Ученые записки Крымского федерального университета имени В. И. Вернадского
Юридические науки. – 2024. – Т. 10 (76). № 1. – С. 48–52.

УДК 343.982.32:004

К ВОПРОСУ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ПРАВОВЫХ ОТНОШЕНИЙ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Ерохин Р. А.

Крымский филиал Краснодарского университета МВД России

В статье анализируются цифровые правовые отношения, стремительно вошедшие в информационно-телекоммуникационную сферу посредством развития общественных отношений между субъектами коммуникации. Отмечается ряд преимуществ, которые внедрились в данную сферу через техническую инфраструктуру, обеспечивающую безопасное использование персональных данных при их вводе на каком-либо сайте. Автором акцентируется внимание на понятии аутентификация, которое существенно влияет на сам процесс идентификации личности при вхождении на сайт и использовании соответствующего пароля и логина для входа. Также рассматриваются преступные схемы, применяемые злоумышленниками для перехвата логина и пароля в целях реализации своих преступных умыслов, а также взлома аккаунтов при таргетированной атаке пользователей, и способы защиты от данных посягательств.

Ключевые слова: цифровизация, правовые отношения, IT-сфера, логин, пароль, аутентификация, взлом, защита, электронная подпись.

В современных условиях развития общественных правоотношений, всё большая их часть переходит в IT-сферу. Как отмечают Зоз В.А. и Лагуточкина А.С., «стремительное развитие и повседневное применение информационных технологий, преобразование информации в важнейший ресурс жизнедеятельности, обуславливает движение человечества к информационному обществу» [1]. Данное условие позволяет упростить коммуникативную функцию между субъектами отношений. Цифровые правоотношения обладают рядом особенностей и преимуществ перед обычными, уже устаревшими способами взаимоотношений. Одной из основных особенностей выделяется сложность определения, то есть идентификации пользователей. Федеральным законом «Об информации, информационных технологиях и о защите информации» термин «идентификация» определяется как проверка лица на принадлежность ему определенного идентификатора и установления правомерности владения им. Данная норма создана для решения проблемы определения субъектов цифровых отношений [2].

В своей статье, Лагуточкин А.В. и Мащенко А.Д. обращают внимание на то, что «на сегодняшний день особую актуальность приобретает проблема обнаружения и фиксации в интернет-пространстве стабильных и достоверных источников получения необходимой оперативно-розыскной информации, дальнейшего упорядочения и оптимизации полученной информации» [3]. При этом существует ряд преимуществ цифровых правовых отношений, который характеризуется возможностью их осуществления на большом расстоянии, а также через техническую инфраструктуру, выступающую посредником между субъектами. Такая инфраструктура представляет множество полезных функций, например, может обеспечивать безопасную сделку между продавцом и покупателем какого-либо товара. Весомым положительным отличием цифровых правоотношений является анонимность доступа пользователя и

невозможность идентифицировать субъект без его согласия. Данная особенность лежит в основе множества цифровых технологий, ярким примером которых является криптовалюта. Её использование проходит без возможности обратной конвертации, таким образом, возврат средств невозможен. Существует множество и иных способов обойти идентификацию на тех сайтах и в тех приложениях, где она необходима. Например, использование лицом VPN [4] сервисов позволяет избежать его разоблачения посредством изменения IP-адреса. Данный способ отличается высокой требовательностью к скорости сети, так как технология VPN базируется на перенаправлении сигнала через различные сервера в других странах, что делает подключение к необходимому сервису дольше из-за трудной системы связи. При этом право в данной отрасли основано на принципе формальной определенности, который требует возникновения прав и обязанностей у определенного лица.

Стоит отметить, что законодательство Российской Федерации активно адаптируется к возникающим изменениям в сфере общественных отношений. Для решения повсеместных проблем, возникающих в правовых отношениях в IT-сфере, законом устанавливается, что гражданин приобретает и осуществляет свои права и обязанности исключительно под свои именем, фамилией и отчеством, приобретение прав и обязанностей от имени других лиц недопустимо.

Федеральным законом «Об информации, информационных технологиях и о защите информации» так же устанавливается понятие «аутентификации». Под данным термином понимается проверка лица на принадлежность ему соответствующего идентификатора и установление законности и правомерности владения им, в результате чего лицо считается установленным. Как правило, такими идентификаторами выступают адрес почтового ящика, никнейм в форуме, профиль в социальной сети и пр. [5]. При входе на какой-либо сайт под своим именем, необходима авторизация, важным компонентом которой является аутентификация. Если аутентификация прошла успешно, система может определить лицо как идентифицированного носителя установленных прав и обязанностей. В любом случае, необходимо понимать, что даже в настолько продуманной системе существуют так называемые «дыры», так как необходимую для аутентификации информацию при должных усилиях можно скомпрометировать. Перехват логина и пароля – достаточно частое явление. Данная техника применяется злоумышленниками посредством различных, зачастую незаконных методов. Примером таких методов может являться создание и распространение вредоносных программ, целью которых является похищение необходимой злоумышленнику информации. Фишинг – наиболее распространенный метод хищения паролей и логинов с помощью создания поддельного известного веб-сайта с незначительно измененным доменным именем, незаметным для обычного пользователя. Введенные для входа данные сразу поступают в распоряжение правонарушителя. Аутентификация посредством биометрии так же не может гарантировать стопроцентную законность, так как принцип работы систем биометрической аутентификации основывается на извлечении биометрических черт регистрируемого пользователя и создания по ним шаблона. Шаблон заносится в специализированную базу данных, которая может быть не только похищена и модифицирована, но и уничтожена, что поможет злоумышленнику без труда войти в систему без биометрической аутентификации. Таким образом, на практике аутентификация не является абсолютно точным методом определения личности зарегистрированного под своим

