

Голубовский В.Ю., Кунц Е.В.

КИБЕРПРЕСТУПЛЕНИЯ: КРИМИНОЛОГИЧЕСКИЕ И ПРОЦЕССУАЛЬНЫЕ АСПЕКТЫ

Golubovsky V.Yu., Kunts E.V.

CYBERCRIMES: CRIMINOLOGICAL AND PROCEDURAL ASPECTS

Государственная политика Российской Федерации с учетом глобальных вызовов современности ориентирована на то, чтобы создать национальную систему безопасности со всеми присущими ей элементами, что предопределяет повышенное внимание к важнейшему её виду, информационной безопасности, без которой не может быть обеспечена национальная безопасность суверенитет.

В связи с бурным развитием информационных технологий, а также глобализацией информационных потоков, необходимо выявление угроз, способствующих совершению киберпреступлений, а также совершенствование уголовно-процессуального законодательства, которое позволяло оперативно расследовать преступления в сфере компьютерных технологий. Исследование обозначенных проблем положено в основу содержания настоящей статьи.

Ключевые слова: вредоносная программа, информационная безопасность, киберпреступления, национальная безопасность, расследование, угроза, хакер.

The state policy of the Russian Federation, taking into account the global challenges of our time, is focused on creating a national security system with all its inherent elements, which predetermines increased attention to its most important type, information security, without which national security and sovereignty cannot be ensured.

In connection with the rapid development of information technology, as well as the globalization of information flows, it is necessary to identify threats that contribute to the commission of cybercrimes, as well as improve criminal procedural legislation, which makes it possible to quickly investigate crimes in the field of computer technology. The study of the identified problems forms the basis for the content of this article.

Keywords: malware, information security, cybercrime, national security, investigation, threat, hacker.

52

Уголовно-правовые науки



За последние годы все чаще имеет место неправомерное вмешательство в компьютерную сеть Интернета. Подобное явление требует немедленного реагирования компетентных органов, чтобы не допустить увеличение числа преступных посягательств в этой сфере. Вирусную атаку компьютерных систем по сути дела можно сравнить с террористическими актами, в результате которой причиняется огромный ущерб пользователям Интернета. Террористы используют Интернет для ведения войн.

Можно предположить, что в недалеком будущем хакеры смогут свободно проникать в электронные системы, устанавливаемые в правительственных зданиях,

выдвигая при этом, политические или иные требования. В случае серьезных нарушений систем большая часть организаций может остаться без электричества, только незначительная часть потенциальных жертв, вероятно, может оказаться защищенной.

МВД Российской Федерации за 2023 год зарегистрировало 677 тыс. IT-преступлений в стране. В 2022 году МВД зафиксировало 522,1 тыс. таких преступлений, на треть меньше, чем в 2023 году. Удельный вес дел по таким правонарушениям увеличился с 26,5% до 34,8%. Выше половины зарегистрированных преступлений с использованием информационных технологий относится к катего-

риям тяжких и особо тяжких. Число преступлений с применением интернета выросло с 381 тыс. до 526,7 тыс. Далее идут преступления, совершённые с использованием средств мобильной связи и пластиковых карт. Выросло количество правонарушений с применением компьютерной техники, программных средств и фиктивных электронных платежей [1].

Имеющиеся в настоящее время у органов, осуществляющих предварительное расследование возможности противодействия этим угрозам как на национальном, так и международном уровне недостаточны для адекватного немедленного реагирования на возникшую опасную ситуацию. Одним из вариантов решения проблемы является наделение органов, осуществляющих уголовное преследование, более широкими полномочиями для осуществления противодействия киберпреступности.

Необходимо соблюдать последовательность этапов в области сотрудничества правоохранительных органов по розыску преступников и расследованию преступлений, связанных с Интернетом.

Киберпреступность отличается также высокой степенью анонимности преступника. Существующие на сегодняшний день VPN/VPS-сервисы для анонимизации трафика, виртуальные номера мобильных телефонов, криптовалютные кошельки (создание которых не требует внесения паспортных данных) обеспечивают лицу возможность практически полностью скрыть свою личность. Даже если следствию удастся идентифицировать, то или иное электронное устройство в качестве орудия совершения преступления, установить причастность конкретного лица к совершению (посредством данного устройства) преступления часто становится затруднительно [2].

