УДК 004.9
DOI https://doi.org/10.32838/2663-5941/2021.1-1/25

Чанышев Р.И.
Национальный университет «Одесская юридическая академия»

УСЛОВИЯ ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ И БЕЗОПАСНОСТИ ДАННЫХ ПОЛЬЗОВАТЕЛЯ ПРИ РАБОТЕ С ПРОВАЙДЕРАМИ ОБЛАЧНЫХ СЕРВИСОВ

Хмарні технології з'явилися і стали впроваджуватися у практику не так давно – приблизно з 2012 р. За минулі роки виявилися численні переваги використання цих технологій у бізнесі, управлінні й у приватному (особистому) їх використанні.

Характер використання публічних хмарних технологій передбачає передачу інформації від користувача (приватної особи або організації) в системи зберігання провайдерів хмарних технологій. Користувач не знає, де саме розташовані використовувані ним сховища даних і хто саме має до них доступ.

Умови використання сервісів публічної хмари обговорюються в умовах надання послуг, в угодах про використання сервісів, у заявах про конфіденційність – конкретна назва документа вибирається провайдером хмарних послуг. Умови угод, декларацій і т. п. приймаються користувачем у момент створення облікового запису, за допомогою якого надається доступ до хмарних послуг у вигляді згоди користувача з умовами договору приєднання. Від користувача не потрібно попереднього ознайомлення з текстом договору, більш того, сама наявність такого тексту подається в неявній (малопомітній) для користувача формі.

У статті розглядається зміст договорів приєднання на прикладі договорів такого провайдера хмарних сервісів, як корпорація Microsoft і здійснюється аналіз умов договору з погляду забезпечення конфіденційності даних користувача. Виявлено, що умови таких договорів передбачають тільки декларативне збереження конфіденційності даних користувача. Фактично ж вони дозволяють повний доступ до даних користувача не тільки самим провайдерам хмарних сервісів, а і третім особам. Умови цих договорів передбачають практично повну деаномізацію користувачів, що укупі з можливістю передачі даних третій стороні відкриває можливість, наприклад, для кримінального переслідування користувачів.

Проблема полягає ще й у тому, що фахівці у сфері інформаційних технологій не мають належних юридичних знань і часто не можуть дати правову оцінку умовам цих угод.

У статті даються рекомендації щодо збереження конфіденційності переданих у хмару даних без порушення умов договору із провайдером хмарних сервісів.

Ключові слова: *хмарні технології, договори приєднання, збереження конфіденційності, проблема деаномізації користувачів, необхідність шифрування даних.*

Постановка проблемы. Переход обычных компьютерных технологий к облачным в Украине начался с 2012 г., и к настоящему времени объем предоставляемых облачных услуг в Украине вырос в 16 раз. Однако их внедрение осуществляется преимущественно технически, при этом правовым аспектам их использования в части сохранения конфиденциальности передаваемых в облачные хранилища информации уделяется недостаточно внимания. Эта проблема возникла в связи с тем, что внедрением облачных технологий занимаются специалисты, занимающиеся компьютерными технологиями, имеющие технические знания, но не имеющие знаний юридических, а между тем перед началом использования любой публичной облачной услуги пользователь должен принять условия договора, составленного организацией, оказывающей услугу доступа к облачным сервисам. Анализ содержания таких договоров свидетельствует о том, что практически каждый из них содержит пункты, непосредственно связанные с нарушением конфиденциальности данных пользователя.

Анализ последних исследований и публикаций. Анализ публикаций, связанных с данной темой, показывает, что эта проблема пока не нашла своего должного отражения в научной литературе. Такой парадокс можно объяснить как новизной самой темы, так и тем, что она находится на стыке таких далеких от друг друга отраслей знаний, как компьютерные технологии и право. Подавляющее большинство пользователей не читают тексты соответствующих соглашений и деклараций уже просто по той причине, что тек-

сты соглашений даются в виде ссылок, причем ссылок, набранных мелким шрифтом и расположенных таким образом, чтобы пользователь их не заметил. Проблема усугубляется тем, что специалисты в сфере информационных технологий не обладают должными юридическими знаниями и зачастую не могут дать правовую оценку условиям этих соглашений.

