Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова
№ 3(104) 2025 г.
Научная статья
УДК 343.98

ОСОБЕННОСТИ СОХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИСПОЛЬЗОВАНИИ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Чаплыгина Анна Дмитриевна
Московский университет МВД России имени В. Я. Кикотя, Москва, Россия

chaplygina.anya@bk.ru

Аннотация. Научная работа посвящена проблематике сохранения персональных данных при использовании электронного документооборота в деятельности правоохранительных органов. Автором проведён анализ рисков возникновения информационных опасностей при использовании электронных документов, передающихся по системам связи. Также в статье уделено внимание рассмотрению фактов утечки персональных данных и предлагаются меры по их недопущению. Описан процесс оценки уязвимостей программных средств, представлена их классификация, выделены основные направления и методы защиты персональных данных.

Ключевые слова: правоохранительные органы, органы внутренних дел, цифровая безопасность, утечка персональных данных, программные средства, защита персональных данных.

Благодарности: работа выполнена при поддержке научного руководителя – профессора кафедры предварительного расследования Московского университета МВД России имени В.Я. Кикотя, доктора юридических наук, профессора Гаврилина Б.Я.

Для цитирования: Чаплыгина А. Д. Особенности сохранения персональных данных при использовании электронного документооборота в деятельности органов внутренних дел // Научный вестник Орловского юридического института МВД России имени В. В. Лукьянова. 2025. № 3(104). С. 347–353.

FEATURES OF PERSONAL DATA PRESERVATION WHEN USING ELECTRONIC DOCUMENT FLOW IN THE ACTIVITIES OF INTERNAL AFFAIRS BODIES

Anna D. Chaplygina
V.Ya. Kikot Moscow University of the Ministry of Internal Affairs of Russia, Moscow, Russia

chaplygina.anya@bk.ru

Annotation. The article focuses on the issue of preserving personal data when using electronic document management in the activities of law enforcement agencies. The author analyzes the risks of information security hazards associated with the use of electronic documents transmitted through communication systems. The article also examines the cases of personal data leaks and proposes measures to prevent them. Additionally, the article describes the process of assessing software vulnerabilities and their classification, as well as highlights the main areas and methods of protecting personal data.

Keywords: law enforcement agencies, internal affairs agencies, digital security, personal data leakage, software, and personal data protection.

Gratitude: The work was carried out with the support of the supervisor, Professor of the Department of Preliminary Investigation at the V.Ya. Kikot Moscow University of the Ministry of Internal Affairs of Russia, Doctor of Law, Professor B.Ya. Gavrilin.

For citation: Chaplygina A. D. Features of personal data preservation when using electronic document flow in the activities of internal affairs bodies // Scientific Bulletin of the Orel Law Institute of the Ministry of Internal Affairs of Russia named after V. V. Lukyanov. 2025. № 3(104). P. 347–353.

В настоящее время мир переживает постоянную трансформацию, одной из проблем которой является безопасность общества. Человечество на протяжении своего существования всегда подвергалось опасностям различного рода, а урбанизация жизненных процессов вынуждает людей соблюдать принципы, диктуемые нам развитием информационного общества, в том числе и цифровой безопасности.

Термин «цифровая безопасность» появился одновременно с информационно-телекоммуникационными технологиями и проник в жизненные процессы, что создало условия для развития и использования электронного документооборота, в том числе и в деятельности органов внутренних дел, поставив вопрос о защите персональных данных. Перед современной государственной политикой стоит вопрос по обеспечению защиты персональных данных при использовании цифрового документооборота путём предоставления персональных данных только в законодательно определённых случаях.

Согласно п. 1 ст. 3 Федерального закона «О персональных данных»[1] ими является любая информация, относящаяся прямо или косвенно к определённому или определяемому физическому лицу (субъекту персональных данных), что даёт возможность говорить об использовании электронного документооборота в деятельности органов внутренних дел и вызывает обеспокоенность проблемой сохранения персональных данных в их деятельности. Несмотря на то, что данный законодательный акт был издан в 2006 году, до настоящего времени безопасность персональных данных остаётся под угрозой в связи с тем, что их обработка не соответствует характеру операций с использованием средств автоматизации.