Справедливо возникает вопрос относительно системы Интернет, насколько она, будучи ориентированной на национальные нормы уголовного права, сможет быть упорядочена так, чтобы отрицательно не повлиять на фундаментальные правовые стандарты. Проблема обеспечения безопасности и соблюдения прав граждан на свободу информации должна решаться не только на национальном, но и наднациональном уровне. Важно не допустить несоразмерной криминализации и чрезмерного контроля информационных связей Интернета.

Существует множество вариантов классификации угроз информационной безопасности. По объекту, на который направлены угрозы можно выделить следу-

ющие её виды: угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному развитию России; угрозы информационному обеспечению государственной политики России; угрозы развитию отечественной индустрии информации, включая производство средств информатизации, телекоммуникации и связи, обеспечения потребителей внутреннего рынка в её продукции и выхода этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов; угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развёрнутых, так и создаваемых на территории России.

Одной из распространённых угроз в информационной сфере является использование компьютерных вирусов с целью хищения (уничтожения, лишения доступа) базы данных у их обладателей.

Определение понятия «вредоносная программа» раскрывается в ст. 273 Уголовного Кодекса Российской Федерации, под которой понимается создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации [3]. Вирус, это самопроизводящийся программный код, который внедряется в установленные на устройстве программы без согласия пользователя [4, с. 376].

Наиболее распространённой вредоносной программой является компьютерный вирус под названием «червь» – она создана, для того, чтобы размножаться посредством различных гиперссылок и используется в атаках на компьютерные системы, создавая киберугрозы обладателям информации. Данная программа заражает различные файлы, флэш-накопители и компьютеры, через которые может передаваться на другие носители информации. Так называемый червь, который проник в вышеуказанные накопители информации как в виде отдельных ссылок, так и в виде файлов, находит доступ к наиболее уязвимому элементу в какой-либо сети или системе для того, чтобы в дальнейшем распространиться на свою копию, тем самым нанести вред элементам всей системы. Он может на-



править свои действия на электронную почту, различные мессенджеры, обменники и файлы с информацией. Так называемый «Червь», хранится посредством файла, как правило, на жёстком диске.

Если рассматривать такой вид программы как «троян», то по различным способам распространения, она очень сильно отличается от других вредоносных вирусов. Здесь все намного проще, происходит занесение в компьютер различных файлов, но уже под видом легального приложения, но помимо тех функций, которые были абсолютно безопасны, заносятся и те, которые обработаны непосредственно злоумышленником. Троянские программы не могут самовоспроизводиться. В такие программы вкладываются задачи, которые имеют разнообразные ходы и наиболее сложные уязвимости в компьютерной системе. Известна, например, троянская программа, использующая вычислительные мощности компьютера-жертвы для генерации электронной валюты Bitcoin.

Ещё одна разновидность вредоносных программ – руткит. Особенность руткита в том, что для сокрытия вредоносного кода и его работы от пользователя и установленного защитного программного обеспечения применяется тесная его интеграция с операционной системой. Более того, некоторые руткиты могут запускаться перед загрузкой операционной системы.

Основное место в распространении преступлений, связанных с получением информации и её безопасности, принадлежит тем программам, которые носят вирусный характер, так как по средству различных ссылок и атак, которым подвергаются лица, не обладающие специальными знаниями, злоумышленники проникают и получают всю необходимую информацию.

В настоящее время активно внедрена работа с базами данных, обработка документов в служебной, производственной деятельности, так называемый документооборот. Следствием этих процессов является криминализация сферы использования компьютерных технологий [5, с. 248].

Сотрудники ФСБ задержали жителя г. Курганца, который взламывал сайты государственных вузов, чтобы получить криптовалюту. Кибератаки хакер производил с домашнего ноутбука на сайты образовательных учреждений, в основном, российских государственных университетов. Целью взлома являлось получение доступа к их ресурсам для генерации криптова-

люты. 42-летнего мужчину обвинили в использовании вредоносных компьютерных программ из корыстной заинтересованности. В отношении его было возбуждено уголовное дело. Мужчине грозит до пяти лет лишения свободы. В 2018 году его уже привлекали к ответственности за аналогичное преступление [6].

