 273 УК РФ – использование компьютерных программ, заведомо предназначенных для нейтрализации средств защиты компьютерной информации.

(Постановление от 25.08. 2023 №1—355/2023)

А могут дополнительно и ст.272 УК РФ вменить

«*А.В., работая в качестве главного технолога АО «Камешковский механический завод», был лично заинтересован в незаконном использовании нелицензионного (контрафактного) программного обеспечения в целях достижения положительных результатов в коммерческой деятельности АО «Камешковский механический завод». В целях реализации своего преступного умысла А.В. планировал использовать способом, не предусмотренным правообладателем, компьютерную программу «Autodesk 2015 products» (xf-adsk2015_x64.exe), заведомо предназначенную для перевода программного продукта «Autodesk -AutoCAD 2015» в полнофункциональный режим, а также использовать инструкцию по незаконным установке и активации указанного программного продукта «readme. txt».*

Органом предварительного следствия, А.В. предъявлено обвинение в совершении преступлений, предусмотренных ч. 2 ст. 146 УК РФ – незаконном использовании объектов авторского права, совершенном в крупном размере; ч.1 ст. 272 УК РФ (2 преступления) – двух эпизодов неправомерного доступа к охраняемой законом компьютерной информации, если это деяние повлекло блокирование компьютерной информации; ч.1 ст. 273 УК РФ (2 преступления) – двух эпизодов использования компьютерной программы и иной компьютерной информации, заведомо предназначенных для несанкционированной нейтрализации средств защиты компьютерной информации»

(Постановление от 07.08.2019 №1—72/2019)

Особенно печально, когда для использования пиратского программного обеспечения используется привилегированный доступ системного администратора, позволяющий отключить средства защиты информации.

«*обвиняемого в совершении преступлений, предусмотренных ч. 1 ст. 272, ч. 1 ст. 273 УК РФ.*

А.В. в период с 09 часов 00 минут 14 февраля 2020 года до 18 часов 00 минут 08 июля 2022 года, находясь на своем рабочем месте, в кабинете № здания <данные изъяты>, находящемся по адресу: <адрес>, во время исполнения своих обязанностей имея преступный умысел, направленный на изменение (модификацию) компьютерной информации в ПЭВМ «IntelCore 2 DuoE4500220» № (настроек средств защиты от несанкционированного доступа «SecretNet»,) предназначенным для обработки информации с ограниченной пометкой – ДСП, для возможности беспрепятственно подключать любой носитель информации для осуществления на указанной ПЭВМ бесконтрольной установки программного обеспечения, осознавая общественную опасность своих действий, предвидя неизбежность наступления общественно опасных последствий и желая их наступления, то есть с прямым умыслом не имея на то законных оснований осуществил вход в операционную систему служебного ПЭВМ «IntelCore

2 DuoE4500220» № под правами администратора на служебной ПЭВМ №, изменив настройки средства защиты информации «SecretNet» с целью доступа к устройствам USB, в результате внесенных изменений (модификаций) компьютерной информации (настроек средств защиты информации от несанкционированного доступа «SecretNet») стало возможным беспрепятственно подключать любой носитель информации, далее действуя в продолжении реализации преступного умысла в нарушение п.18 Руководства подключил свой личный USB-накопитель информации к указанному ПЭВМ и осуществил установку заранее приисканного и скопированного им же ранее в сети интернет вредоносного файла «Keygen. exe» не входящего в перечень программных средств, допускаемых к установке на автоматизированных рабочих местах.