Постановка задания. Целью данной статьи является анализ содержания соглашений, условий и деклараций, предлагаемых провайдерами облачных сервисов на примере соглашений и деклараций корпорации Microsoft, выявление в них условий, потенциально нарушающих конфиденциальность данных пользователя (и тем самым влияющих на общую безопасность использования облачных сервисов) для последующей разработки общих рекомендаций для пользователей облачных сервисов.

Изложение основного материала исследования. Публичные облачные сервисы используют традиционную клиент-серверную технологию, дополненную тем, что в данном случае серверы размещаются удаленно, и пользователь (частное лицо или организация) не имеют к ним непосредственного (физического) доступа. Тем самым пользователь облачных сервисов (далее – пользователь ОС) полностью лишен возможности каким-либо образом контролировать процесс работы и обслуживания сервера, в т. ч. и удаленно, с помощью программных средств.

В этом случае пользователю приходится полностью полагаться на честность и добросовестность провайдеров облачных сервисов (далее – провайдеров ОС).

Безусловно, существует альтернатива в виде приватных облаков, создаваемых самими пользователями (например, организацией или предприятием для своих сотрудников), но их создание и поддержка требуют значительных затрат, непозволительных для простых пользователей и для организаций, не имеющих своих отделов ИТ.

Пользователи ОС имеют возможность выбора из нескольких планов различной стоимости и с различными наборами услуг [1], но в любом случае пользователю ОС приходится принимать условия, предложенные ему провайдером ОС.

Известны случаи, когда составители соглашений с конечным пользователем вносили в них довольно странные требования. Например, британская компания Game Station включила в текст соглашения пункт о том, что пользователь обязуется отдать после смерти «свою бессмертную душу» этой компании. В итоге это соглашение приняли 7 500 человек, что составило 88% процентов от общего числа всех пользователей [2].

Такая статистика свидетельствует о том, что большая часть пользователей вообще никогда не читает такие документы. Однако все эти соглашения юридически являются договором присоединения (вид договоров, при заключении которых одна сторона может только принять или не принять условия договора, предложенные другой стороной, но не имеет возможности изменить эти условия). Таким образом, пользователь, нажимая на предложенную ему кнопку («ОК», «Да», «Далее», «Продолжить» и т.п.), заключает договор с другой стороной и тем самым принимает на себя определенные обязанности и предоставляет определенные права другой стороне.

Ссылка на условия провайдеров ОС обычно дается мелким шрифтом и малозаметна для пользователя. Принятие условий (согласие с ними) осуществляется путем нажатия на кнопку, с текстом условий никак не связанную, хотя и расположенную на том же экране (рис. 1).

Так, корпорация Microsoft дает ссылку на Заявление о конфиденциальности в одной строке с приглашением присылать, по факту, рекламную информацию, а корпорация Google не только использует мелкий шрифт, но и не выделяет ссылку подчеркиванием и цветом. Кроме того, в самом тексте наиболее важные по смыслу части документа скрываются при помощи ссылок. Подобная практика однозначно свидетельствует о том, что провайдеры ОС не стремятся к тому, чтобы пользователи нашли и прочли эти условия.

Далее в статье рассматриваются и анализируются положения двух документов – Соглашения об использовании служб Майкрософт (далее – Соглашение) [3] и Заявления о конфиденциальности (далее – Заявление) [4].

В первом же абзаце Соглашения указывается: «Принимая данные Условия, Вы тем самым даете согласие на сбор, использование и раскрытие Вашего содержимого и Данных согласно положениям Заявления о конфиденциальности».

Далее дается разъяснение, что после отправки содержимого (т.е. информации) «другим людям» они смогут использовать его в «мировом масштабе», «для цели, для которой Вы предоставили доступ к Вашему содержимому в Службах» без предоставления пользователю компенсации.