Житель Щучанского округа (Курганская область) признан виновным в совершении преступлений, предусмотренных ч. 1 ст. 273 УК РФ (использование компьютерной программы, заведомо предназначенной для копирования компьютерной информации или нейтрализации средств защиты компьютерной информации), осуществил воздействие на интернет-сайты, принадлежащие органам власти. Суд назначил наказание в виде 1,5 года ограничения свободы. В феврале 2021 года он с ее помощью проник на сайты органов власти в г. Саратове и г. Калуге, но причинить особого вреда не сумел [7].

Одна из главных проблем расследования киберпреступлений связана с невозможностью единообразного подхода к расследованию преступлений. Закрепленные в УПК РФ следственные действия, при расследовании данного вида преступлений не будут обладать эффективностью.

С учетом актуальности проблем киберпреступности, помимо профилактики и разъяснительной работы среди граждан, важное значение имеет качественная коммуникация между всеми участниками процесса расследования таких преступлений. Главные причины этой ситуации, это доверчивость граждан и низкий уровень технической грамотности [8, с. 51].

Большое количество преступлений стало выявляться в кредитно-финансовой сфере. Для того, чтобы совершить преступление, связанное с хищением наличных и безналичных средств путём перевода на фиктивные счета, а также осуществить фальсификацию финансовых документов, в частности, платёжных документов, провести «отмывание» денег, используют прежде всего компьютерные технологии.

Борьба с преступлениями в сфере использования информационных технологий занимает всё более важное место в деятельности правоохранительных органов. Это подтверждается различными опросами, статистикой, изучением материалов различных уголовных дел и исследованием судебных практик.

А.Н. Сухов выделяет следующие виды

классификации угроз в сфере информационной безопасности [9, с. 104]: использование иностранной информационной платформы, что таит в себе опасность тотального информационного контроля; трудности доступа в определённых случаях в иностранные поисковые, социальные, видео сети; хакерские атаки, взломы, вмешательство, вторжение в национальную информационную систему; криминальные информационные угрозы; информационно-психологическая война.

В настоящее время особую угрозу представляют информационные войны, которые ведут против России её противники. Информационная война предполагает наличие специализированных формирований, а также предпринимаемых враждебных действий для достижения информационного превосходства над неприятелем, главная цель которых нанести вред противнику с помощью воздействия

на информационную безопасность. Информационная война предполагает наличие особого управления и коммуникаций, соответствующей материальной базы, осуществления разведки и контрразведки, обеспечивающих превосходство над противником [10].

В сфере обеспечения информационной безопасности существует множество угроз, которые делятся на внешние и внутренние, создаваемые преднамеренно и возникающие вследствие сбоев техники и просчётов персонала. В отношении каждой должен быть проведен анализ, результаты которого предполагают немедленное реагирование со стороны органов государственной власти, институтов гражданского общества, что подразумевает постоянное совершенствование нормативно-правовой базы обеспечения информационной безопасности.

Литература

1. МВД РФ: в 2023 году в стране зарегистрировано рекордное количество IT-преступлений. URL: <https://habr.com/> (дата обращения: 12.03.2024).
2. Расследование киберпреступлений несколько слов об отраслевой специфике. URL: <https://habr.com/> (дата обращения: 11.03.2024).
3. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ. URL: <http://www.consultant.ru/> (дата обращения: 11.03.2024).
4. Евкина, И.И. Киберпреступность как угроза информационной безопасности / И.И. Евкина, Т.Н. Шарыпова // Инновации. Наука. Образование. – 2021. – № 36. – С. 376.
5. Чайковский, П.П. Средства реализации угроз информационной безопасности / П.П. Чайковский // Вестник науки. – 2022. – Т. 4. – № 11 (56). – С. 248.
6. ФСБ поймала курганского хакера, который взламывал сайты госучреждений. URL: <https://ura.news/> (дата обращения: 11.03.2024).
7. Курганскому хакеру вынесли приговор за взлом сайтов чиновников. URL: <https://ura.news/> (дата обращения: 11.03.2024).
8. Голубовский, В. Ю. Проблемы противодействия киберпреступлениям против собственности / В. Ю. Голубовский // Проблемы противодействия киберпреступности: Материалы международной научно-практической конференции, Москва, 28 апреля 2023 года. – Москва: Московская академия Следственного комитета Российской Федерации, 2023. – С. 50-52. – EDN UYUJOR. С. 51.
9. Сухов, А.Н. Понятия и виды угроз информационной безопасности / А.Н. Сухов // Человеческий капитал. – 2022. – № 2 (158). – С. 104.
10. Лукин, А.Н. Информационная война против России: уроки, которые необходимо извлечь / А.Н. Лукин, А.Н. Медведев // Бизнес и общество. – 2022. – № 1 (33). – URL: http://business-society.ru/2022/num-1-33/12_medvedev.pdf. (дата обращения 21.12.2023).