именем лица. Некоторые научные деятели, например Волков В.Э. считают, что существует лишь оспоримая юридическая презумпция (предположение) о принадлежности цифровых прав и обязанностей определенному лицу. Он подразделяет факторы аутентификации человека на три типа:

- Многоразовые и одноразовые пароли – то, что знает человек, зарегистрированный под своим именем и фамилией;
- Аппаратные аутентификаторы – флеш-накопители, токены, магнитные ключ-карты;
- Биометрия – биологические и физиологические признаки, принадлежащие определенному человеку и используемые им в качестве идентификаторов [6].

Можно выделить и смежные типы, например использование электронной подписи, хранящейся на флеш-накопителе, которая для аутентификации требует подтверждения личности пользователя с помощью отправленного на его мобильный телефон SMS-кода, имени, фамилии и отчества, а так же пароля.

Парольный способ защиты достаточно популярен и удобен в использовании, но как и всем способам защиты, ему присущи некоторые слабости. Изначально все пароли можно классифицировать на три группы:

1. Сгенерированные программными и аппаратными средствами;
2. Придуманные самим пользователем;
3. Назначенные системным администратором информационной системы.

Каждая из данных групп отличается степенью устойчивости к попытке взлома. Если субъект пользуется собственными паролями, то возможность взлома его аккаунтов при таргетированной атаке достаточно велика, так как большинство современных пользователей при регистрации вводят один и тот же придуманный ими пароль. Зачастую такой пароль состоит из имени или фамилии, номера телефона пользователя, даты его рождения. Если злоумышленник знает вышеперечисленные данные конкретного лица, то ему не составит труда угадать пароль. Наиболее подверженным взлому паролем является последовательность латинских символов, совпадающей с английской раскладкой клавиатуры: QWERTY, возможно использование последовательно идущих цифр от одного до девяти. Согласно статистике сервиса NordPass [7] за 2022 г., пароль QWERTY используется более чем 309.679 пользователями сети Интернет. Так же в список самых распространённых входят такие пароли, как password, guest, 123123 и так далее. Стоит отметить, что все подобные пароли взламываются специальными программами, основанными на методе перебора, менее чем за секунду.

Остальные группы характеризуются более сложно угадываемыми паролями. Зачастую сгенерированные пароли состоят из букв латинского алфавита различного регистра, сгенерированной последовательности цифр и специальных символов. У таких паролей есть существенный минус – сложная запоминаемость и долгое введение вручную. Тем не менее, такие пароли теми же брутфорс-программами, основанными на методе перебора, взломать будет на много дольше. Сегодня системные администраторы используют сгенерированные системой пароли, чтобы не подвергать важную информацию опасности.

Обычно именно сгенерированными паролями пользуются при создании электронной подписи, которая так актуальна на сегодняшний день. Актуальность и

удобство использования электронной подписи не может обойти общественные отношения, поэтому государство предлагает внедрить данную технологию повсеместно. Согласно Федеральному закону «Об организации предоставления государственных и муниципальных услуг» каждому гражданину возможно получить электронную подпись бесплатно [8]. Это осуществляется через электронный сайт предоставления государственных услуг gosuslugi.ru. Некоторые рекомендации со временем стали обязательными для исполнения. Например, на сегодняшний день индивидуальным предпринимателям практически невозможно обойтись без электронной подписи. На подтверждении личности с помощью данных технологий строится практически всё ведение бизнеса в России. Так же существует возможность использования электронной подписи для придания электронному документу юридической силы при страховании гражданской ответственности владельцев автомобилей. Однако присутствуют и существенные недостатки в использовании электронной подписи. Одним из них можно выделить тот факт, что после подписания ею электронного документа, нет гарантии того, что в него не будут внесены изменения. В связи с этим недостатком сфера её использования имеет ограничения. Электронная подпись может приравниваться поставленной лицом подписи собственноручно не во всех случаях, а только в тех, когда это предусмотрено соответствующим нормативным актом.

Таким образом, на сегодняшний день достаточно быстро происходит процесс внедрения автоматизированных систем в правовую сферу. Данное явление объясняется развитием информационно-телекоммуникационных технологий, которые становятся всё более привычны для повсеместного использования. Государственная власть принимает меры по легализации таких технологий в целях упрощения взаимодействия между государством и личностью. Переход от подчинения правоотношений юридическим фактам к определению правовых отношений с помощью записей имеет достаточно трудоёмкий процесс в плане законодательства, но законодательная власть применяет все средства для внесения новых видов технологий в нормативную базу.