Поскольку широкое понятие «другие люди» может включать в себя и самого провайдера ОС, данный пункт можно считать предупреждением о

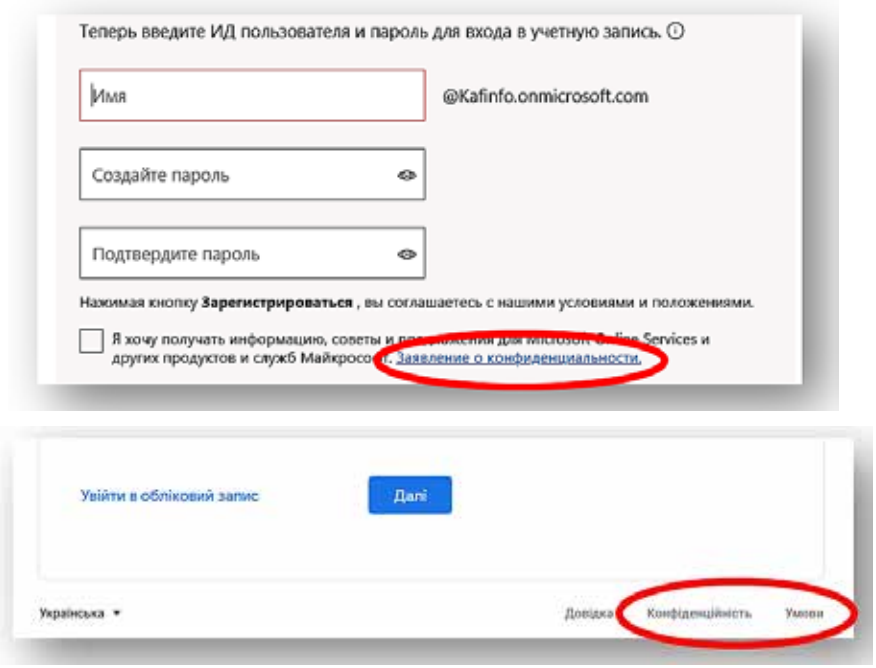

Рис. 1

возможности использования отправленной пользователем ОС информации в интересах самого провайдера ОС.

В упомянутом выше Заявлении о конфиденциальности в первом же пункте указано, что Microsoft собирает персональные данные своих пользователей, причем не только те, что предоставляются ей пользователями напрямую, но и те, что предоставляются Microsoft от третьих сторон. Кроме того, анализируются и действия пользователей в службах, предоставляемых этим провайдером ОС.

Принцип получения данных от третьих сторон может означать анализ информации, получаемой от пользователя служб Microsoft, с целью выявления в ней информации, связанной с другими пользователями таких служб.

В Заявлении перечисляются источники информации от третьих сторон, к числу которых относятся брокеры демографических данных, открытые публикации в социальных сетях, сообщения электронной почты, к которым не закрыт доступ, информация от провайдеров мобильной и стационарной связи, с помощью которой можно определить местонахождение компьютерного устройства пользователя, интернет-магазины и другие торговые площадки, разработчики программного обеспечения и прочие общедоступные источники, включая и государственные базы данных, к которым открыт свободный доступ.

Таким образом, в Заявлении допускается сбор всей возможной информации о пользователе из открытых источников. При этом подчеркивается, что отказ от предоставления данных, необходимых для работы продукта или компонента, может привести к недоступности некоторых функций или услуг.

В Заявлении указывается, что собирается следующая информация о пользователе: имя, фамилия, адрес электронной почты, почтовый адрес, номер телефона, используемые пароли, подсказки по паролям, данные о возрасте, поле, стране, предпочитаемом языке, данные банковской карты, защитный код карты, данные о лицензиях на используемое программное обеспечение, произведенные поисковые запросы, данные о посещенных пользователям веб-страницах, просмотренных через поисковые системы изображениях, данные контактов пользователя, данные об используемом пользователем компьютерном оборудовании, данные об используемой пользователем компьютерной сети и о других беспроводных сетях, находящихся в зоне приема, коды IMEI телефонов, подключённых к сети или к компьютеру.