References

1. MVD RF: v 2023 godu v strane zaregistrovano rekordnoye kolichestvo IT-prestupleniy. URL: <https://habr.com/> (data obrashcheniya: 12.03.2024).
2. Rassledovaniye kiberprestupleniy neskol'ko slov ob otraslevoy spetsifike. URL: <https://habr.com/> (data obrashcheniya: 11.03.2024).
3. Ugolovnyy kodeks Rossiyskoy Federatsii ot 13.06.1996 № 63-FZ. URL: <http://www.consultant.ru/> (data obrashcheniya: 11.03.2024).
4. Yevkina, I.I. Kiberprestupnost' kak ugroza informatsionnoy bezopasnosti / I.I. Yevkina, T.N. Sharypova // Innovatsii. Nauka. Obrazovaniye. – 2021. – № 36. – S. 376.
5. Chaykovskiy, P.P. Sredstva realizatsii ugroz informatsionnoy bezopasnosti / P.P. Chaykovskiy // Vestnik nauki. – 2022. – T. 4. – № 11 (56). – S. 248.
6. FSB poymala kurganskogo khakera, kotoryy vzlamyval sayty gosuchrezhdeniy. URL: <https://ura.news/> (data obrashcheniya: 11.03.2024).
7. Kurganskomu khakeru vynesli prigovor za vzlom saytov chinovnikov. URL: <https://ura.news/> (data obrashcheniya: 11.03.2024).
8. Golubovskiy, V. YU. Problemy protivodeystviya kiberprestupleniyam protiv sobstvennosti / V. YU. Golubovskiy // Problemy protivodeystviya kiberprestupnosti:



Materialy mezhdunarodnoy nauchno-prakticheskoy konferentsii, Moskva, 28 aprelya 2023 goda. – Moskva: Moskovskaya akademiya Sledstvennogo komiteta Rossiyskoy Federatsii, 2023. – S. 50-52. – EDN UYUJOR. S. 51.

9. Sukhov, A.N. Ponyatiya i vidy ugroz informatsionnoy bezopasnosti / A.N. Sukhov // Chelovecheskiy kapital. –2022. –№ 2 (158). – S. 104.

10. Lukin, A.N. Informatsionnaya voyna protiv Rossii: uroki, kotoryye neobkhodimo izvlech' / A.N. Lukin, A.N. Medvedev // Biznes i obshchestvo. – 2022. – № 1 (33). – URL: http://business-society.ru/2022/num-1-33/12_medvedev.pdf. (data obrashcheniya 21.12.2023).

ГОЛУБОВСКИЙ Владимир Юрьевич, доктор юридических наук, профессор, главный научный сотрудник ФГКУ ВНИИ МВД России. 121069, г. Москва, ул. Поварская, д. 25, стр. 1. E-mail: 63wladimir@mail.ru.

КУНЦ Елена Владимировна, доктор юридических наук, профессор, главный научный сотрудник ФКУ НИИ ФСИН России. 125130, г. Москва, ул. Нарвская, 15А, стр. 1. E-mail: 73kuntc@mail.ru

GOLUBOVSKY Vladimir Yurievich, Doctor of Law, Professor, chief researcher of the Federal State Institution All-Russian Research Institute of the Ministry of Internal Affairs of Russia. 121069, Moscow, st. Povarskaya, 25, building 1. E-mail: 63wladimir@mail.ru.

KUNTS Elena Vladimirovna, Doctor of Law, Professor, Chief Researcher, PKU Research Institute of the Federal Penitentiary Service of Russia. 125130, Moscow, st. Narva, 15A, p. 1. E-mail: 73kuntc@mail.ru

