Солдатова Екатерина Александровна

Магистрант

Направление: Юриспруденция

Магистерская программа: Правоохранительная

Уголовное законодательство Российской Федерации об ответственности за неправомерный доступ к компьютерной информации

Аннотация. Статья посвящена исследованию уголовно-правовых норм Российской Федерации об ответственности за неправомерный доступ к компьютерной информации.

Ключевые слова: компьютерные технологии, система безопасности, компьютерная информация, ответственность за неправомерный доступ.

Телекоммуникационные преступления – это противоправные действия, совершаемые с использованием компьютерных технологий в виртуальном пространстве - имитируемой информационной среде, содержащей информацию о людях, объектах, данных, событиях, явлениях и процессах, представленную в математической, символьной или любой другой форме и передаваемую через локальные и глобальные компьютерные сети, или информацию, хранящуюся в памяти реального компьютера. Проблема телекоммуникационной преступности для мирового сообщества стоит на первом месте.

В Российской Федерации действует Доктрина информационной безопасности [4], в которой сформулирован перечень основных национальных угроз, среди которых законодатель выделяет – расширение масштабов использования специальными службами отдельных государств средств оказания информационно-психологического воздействия, направленного на дестабилизацию внутриполитической и социальной ситуации в различных регионах мира и приводящего к подрыву суверенитета и нарушению территориальной целостности других государств.

Главой 28 Уголовного кодекса Российской Федерации, предусмотрена уголовная ответственность за компьютерные преступления.

В частности, незаконный доступ к компьютерной информации (статья 272 Уголовного кодекса Российской Федерации); создание, использование и распространение вредоносных компьютерных программ (статья 273 Уголовного кодекса Российской Федерации); нарушение правил эксплуатации компьютерной информации и средств хранения, обработки или передачи информации и телекоммуникационных сетей (статья 274 Уголовного кодекса Российской Федерации); неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (274.1 УК РФ) и т.д.

Уголовный кодекс Российской Федерации (УК РФ) от 13 июня 1996 г. № 63-ФЗ [2] призван охранять самые важные общественные отношения. Как настоящий живой организм уголовный закон реагирует на изменения, происходящие в обществе, пополняясь новыми нормами.

С появлением компьютерных технологий возникли отличные о ранее использованных способы совершения преступлений, наносящие вред нормальному функционированию общества и государства. Как следствие, возникла проблема недостаточной защищенности систем безопасности, в которых содержится информация, охраняемая законом. Это говорит не только об уязвимости систем безопасности, защищаемых компьютерами, но и тех систем, защиту которых обеспечивает человек.

Активное использование преступниками методов социальной инженерии в настоящее время, позволяет им получить доступ к информации, не используя специальные знания. Применяя психологические манипуляции с целью совершения определенных действий можно получить засекреченные данные компании, просто разговаривая с сотрудником безопасности данной организации по телефону.

Организациям, осуществляющим защиту охраняемой законом информации, необходимо анализировать методы воздействия преступника не только на электронные ресурсы, но и на сотрудников, имеющих доступ к такой информации.

Как одно из средств возможного противодействия преступным посягательствам

в систему норм УК РФ включена ст. 272 УК РФ «Неправомерный доступ к компьютерной информации». Однако, толкование и применение этой нормы вызывает некоторые дискуссии среди ученых и практиков.

Так, ни в теоретических источниках, ни в судебной практике нет однозначного перечня информации, которая является предмет указанного преступления.

Конституцией [1] каждому гарантировано право на свободный доступ к информации. Это означает, что люди обладают возможностью искать, получать, передавать, создавать и распространять информацию правомерным способом, используя различные методы. Незаконный доступ к данным является одной из форм работы с ними. В Постановлении Пленума Верховного Суда РФ от 15 декабря 2022 года № 37 [5] было разъяснено, что незаконным он является, когда у лица нет полномочий для выполнения определенных действий. Уголовная ответственность по статье 272 УК РФ возникает только при незаконном получении доступа к компьютерной информации, который приводит к ее уничтожению, блокированию, копированию или изменению. Незаконное ознакомление с компьютерной информацией не подпадает под уголовную ответственность, это не означает, что такие действия являются законными и допустимыми. Следовательно, законодателю стоит дополнить ч. 1 ст. 272 УК РФ положением о неправомерном ознакомлении, поскольку это может иметь опасные последствия для владельца этой информации. Важно всесторонне обеспечить соблюдение предписаний о защите персональных данных и не нарушать права других людей на информационную безопасность, в частности такую ее составляющую как конфиденциальность.