Необходимо отметить, что законодатель рассматривает персональные данные как общую и специальную категорию, относя к последней информацию о состоянии здоровья субъекта персональных данных, об участии его в религиозных организациях или общественных объединениях, данные об участии субъекта в связи с осуществлением в отношении него оперативно-разыскной деятельности и пр. Отметим, что обработка персональных данных из специальной категории лиц должна быть незамедлительно прекращена при утрате оснований для их проведения.

При этом следует исходить из того, что толкование понятия персональных данных предполагает признание их через непосредственную идентификацию физической личности человека и данных электронного документооборота, лежащих в основе функционирования, и в частности, органов внутренних дел. Проблему защиты информации в системах электронного документооборота можно решить лишь через сохранение целостности присутствующей информации, в том числе и персональных данных. Также перед органами внутренних дел стоит задача по устранению нарушений конфиденциальности персональных данных, влекущих их доступность.

Говоря об утечке персональных данных, стоит отметить возможность их использования при совершении мошеннических действий, создающих угрозы для экономической стабильности страны и населения. Однако у правоохранительных органов в целом и у органов внутренних дел в частности возникают проблемы по созданию систем со-

[1] О персональных данных[Электронный ресурс]: Федер. закон Рос. Федерации от 27 июля 2011 г. № 261-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

хранности персональных данных при использовании цифрового документооборота. Полагаем, что цифровой документооборот должен представлять единый механизм по работе с электронными документами и обеспечивать реализацию модели «безбумажного делопроизводства» в их деятельности путём введения, например, «электронного уголовного дела».

Согласно ст. 17 Федерального закона Российской Федерации «О полиции»[1] органы внутренних дел имеют право на обработку персональных данных при реализации трудовых и служебных отношений, а также в связи с оказанием государственных услуг и осуществлением государственных функций в соответствии с целями и в отношении категорий субъектов, предусмотренных нормативно-правовыми актами Российской Федерации. При этом законодатель не использует категорию «персональные данные», хотя, по сути, их накопление и происходит, что связано с тем, что общественные отношения, в рамках которых происходит обработка данной информации, имеют свою особенность: в них публично-правовые начала превалируют над частными правовыми.

В свою очередь, Министерством внутренних дел Российской Федерации (далее - МВД России) были изданы ведомственные нормативные правовые акты[2], определяющие меры, направленные на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных». «Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы» также предусмотрела введение электронного документооборота в структуры государственных учреждений[3].

Попутно заметим, что правоприменители в своей деятельности часто сталкиваются со сложностями восприятия определения «персональные данные» из-за его терминологической объёмной конструкции и невозможности понимания, в каких случаях можно считать персональными данными ту или иную информацию, а также определения типа возникающих угроз. Следует иметь в виду, что к электронному документообороту, используемому в деятельности правоохранительных органов Российской Федерации, предъявляются определённые требования в части степени его защиты. Так, руководитель органа внутренних дел либо его заместитель имеет возможность самостоятельно определить тип угроз для персональных данных или поручить разработчику программного обеспечения спроектировать модель угроз.

Список персональных данных, обрабатываемых в системе МВД России, указан в нормативных правовых актах и является открытым в связи с тем, что субъект персональных данных имеет право дополнительно сообщить иные сведения о себе [1]. Для каждой из целей обработки персональных данных определяется их содержание исходя из соответствующей категории субъектов, к которым относятся все должности рядового и начальствующего состава органов внутренних дел и должности федеральной государственной гражданской службы, если в их обязанности входит обработка персональных данных или осуществление доступа к ним.

В этой части МВД России установлен порядок защиты персональных данных, полученных при реализации трудовых, служебных сообщений или возникающих в связи с оказанием государственных услуг, при предоставлении их третьим лицам.

---

[1] О полиции [Электронный ресурс]: Федер. закон Рос. Федерации от 7 февраля 2011 г. № 3-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] О некоторых мерах, направленных на обеспечение выполнения МВД России обязанностей, предусмотренных Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» [Электронный ресурс]: приказ МВД России от 21 декабря 2017 г. № 949. Доступ из справ.-правовой системы «КонсультантПлюс».

[3] Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы [Электронный ресурс]: Указ Президента Рос. Федерации от 9 мая 2017 г. № 203. Доступ из справ.-правовой системы «КонсультантПлюс».