Кроме того, при настройке профиля пользователя пользователю предоставляется возможность установить в качестве аватара свою собственную фотографию. При этом не дается никаких предупреждений о том, что данное действие ведет к раскрытию персональных данных пользователя.

Такой набор данных в своей совокупности позволяет точно идентифицировать конкретного

человека и определить его точное местоположение в реальном масштабе времени.

Последнее возможно благодаря использованию системы WPS (Wi-Fi Positioning System), определяющей положение объекта по координатам точек доступа Wi-Fi, положение которых точно известно и внесено в соответствующую базу данных компании Skyhook Wireless и некоторых других компаний [5; 6].

Поскольку провайдеры ОС собирают данные о других точках доступа, находящихся в зоне действия приёмопередатчика Wi-Fi, для определения точных координат пользователя достаточно найти соответствие между этими данными и данными, хранящимися в базе данных WPS [7].

Характерной особенностью сбора информации именно компанией Microsoft является то, что эта компания является производителем самой распространенной операционной системы в мире.

В случае сбоя в программном обеспечении, не обязательно произведенного компанией Microsoft, но установленном на компьютере, работающим под управлением ОС производства Microsoft, в эту компанию отправляется информация об ошибках, возникших в этом программном обеспечении, а, следовательно, и о том, какое именно стороннее программное обеспечение установлено на данном компьютере. Об этом факте также упоминается в Заявлении о конфиденциальности.

Помимо технической информации, собирается и информация, которую можно отнести к социологической: данные об интересах пользователя (за какие спортивные команды болеет, за какими новостями следит, часто ли интересуется погодой или дорожной ситуацией), данные о просмотре телепередач, прослушиваемой музыке, какие книги читает и в какие игры играет), данные о взаимодействии между пользователем и другими людьми, о том, что нравится или не нравится пользователю, о взаимодействии пользователя с различными организациями. При этом указанные данные могут быть собраны не только при прямом указании, но и определены по совокупности других собранных данных.

Собираются также и голосовые данные пользователя, полученные при использовании программного обеспечения, работающего с микрофоном («Кортана»). При этом отмечается, что могут учитываться и фоновые звуки, случайно попадающие в микрофон.

Корпорация Microsoft выпускает и устройства с поддержкой рукописного ввода (например, планшеты Surface). В Заявлении отмечается, что данные рукописного ввода тоже собираются, наряду с данными, вводимыми с клавиатуры.

Собираются также данные сканирования телосложения при использовании приставки Kinect и данные о количестве пройденных шагов, полученные при использовании устройств с соответствующими датчиками.

Пункт «Содержимое» Заявления представляется наиболее интересным. В нем указывается, что Microsoft собирает данные о содержимом файлов, передаваемых через сообщения электронной почты, программу Skype (включая транслируемое видео, текст и звук), и файлов (фотографий, изображений, музыки, фильмов, программного обеспечения), хранящихся в облачных хранилищах.

В пункте «Использование персональных данных» Заявления указывается, что собираемые данные подвергаются автоматизированной и ручной обработке.

Под автоматизированными методами подразумевается использование программ искусственного интеллекта (ИИ), результаты работы которых могут быть подвергнуты дополнительной ручной обработке, например, в виде прослушивания фрагментов полученных голосовых данных.

В связи с вышеизложенным вполне логично предположить, что автоматизированной обработке (т.е. анализу) подвергается весь объем собираемой информации, в т. ч. и хранящейся в виде файлов в облачных хранилищах.

Далее в Заявлении отмечается, что обработка персональных данных пользователя может производится как с согласия пользователя, так и без него: «Когда мы обрабатываем Ваши персональные данные, мы делаем это с Вашего согласия и (или) по мере необходимости для предоставления продуктов, которыми Вы пользуетесь, ведения нашей деятельности, соблюдения наших договорных и установленных законодательством обязательств, обеспечения безопасности наших систем и пользователей или исполнения других законных прав корпорации Майкрософт».