То есть, осуществил неправомерный доступ к охраняемой законом компьютерной информации, повлекшей модификацию компьютерной информации. »

(Постановление от 22.05.2023 №1—772/2023)

Майнинг

Обговорим сразу, что разговор пойдет не только про самовольную установку «майнера» на рабочий компьютер, здесь все очевидно – минимум ст. 273 УК РФ (все экспертизы признают «майнер» вредоносным программным обеспечением):

«*согласно заключению специалиста.. определяется антивирусным программным обеспечением «Kaspersky Endpoint Security 11.1.1.126» [Касперский Интпоинт Секьюрити] как вредоносное: «HEUR: «Trojan.Win32.Miner.gen» [ХАЯ: Троян. Вин32.Майне. джен], способное скрытно использовать вычислительную мощность ЭВМ, на которой оно исполняется, путем ее утилизации для решения вычислительных задач в соответствии с заданным алгоритмом, в том числе алгоритмом для майнинга криптовалюты Ethereum [Эсериум]*

Признать Д. виновным в совершении преступления, предусмотренного ч. 2 ст. 273 Уголовного кодекса Российской Федерации, и назначить ему наказание в виде принудительных работ на срок 2 (два) месяца с удержанием 5 (пяти) процентов заработной платы осуждённого в доход государства, с отбыванием в местах, определяемых учреждениями и органами уголовно-исполнительной системы.»

(Приговор от 25.10.2022 №1—451/2022)

Если «майнить» на критической информационной инфраструктуре, то осудят по ч.1 ст. 274.1 УК РФ, что вполне логично. Вот пример с излишне инициативным системным администратором предприятия ОПК

«*ФИО2 совершил создание и использование компьютерной программы, заведомо предназначенной для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации.*

ПРИГОВОРИЛ:

Признать ФИО2 виновным в совершении преступления, предусмотренного ч. 1 ст. 274.1 УК РФ и назначить ему наказание в виде лишения свободы сроком на два года и штрафа в 500 тысяч рублей»

(Приговор от 07.12.2022 №1—476/2022)

Могут добавить квалификацию по ст.272 УК РФ или по ст.274 УК РФ.

Самый показательный пример – это, конечно, начальник вычислительной лаборатории федерального ядерного центра в Арзамас-16, который организовал «майнинг» на суперЭВМ с вычислительной мощностью более 1 ТФлоп/с.

«*В период.. лицо N 1 и лицо N 2, находясь в ИТМФ, расположенном по адресу:…, …, действуя умышленно, из корыстной заинтересованности, обладая специальными познаниями в сфере компьютерной техники, заведомо зная о действующих во ФГУП «РФЯЦ-ВНИИЭФ» правилах доступа к охраняемой законом компьютерной информации, договорились об использовании вычислительных мощностей находящегося в ИТМФ неиспользуемого компьютерного оборудования и возможностей СЛВС, предназначенной для обработки конфиденциальной информации уровня конфиденциальности «для служебного пользования», «персональные данные» и «коммерческая тайна», для вычисления (майнинга) криптовалюты и ее последующего обращения в свою пользу, вопреки служебным интересам ФГУП «РФЯЦ-ВНИИЭФ.*

лицо N 1, находясь в ИТМФ, расположенном по адресу:…, действуя умышленно, из корыстной заинтересованности, выполняя свою роль в совершаемом преступлении, используя свое служебное положение начальника научно-исследовательского отдела – начальника научно исследовательской лаборатории научно-исследовательского отделения вычислительной математики ИТМФ, пришкал необходимое для организации вычислений (майнинга) криптовалюты оборудование, – имеющийся в ИТМФ и незадействованный в работе коммутатор

«Ethernet», несколько имеющихся в ИТМФ и незадействованных в работе серверов, а также GSM-модем, – которое предоставил Б.Д.

убедившись в работоспособности собранной «фермы», с целью создания условий для увеличения прибыли от вычисления (майнинга) криптовалюты, продолжая реализацию совместного преступного умысла, лицо N 2, действуя умышленно и согласованно с лицом N 1 и Б.Д., группой лиц по предварительному сговору с ними, под видом осуществления научно-исследовательских работ в интересах ИТМФ, получил на складе в здании № ИТМФ… ФГУП «РФЯЦ-ВНИИЭФ» несколько незадействованных в работе серверов, которые передал Б.Д.