Согласно разъяснениям Верховного суда обязательными последствиями неправомерного деяния можно считать содержащие в своем структурном содержании характеристики следующие понятия. «Уничтожение» компьютерной информации подразумевает приведение ее в состояние, когда она становится полностью или частично непригодной для использования с целью исключения возможности ее восстановления, дальнейшего эксплуатирования. «Блокирование» означает временное ограничение доступа к ней для пользователей без преобразования в непригодное состояние. «Модификация» информации, в свою очередь, включает

любые изменение ее первоначального вида, включая, в первую очередь, такие нарушения или видоизменения таких характеристик, как целостность и достоверность, однако охват любого реверсирования данных, направленного на улучшение или обновление информации не считается разумным, что и подтверждает позиция законодателя. «Копирование» представляет собой совокупность действий по дублированию сведений, то есть транспозиция на иное электронное техническое устройство при сохранении первоначальной информации либо ее воспроизведение в физическом воплощении. Основываясь на объективных признаках преступления, требуется провести анализ других аспектов, представляющих другую часть состава.

Генеральная прокуратора РФ полагает, что статьей охватывается только та информация, которая входит в спектр действия понятия «информация ограниченного доступа». Однако в российском законодательном поле существует около 80 нормативных актов, устанавливающих ограниченный доступ к информации. Например, Закон РФ от 21 июля 1993 г. № 5485-1 «О государственной тайне» [3]. Но не все суды разделяют точку зрения Генеральной прокуратуры РФ и в некоторых случаях самостоятельно относят информацию к той или иной категории.

При квалификации деяний виновного по ст. 272 УК РФ, важное значение приобретает способ совершения преступления, т. е. неправомерность действий. Так как существует правомерный, не наказуемый законом, доступ к компьютерной информации (например, в связи с уровнем допуска или в виду осуществления трудовых полномочий, лица наделяются правом законного доступа к данной категории информации), то неправомерный доступ в свою очередь, подразумевает использование информации для деятельности, не связанной с осуществлением данных полномочий.

Для качественной борьбы с киберпреступностью на территории нашей страны, а также в мировом сообществе, необходимо разработать качественно новые нормативные документы, которые будут содержать точное описание схем выявления и расследования компьютерных преступлений, а также создать техническую базу для их реализации. Необходимо уделить внимание разработке новых систем безопасности, которые смогут отражать кибератаки не только на объекты

критической инфраструктуры Российской Федерации, но и на операционные системы организации и частных пользователей.

Таким образом, только комплексный подход к решению данной проблемы сможет кардинально поменять ситуацию к лучшему. Изменений только нормативной базы не хватит для того, чтобы в вышеупомянутой сфере началась положительная тенденция. Необходимо создать рабочие эффективные механизмы, в том числе и технологическую базу, чтобы сотрудникам правоохранительных органов было легче выявлять и расследовать такого рода преступления. Сложность работы сейчас заключается непосредственно в недостаточной обеспеченности именно инновационными средствами, связанной с нехваткой государственного финансирования. Государству следует провести масштабную работу – переоборудовать управления МВД, повысить квалификацию сотрудников, а также увеличить численность штата, в подведомственности которых находится расследование данной категории дел.

Литература

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // Официальный текст Конституции РФ, включающий новые субъекты Российской Федерации - Донецкую Народную Республику, Луганскую Народную Республику, Запорожскую область и Херсонскую область, опубликован на Официальном интернет-портале правовой информации http://pravo.gov.ru, 06.10.2022.

2. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 06.04.2024) // Российская газета, № 113, 18.06.1996, № 114, 19.06.1996, № 115, 20.06.1996, № 118, 25.06.1996.

3. Закон РФ от 21.07.1993 № 5485-1 (ред. от 04.08.2023) О государственной тайне (с изм. и доп., вступ. в силу с 01.02.2024) //Российские вести, № 189, 30.09.1993.

4. Указ Президента РФ от 05.12.2016 № 646 Об утверждении Доктрины информационной безопасности Российской Федерации // Собрание законодательства РФ, 12.12.2016, № 50, ст. 7074.

5. 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» // Бюллетень Верховного Суда РФ», № 3, март, 2023