В разделе «Причины раскрытия персональных данных» Заявления указывается, что раскрытие персональных данных может быть произведено для запросов от правоохранительных органов или иных государственных организаций, в рамках судебного процесса, при угрозах жизнью и здоровью, при попытках совершения мошеннических действий, для предотвращения атак на компьютерные системы, для защиты прав или собственности корпорации Майкрософт.

По данным корпорации Microsoft, за 2020 год было получено от правоохранительных органов 24 093 запроса, связанные с 49 715 учетными записями, из которых около 20% было отклонено, для 15% не было найдено необходимой информации. При этом 1 395 удовлетворенных запросов было связано с доступом к содержимому файлов, а остальные 14 373 запроса были связаны с получением персональных данных пользователей, таких как адреса электронной почты, ФИО, почтовых и IP-адресов, данных банковских карт [8].

В апреле 2014 г. полиция США арестовала Тайлера Джеймса Хофмана, 20-летнего жителя американского штата Пенсильвания после того, как Microsoft сообщила об обнаружении в почтовом ящике его облачного хранилища OneDrive фотографии, содержащей детскую порнографию. Корпорация Microsoft сообщила о своей находке в Национальный центр пропавших и эксплуатируемых детей (National Center for Missing and Exploited Children), представители которого затем обратились в полицию. В результате проведенных следственных действий полиции удалось установить IP-адрес подозреваемого и определить место его проживания [9].

Раскрытие преступления стало возможным благодаря работе технологии PhotoDNA, разработанной в Microsoft и способной распознавать и анализировать изображения, в автоматическом режиме определяя наличие на фотографиях детской порнографии.

Подобное преступление было раскрыто и с помощью аналогичной системы, используемой корпорацией Google [10].

В подпункте «Вход в учетную запись Майкрософт» пункта «Учетная запись Майкрософт» Заявления упоминается о том, что при каждом входе в учетную запись Microsoft создается регистрационная запись входа, содержащая дату, время, имя учетной записи, уникальный идентификатор учетной записи, уникальный идентификатор устройства, с помощью которого был произведен вход, текущий IP-адрес и данные об используемом программном обеспечении. Как видно из изложенного, учитываются не только персональные данные пользователя и используемый им контент, но и идентификаторы используемого пользователем устройства.

В пункте «Как мы храним персональные данные» упоминается, что корпорация Microsoft продолжает сохранять удаленные пользователем данные на протяжении 30 суток до их окончательного удаления. Это, например, означает, что файлы, удаленные пользователем не только из папки, где они хранились, но и из папки «Корзина», будут сохраняться в неявной для пользователя форме еще 30 суток. Точно такое же правило относится и к сообщениям электронной почты.

В подпункте «Сообщила ли компания Майкрософт о том, что данные определенного типа будут храниться в соответствии с особыми условиями?» упоминается о том, что сведения об IP-адресах удаляются только через 6 месяцев, а записи об идентификаторах учетных записей и устройств – только через 18 месяцев.

В подпункте «Хранение данных» пункта «Реклама» Заявления упоминается, что используемые для подбора персонализированной рекламы данные сохраняются на протяжении 13 месяцев.

В пункте «Изменения в заявлении о конфиденциальности» упоминается о том, что текст Заявления может быть изменен в любое время и пользователям рекомендуется «регулярно перечитывать настоящее заявление о конфиденциальности». При этом корпорация Microsoft обычно оповещает о произошедших изменениях присылкой соответствующего сообщения по электронной почте.

Еще одним документом, условия которого принимаются пользователем при регистрации учетной записи, является «Соглашение об использовании служб Майкрософт» (далее – Соглашение).