используя свое служебное положение начальника научно-исследовательского отдела – начальника научно исследовательской лаборатории научно-исследовательского отделения вычислительной математики ИТМФ, под видом осуществления научно-исследовательских работ в интересах ИТМФ, получил от вышестоящего руководства ИТМФ разрешение на выделение электроэнергии и хладоснабжения, необходимого для вышеуказанного собранного Б.Д. вычислительного ресурса.

Таким образом, указанные действия лица N 1, лица N 2 и Б.Д. повлекли модификацию компьютерной информации, которая выразилась в генерации сетевого трафика в каналах СЛВС.

Кроме того, вышеуказанные действия лица N 1, лица N 2 и Б.Д. по нарушению установленных в ИТМФ правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации привели к нарушению условий действия аттестата соответствия на объект информатизации АСЗИ «СВС РФЯЦ-ВНИИЭФ» N от 29.07.2016, что, в соответствии с п. 7.3 ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения» повлекло необходимость в проведении внеочередной повторной аттестации АСЗИ «СВС РФЯЦ-ВНИИЭФ», сегментом которой является СЛВС ИТМФ, стоимость которой составила 1140157 (Один миллион сто сорок тысяч сто пятьдесят семь) рублей 10 копеек.

Таким образом, нарушение правил эксплуатации средств хранения, обработки и передачи охраняемой компьютерной информации, совершенное лицом N 1, лицом N 2 и Б.Д. вышеописанным способом, повлекло причинение ФГУП «РФЯЦ-ВНИИЭФ» крупного материального ущерба, составляющего 1140157 (Один миллион сто сорок тысяч сто пятьдесят семь) рублей 10 копеек.

Б.Д. признать виновным в совершении преступлений, предусмотренных ч. 3 ст. 272 и ч. 1 ст. 274 УК РФ»

(Приговор от 17.09.2019 №1—149/2019)

А, если еще пытаться скрыть следы своей преступной деятельности по «майнингу», то можно получить весь набор компьютерных статей УК РФ

*«В период с **** по **** заместитель начальника научно-исследовательского отдела – начальник научно-исследовательской лаборатории научно-исследовательского отделения вычислительной математики <данные изъяты> Ш. и начальник научно-исследовательской группы научно-исследовательского отдела научно-исследовательского отделения вычислительной математики <данные изъяты> – лицо N, находясь на своих рабочих местах в служебных кабинетах… систематически запускали процесс вычисления (майнинга) криптовалюты с использованием собранного ими вычислителя («фермы»), состоящего из сегмента <данные изъяты>, входящего в состав <данные изъяты> <данные изъяты>), предназначенной для хранения, обработки и передачи сведений, составляющих государственную тайну, до уровня «совершенно секретно», находящегося в здании…, а полученную в результате совершения преступления прибыль обращали в свою пользу.*

*В период с 01 по **** Ш. и лицо N, находясь в…, опасаясь раскрытия их противоправной деятельности другими сотрудниками <данные изъяты>, и возможного привлечения*