Список литературы:

1. Зоз В.А., Лагуточкина А.С. Личность интернет-преступника и отдельные способы их выявления в глобальной информационной сети // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. 2023. Т. 9. № 2. С. 306-312.
2. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07 2006 № 149-ФЗ // Гарант.ру: сайт. URL: https://base.garant.ru/12148555/ (дата обращения: 12.12.2023).
3. Лагуточкин А.В., Мащенко А.Д. Об использовании цифровых источников получения информации подразделениями органов внутренних дел,осуществляющими оперативно-розыскную деятельность // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. 2022. Т. 8. № 1. С. 176-182.
4. Что такое VPN-соединение и как им пользоваться. URL: https://netpeak.net/ru/blog/chto-takoye-vpn-soyedineniye-i-kak-im-pol-zovat-sya-story/ (дата обращения: 13.12.2023).
5. Зоз В.А., Чехун А.Ф. Идентификация личности преступника по виртуальным следам в сети Интернет // Актуальные проблемы теории и практики оперативно-розыскной деятельности: материалы IX Всероссийской научно-практической конференции. Редколлегия: А.А. Сафронов [и др.]. Краснодар, 2021. С. 75-79.
6. Цифровое право. Общая часть: учебное пособие / В.Э. Волков. – Самара: Издательство Самарского университета, 2022. С. 63.
7. NordPass – your digital life manager. URL: nordpass.com (дата обращения: 13.12.2023).

8. Об организации предоставления государственных и муниципальных услуг: Федеральный закон от 27.07.2010 № 210-ФЗ ФЗ // Гарант.ру: сайт. URL: https://base.garant.ru/12177515/ (дата обращения: 13.12.2023).

Erokhin R.A. To the question of indetification and authentification in the CONDITIONS OF digitalisation of legal relationships in the Russian Federation // Scientific notes of V. I. Vernadsky crimean federal university. Juridical science. – 2024. – T. 10 (76). № 1. – P. 48–52.

The article analyses the digital legal relations that have rapidly entered the information and telecommunication sphere through the development of social relations between the subjects of communication. A number of advantages that have been introduced into this sphere through the technical infrastructure that ensures the safe use of personal data when entering them on any website are noted. The author focuses on the concept of authentication, which significantly affects the very process of personal identification when entering a site and using the appropriate password and login for entry. The author also considers criminal schemes used by attackers to intercept login and password in order to realise their criminal intentions, as well as hacking of accounts in the case of targeted attack of users, and ways to protect against these encroachments.

Keywords: digitalisation, legal relations, IT-sphere, login, password, authentication, hacking, protection, electronic signature.

Spisok literatury:

1. Zoz V.A., Lagutochkina A.S. Lichnost' internet-prestupnika i otdel'nye sposoby ih vyyavleniya v global'noj informacionnoj seti // Uchenye zapiski Krymskogo federal'nogo universiteta imeni V.I. Vernadskogo. YUridicheskie nauki. 2023. T. 9. № 2. S. 306-312.
2. Ob informacii, informacionnyh tekhnologiyah i o zashchite informacii: Federal'nyj zakon ot 27.07 2006 № 149-FZ // Garant.ru: sajt. URL: https://base.garant.ru/12148555/ (data obrashcheniya: 12.12.2023).
3. Lagutochkin A.V., Mashchenko A.D. Ob ispol'zovanii cifrovyh istochnikov polucheniya informacii podrazdeleniyami organov vnutrennih del,osushchestvlyayushchimi operativno-rozysknuyu deyatel'nost' // Uchenye zapiski Krymskogo federal'nogo universiteta imeni V.I. Vernadskogo. YUridicheskie nauki. 2022. T. 8. № 1. S. 176-182.
4. CHto takoe VPN-soedinenie i kak im pol'zovat'sya. URL: https://netpeak.net/ru/blog/chto-takoye-vpn-soyedineniye-i-kak-im-pol-zovat-sya-story/ (data obrashcheniya: 13.12.2023).
5. Zoz V.A., CHekhun A.F. Identifikaciya lichnosti prestupnika po virtual'nym sledam v seti Internet // Aktual'nye problemy teorii i praktiki operativno-rozysknoj deyatel'nosti: materialy IX Vserossijskoj nauchno-prakticheskoj konferencii. Redkollegiya: A.A. Safronov [i dr.]. Krasnodar, 2021. S. 75-79.
6. Cifrovoe pravo. Obshchaya chast': uchebnoe posobie / V.E. Volkov. – Samara: Izdatel'stvo Samarskogo universiteta, 2022. S. 63.
7. NordPass – your digital life manager. URL: nordpass.com (data obrashcheniya: 13.12.2023).
8. Ob organizacii predostavleniya gosudarstvennyh i municipal'nyh uslug: Federal'nyj zakon ot 27.07.2010 № 210-FZ FZ // Garant.ru: sajt. URL: https://base.garant.ru/12177515/ (data obrashcheniya: 13.12.2023).