Помимо того, что уже было рассмотрено выше, в Соглашении декларируется, что «Microsoft не является собственником Вашего содержимого, не контролирует, не проверяет, не оплачивает, не подтверждает его и не принимает на себя какую-либо иную ответственность за Ваше содержимое», однако в следующем же пункте указано на то, что пользователь предоставляет Microsoft «всемирную безвозмездную лицензию на использование интеллектуальной собственности, например, на копирование, сохранение, передачу, переформатирование, отображение и распространение информации» с дополнением о том, что информация пользователя «может появиться в демонстрациях или материалах, рекламирующих Службу».

При этом оговаривается, что указанное относится к информации, хранящейся на тех ресурсах пользователя, на которые он не установил ограничения. Характерно, что при этом не оговаривается, какие именно ресурсы могут считаться «широкодоступными в сети без ограничений».

Например, в папке пользователя облачного хранилища OneDrive имеется вложенная папка

защищенного хранилища («Сейф»). Можно предположить, что все остальные вложенные папки, с точки зрения Microsoft, являются «широкодоступными», так как статус широкодоступности нигде не оговаривается.

В третьем разделе («Правила поведения») в пункте a.III указано, что нежелательным поведением является рассылка спама. При этом дается определение того, что в этом соглашении считается спамом: «Спам – это нежелательная и не запрошенная почта…». Поскольку данные критерии весьма расплывчаты (сам принцип почты предусматривает получение не только запрошенных сообщений, а критерий «нежелательное сообщение» выбирается самим получателем сообщения).

Как следствие, Microsoft берется сама определять, являются ли данные сообщения электронной почты спамом, что довольно часто приводит к неожиданной блокировке учетной записи пользователя, отправившего подряд несколько электронных писем, содержащих ссылку, через облачный сервис Microsoft.

Право Microsoft на блокировку ученой записи оговорено в пункте b раздела «Правила поведения» Кроме того, в этом пункте Microsoft оставляет за собой право удалять содержимое «по любой причине». В случае проведения расследования нарушений, указанных в разделе «Правила поведения», Microsoft сохраняет за собой право просматривать сохраненную в облачных папках и в почтовых сообщениях информацию, а принявшие соглашение пользователи тем самым «уполномочивают такой пересмотр».

В четвёртом разделе Соглашения («Использование Служб и поддержки») указано, что при получении записи пользователь должен «не указывать какую-либо ложную, неточную или недостоверную информацию».

Поскольку при регистрации учетной записи Microsoft требуется указать имя, фамилию, дату рождения и номер телефона (для осуществления покупок в интернет-магазине Microsoft – и данные своей банковской карты), то выполнение этих требований дает корпорации Microsoft достаточное количество сведений для того, чтобы однозначно идентифицировать конкретного человека.

Более того, анализ данных в базах данных сможет выявить совпадения (например, в номере телефона) и тем самым определить и другие учетные записи других провайдеров ОС, принадлежащие этому же пользователю. С учетом того, что данные из баз данных довольно систематически похищаются взломщиками, эти данные пользователя могут попасть и в руки злоумышленников [11; 12].

По этой причине в целях безопасности обычно рекомендуется не указывать подлинные имена, фамилии и даты рождения, заменяя их псевдонимами, однако следование этим рекомендациям (вполне разумным) автоматически означает нарушение упомянутого выше пункта. Тем самым Microsoft получает законное основание на блокировку данных пользователя и на проведение расследования (с получением доступа к данным пользователя).

Далее в этом пункте упоминается правило, согласно которому нельзя передавать регистрационные данные своей учетной записи другим пользователям, после чего говорится о том, что пользователь «несет ответственность за все действия, которые осуществляются под Вашей учетной записью Microsoft».

С учетом упомянутой выше возможности похищения учетных записей злоумышленниками такое условие является довольно жестким и открывает возможности для дискредитации пользователя любым лицом, получившим каким-то образом доступ к данным его учетной записи.

Если пользователь решит удалить свою учетную запись, удаление его данных из хранилища будет зависеть от решения самой Microsoft: «Мы удалим Данные или Ваше содержимое, связанное с Вашей учетной записью Microsoft, *либо иным образом устраним связь* между такими данными или содержимым, Вами и Вашей учетной записью». При этом Microsoft делает оговорку, ссылаясь на случаи, когда законодательство требует сохранения данных или передачи их третьему лицу. Тем самым данный провайдер ОС не берет на себя никаких обязательств, что данные пользователя будут удалены после удаления его учетной записи.