к уголовной ответственности, а также с целью устранения препятствий к незаконному получению прибыли от вычисления (майнинга) криптовалюты с использованием указанного оборудования <данные изъяты>, договорились о принятии мер по сокрытию запускаемых ими на <данные изъяты> нештатных процессов, в том числе процесса работы программного обеспечения (далее – ПО), предназначенного для вычисления (майнинга) криптовалюты. Для решения указанной задачи Ш. и лицо N приняли решение о создании и использовании компьютерной программы, заведомо предназначенной для нейтрализации средств защиты компьютерной информации, – версии программной закладки (программы) "<данные изъяты>" с функциями запуска процессов с привилегиями администратора и сокрытия пользовательских процессов. При этом указанные лица распределили свои роли в планируемом преступлении следующим образом. Лицо N приискивает в <данные изъяты> «Интернет» исходный код программы "<данные изъяты>», который предоставляет Ш. с инструкциями по его компиляции с целью создания на его основе версии программы "<данные изъяты>», пригодной для использования в оборудовании <данные изъяты>, и заведомо предназначенной для нейтрализации средств защиты компьютерной информации. Ш. и лицо N приискивают исходные коды ядра операционной системы, используемой на узлах <данные изъяты>, необходимые для компиляции (создания) программы "<данные изъяты>" из приисканных лицом N исходных кодов; Ш. на основании полученных от лица N инструкций, а также под контролем последнего, на основании предоставленного лицом N исходного кода программы "<данные изъяты>», а также приисканных ими исходных кодов ядра операционной системы, используемой на узлах <данные изъяты>, осуществляет компиляцию (создание) программы "<данные изъяты>», пригодной для использования на оборудовании (узлах) <данные изъяты>, и заведомо предназначенной для нейтрализации средств защиты компьютерной информации. Созданную указанным образом программу "<данные изъяты>" Ш. и лицо N запускают (используют) одновременно с процессом вычисления (майнинга) криптовалюты на узлах <данные изъяты> с целью сокрытия данного процесса от обнаружения иными сотрудниками <данные изъяты>.

Признать Ш. виновным в совершении преступлений, предусмотренных ч. 3 ст. 272, ч. 4 ст. 272, ч. 1 ст. 274, ч. 2 ст. 273 УК РФ»

(Приговор от 16.10.2019 по делу №1—166/2019)

Проблема даже не в обвинениях по компьютерным преступлениям, если принести на работу свою «майнинговую ферму» и никоим образом не осуществляли воздействий на рабочие информационные системы, все равно можно стать осужденным, но уже по экономической статье УК РФ.

Вот так это разъясняла прокуратура Тульской области в марте 2025 года

«*Под «майнингом» предполагается понимать выпуск цифровой валюты, то есть действия с использованием объектов российской информационной инфраструктуры и (или) пользовательского оборудования, размещенного на территории Российской Федерации.*

Цифровая валюта – это совокупность электронных данных (цифрового кода или обозначения), содержащихся в информационной системе, которые предлагаются и (или) могут быть приняты в качестве средства платежа (не являющегося денежной единицей какого-либо государства и (или) международной денежной или расчетной единицей) и (или) в качестве инвестиций.

Уголовная же ответственность за бездоговорное потребление электроэнергии может наступить по ст. 165 УК РФ «Причинение имущественного ущерба путем обмана или злоупотребления доверием при отсутствии признаков хищения».

За причинение ущерба от 250 тыс. руб., предусмотрено наказание в виде:

– штрафа в размере до 300 тыс. руб. или в размере дохода осужденного за период до 2 лет;

– принудительных работ на срок до 2 лет с ограничением свободы на срок до 1 года или без такового;

– лишения свободы на срок до 2 лет со штрафом в размере до 800 тыс. руб. или в размере дохода осужденного за период до 6 мес. или без такового и с ограничением свободы на срок до 1 года или без такового.

За совершение данного преступления группой лиц по предварительному сговору либо организованной группой, а также при ущербе от 1 млн. руб. предусмотрено наказание в виде:

– принудительных работ на срок до 5 лет с ограничением свободы на срок до 2 лет или без такового,

– лишения свободы на срок до 5 лет со штрафом в размере до 80 тыс. руб. или в размере заработной платы или иного дохода осужденного за период до 6 мес. или без такового и с ограничением свободы на срок до 2 лет или без такового.»

Электричество в рабочем помещении стоит денег и подключение «майнинговых ферм» расценивается как хищение денег работодателя, просто в форме электричества.

«*ВН было получено сообщение, что из локальной вычислительной сети (далее ЛВС) ИЛФ СО РАН регистрируется работа вредоносного программного обеспечения (ПО), включая фиксацию процесса майнинга.*

В ходе проведения проверки анализа работы компьютерной сети института информация подтвердилась, в связи с чем, по решению руководителя ИЛФ СО РАН была создана специальная комиссия.

Комиссия ИЛФ СО РАН в 10:20 в помещении N корпуса прочности института изъяла системные блоки в количестве 5 штук, с установленным ПО и видеокартами для майнинга.

В ходе проведенной проверки по информации, полученной из ФСБ России, было выявлено конкретное расположение компьютеров, на которых работало вредоносное ПО и производилась генерация криптовалюты (майнинг).

Как следует из пояснений ответчика, по результатам проверки жестких дисков было установлено, что на изъятых компьютерах действительно работало вредоносное ПО, перечисленное в уведомлении ФСБ России, а также все пять компьютеров применялись для генерации криптовалюты. Сведений составляющих гостайну, информации ограниченного доступа и ПО для хищения и передачи третьим лицам не обнаружено. Изъятое оборудование находится на хранении на складе института до решения руководства ИЛФ СО РАН, так как в процессе генерации криптовалюты указанные компьютеры длительное время (несколько лет) работали круглосуточно и потребляли электроэнергию, которая оплачивалась из бюджета института. Фактически за время майнинга криптовалюты было совершено хищение бюджетных средств института в размере нескольких сотен тысяч рублей.»

(Определение от 18.07.2023 г. по делу №2—507/2023)

А могут обвинить в злоупотреблении доверием – по ст. 165 УК РФ (причинение имущественного ущерба путём злоупотребления доверием)

«*имея доступ к помещению архива и техническому помещению, расположенным на 1 этаже в здании № ВРУ-3 на территории УГИБДД ГУ МВД России по <адрес> по адресу: <адрес>, ул. 6-й <адрес>, б/н, стр. 1, смонтировал, установил и подключил к электрической сети ГУ МВД России по <адрес> электротехническое оборудование – ASIC майнерWhatsminer M32 WhatsPower P222C P/N:P222C-GB-14-3300-C-V01, S/N: GB1355Z№, ASIC майнерWhatsminer M32 WhatsPower P222C P222C P/N:P222C-AR-14-3300-C-V01, S/N: AR4D204600995, а также Wi-Fi-роутер «Yota» B315 модель B315s-22 IMEI:№ с сим-картой YOTA 010 487 3096 и дополнительное электрооборудование – блок питания формата ATX «P/N 9PA400BA01, «S/N S5341051663», блок питания формата ATX «P/N 10PP300J2000N1, «S/N 66167056204515», блок бесперебойного питания ИБП IpponBackPowerPro 5, обеспечивающее работу указанных устройств, которые потребляли электрическую энергию, предназначенную*

для обеспечения работы подразделений ГУ МВД России по <адрес> и производили криптовалюту для сотрудника полиции ФИО1, который впоследствии смог бы обменять криптовалюту на деньги и иные материальные ценности.

Учитывая, что два устройства ASIC майнерWhatsminer M32 WhatsPower P222C ежемесячно расходовали электроэнергию 5 132,16 кВт/час, которая была оплачена ФКУ «Центр хозяйственного и сервисного обеспечения ГУ МВД России по <адрес>» в сумме 231 000 рублей, указанному учреждению причинен материальный ущерб в сумме 231 000 (двести тридцать одна тысяча) рублей со стороны сотрудника полиции ФИО1, который подключил и использовал вышеуказанные устройства в личных целях.

Указанные действия ФИО1 повлекли существенное нарушение прав и законных интересов организации и охраняемых законом интересов общества и государства, выразившихся в дискредитации правоохранительных органов перед обществом и государством, что подрывает доверие граждан к деятельности правоохранительных органов, а также ведет к подмене возложенной на правоохранительные органы функций по защите личности, общества, государства от противоправных посягательств, а также в причинении имущественного вреда организации – ФКУ «Центр хозяйственного и сервисного обеспечения ГУ МВД России по <адрес>» в вышеуказанном размере в результате незаконного подключения к электрической сети оборудования для производства криптовалюты

Конец ознакомительного фрагмента.