Также как и в Заявлении, в Соглашении оговаривается их периодическое изменение (раздел «Обновления Служб или программного обеспечения и изменения настоящих Условий», п. «a»). При этом подчёркивается, что свое согласие с внесенными изменениями пользователь дает, продолжая использовать Службы (сервисы) Microsoft.

В разделе «Сторона Соглашения, выбор законодательства и места рассмотрения споров» в п. «c» «Европа, Ближний Восток и Африка» указывается, что для пользователей из европейских стран «толкование настоящих Условий, а также требования в связи с их нарушением, независимо от принципов коллизионного права, регулиру-

ются законодательством Ирландии… Вы и мы полностью соглашаемся с тем, что любые споры, связанные с настоящими Условиями или Службами, подлежат рассмотрению исключительно в судах Ирландии».

Выводы. Проведенный выше анализ показывает, что при использовании сервисов предоставляемыми провайдерами ОС можно придерживаться одной из двух тактик: либо безоговорочно довериться авторитету провайдера ОС и не принимать никаких мер, тщательно соблюдая установленные в Заявлении и Соглашении правила и надеясь на такое же тщательное их соблюдение другой стороной, либо учесть все вышеизложенное и разработать стратегию минимизации рисков, возникающих при указанных условиях.

Первый вариант осуществляется проще, но в этом случае всегда остается большой риск того, что в результате действий злоумышленников персональные данные пользователей, накопленные провайдерами ОС (ФИО пользователей, номера телефонов, место проживания, номера банковских карт, сообщения электронной почты, информация о сделанных покупках, конфигурация и состав имеющихся компьютерных устройств, информация об обращениях пользователей к сайтам государственных услуг и прочее), могут попасть в преступные руки, а от подобных взломов пострадали уже почти все крупные провайдеры ОС, включая Google [13] и Apple [14].

Второй вариант более сложен, так как требует совершения действий, несколько противоречащих требованиям, указанных в рассмотренных Заявлении и Соглашениях, в частности – требованиям указания правильных персональных данных и места проживания.

К таким действиям можно отнести использование псевдонимов при указании имени и фамилии, даты рождения, использование телефонных номеров предоплаченной мобильной связи, не связанных с подлинными персональными данными пользователя, специальных мобильных телефонов, предназначенных для обмена сообщениями только с конкретным провайдером ОС.

Шифрование всех передаваемых на хранение в облачные хранилища файлов не противоречит условиям Заявления и Соглашения и является наиболее эффективной мерой по сохранению конфиденциальности. Следует только помнить о том, что шифрование файлов должно быть произведено до их передачи в облачные хранилища (упомянутый выше «Сейф» не соответствует этому требованию), а их расшифровка – после выгрузки из облачного хранилища.

Корпорация Microsoft оговаривает возможность заключения соглашения между ней и какой-либо организацией, регулирующего порядок обработки персональных данных (при условии использования этой организацией продуктов корпорации Microsoft).

В качестве примера можно привести особые условия, принятые для продуктов Майкрософт для начального и среднего образования, в частности «Microsoft 365 для образования», в которых указано, что Microsoft не будет собирать и использовать персональные данные учащихся, не будет их продавать или сдавать в аренду, предоставлять или использовать их в рекламных целях и не будет создавать без разрешения родителей персональные профили учащихся. При этом Microsoft обязуется требовать соблюдения таких же правил и от других поставщиков образовательных услуг.

Тем самым открывается возможность для заключения договора, устраивающего обе стороны. Но поскольку большое число пользователей не связаны с какой-либо организацией, подобные меры необходимо принимать на государственном уровне (как это, например, делается в ЕС).

Список литературы:

1. Підвищте продуктивність за допомогою Microsoft Teams і Microsoft 365. URL: https://cutt.ly/pjTx8bQ (дата обращения: 17.12.2020).
2. Дьяченко В. Лицензионный договор на программное обеспечение. URL: https://cutt.ly/KjTxVJo (дата обращения: 18.12.2020).
3. Соглашение об использовании служб Майкрософт. URL: https://cutt.ly/5jknlo8 (дата обращения: 17.12.2020).
4. Заявление о конфиденциальности корпорации Майкрософт. URL: https://cutt.ly/2jknQCG (дата обращения: 17.12.2020).
5. Wi-Fi positioning system. URL: https://cutt.ly/rjTcxxI (дата обращения: 19.12.2020).
6. Wi-Fi следит за тобой, или Wi-Fi как система мониторинга. URL: https://cutt.ly/UjTcRvU (дата обращения: 19.12.2020).
7. Позиционирование в сетях Wi-Fi с высокой точностью. URL: https://cutt.ly/yjTcnOZ (дата обращения: 19.12.2020).

8. Law Enforcement Requests Report. URL: https://cutt.ly/kjTcKfl (дата обращения: 19.12.2020).
9. Microsoft прочитал почту пользователя и «сдал» его полиции. URL: https://cutt.ly/cjkn8dX (дата обращения: 10.12.2020).
10. Google «сдал» пользователя полиции, прочитав его почту. Пользователю грозит 5 лет тюрьмы. URL: https://cutt.ly/tjkmpfj (дата обращения: 10.12.2020).
11. Личные данные 267 млн пользователей Facebook оказались в свободном доступе. URL: https://cutt.ly/gjTvwAa (дата обращения: 20.12.2020).
12. Объем украденных данных в этом году вырос в несколько раз. URL: https://cutt.ly/IjTvy0D (дата обращения: 20.12.2020).
13. Google сообщила об утечке сотен тысяч паролей пользователей. URL: https://cutt.ly/djTvlI4 (дата обращения: 20.12.2020).
14. 40 млн пользователей iCloud могли стать жертвами утечки данных URL: https://cutt.ly/qjTvEy0 (дата обращения: 20.12.2020).

Chanyshev R.I. CONDITIONS OF PROVIDING CONFIDENTIALITY AND SECURITY OF USER DATA WORKING WITH CLOUD SERVICE PROVIDERS

Cloud computing appeared and began to be introduced into practice not so long ago – from about 2012. Over the years, the numerous benefits of using this technology in business, management and private (personal) use have become clear.

The nature of the use of public cloud computing involves the transfer of information from a user (individual or organization) to the storage systems of cloud providers. In this case, the user does not know exactly where the data storages used by him/her are located, and who exactly has access to them.

The terms of use of public cloud services are stipulated in the terms of service, in service use agreements, in privacy statements – the specific name of the document is chosen by the cloud provider. Terms of agreements, declarations, etc. are accepted by the user at the time of creation of an account, through which access to cloud services is provided in the form of the user's consent to the terms of the connection agreement. At the same time, the user is not required to familiarize himself with the text of the agreement, moreover, the very presence of such a text is presented in an implicit (unobtrusive) form for the user.

This article examines the content of these interconnection agreements using the example of a cloud service provider such as Microsoft, and analyzes the clauses they contain for privacy. It was revealed that the terms of such contracts provide only declarative preservation of the confidentiality of user data. In fact, they allow full access to user data not only for the cloud service providers themselves, but also for third parties. At the same time, the terms of these agreements provide for almost complete deanomization of users, which, together with the possibility of transferring data to a third party, opens up the possibility, for example, for criminal prosecution of users.

The problem is aggravated by the fact that IT specialists do not have the proper legal knowledge and often cannot provide legal assessment of the terms of these agreements.

The article provides recommendations for maintaining the confidentiality of data transferred to the cloud without violating the terms of the contract with the cloud service provider.

Key words: *cloud computing, interconnection agreements, preservation of privacy, problem of deanonymization of users, need for data encryption.*