По межведомственным запросам органов государственной власти и органов местного самоуправления, предоставляющих государственные или муниципальные услуги, в обязательном порядке предоставляются сведения о наличии у лица непогашенной или неснятой судимости. Также МВД России по запросу в рамках расследуемых уголовных дел и находящихся в производстве дел об административных правонарушениях, а также в связи с проверкой зарегистрированных в установленном порядке заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях, разрешение которых отнесено к компетенции полиции, имеет право запрашивать и получать на безвозмездной основе по мотивированному запросу уполномоченных должностных лиц полиции от государственных и муниципальных органов, общественных объединений, организаций, должностных лиц и граждан сведения, справки, документы (их копии), иную необходимую информацию, в том числе персональные данные граждан, за исключением случаев, когда федеральным законом установлен специальный порядок получения информации.

Одним из главных параметров персональных данных является электронная подпись, внедрённая в работу государственных, частных социальных и юридических структур и служащая для оформления любого правового акта без особых затрат вне зависимости от территориального присутствия [2, с. 9]. Она позволяет экономить временные и финансовые ресурсы, однако наряду с явными преимуществами её использования в рамках облегчения процесса оформления документов цифровая подпись имеет ряд недостатков в её применении, заключающихся в формировании новой формации информационной безопасности.

Электронной подписью является информация в электронной форме, присоединённая к другой информации в электронной форме или иным образом связанная с такой информацией и используемая для определения лица, подписывающего информацию. В свою очередь, в соответствии со ст. 5 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» квалифицированной электронной подписью является «электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам: ключ проверки электронной подписи указан в квалифицированном сертификате; для создания и проверки электронной подписи используются средства электронной подписи, имеющие подтверждение требованиям, установленным в соответствии с этим нормативным правовым актом»[1]. Данный тезис подчёркивает, что не любой документ может быть переведён в электронную форму. Он должен сохранить юридическую силу и влечь за собой определённые последствия правового содержания. Любые материалы, прилагаемые к обращениям лиц, участвующих в уголовном процессе, также должны быть обличены в форму электронного документа. В противном случае исключается возможность использования такой процессуальной формы при создании документов.

Соблюдая стандартные принципы безопасного поведения в условиях стремительно развивающейся цифровизации, необходимо сформулировать и задачи безопасности цифровой среды:

1. Идентификация цифровой опасности, выраженная в обнаружении угроз и вызовов путём считывания их возникших характеристик.
2. Препятствование возникновению вероятного риска.
3. Обеспечение гарантий цифровой безопасности жизнедеятельности путём защиты от угрозы и вызовов, исходящих от цифровой среды [3, с. 12].

Идентификация цифровых опасностей должна проводиться через призму рассмотрения существования стандартных опасностей в жизнедеятельности общества, при

[1] Об электронной подписи [Электронный ресурс]: Федер. закон Рос. Федерации от 6 апреля 2011 г. № 63-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

том что их отличие заключается в сущности самой опасности в виде утечки персональных данных, вторжения в частную жизнь, угрозы завладением интеллектуальной собственностью и прочих [4, с. 87]. Таким образом, гарантией цифровой безопасности жизнедеятельности должны выступать меры, направленные на защиту информации и решение проблем уязвимости в самом программном обеспечении.

Термин «уязвимость» применяется для описания изъяна в системе, который разрушает общую структуру процесса и провоцирует отклонение от правильности функционирования. Уязвимости в программном обеспечении могут выражаться в ошибке программиста в написании кода программы, неправильных расчётах в создании системы, в вирусах, проникших в программное обеспечение, в слабых паролях [5, с. 76].

К основным видам цифровых уязвимостей относятся: висячие указатели, переполнение буфера, обход каталогов, ошибки форматирующей строки, уязвимость нулевого дня, гонки символьных ссылок, ошибки времени, межсайтовый скриптинг в веб-приложениях, подделка межсайтовых запросов в веб-приложениях, неверная поддержка интерпретации метасимволов командной оболочки и пр.

Для поиска подходящего решения по защите персональных данных необходимо понимать, с какими уязвимостями цифровой информации при осуществлении электронного документооборота можно встретиться в том или ином случае. В 2024 году «Лаборатория Касперского» опубликовала статистические данные, указывающие на обнаружение уязвимостей в программном обеспечении [6], позволившие провести классификацию уязвимостей программных средств и выделить три основных направления защиты:

1. Исключение ошибок при составлении программного кода, который не содержит встроенных средств защиты программного продукта.
2. Исключение внедрения вирусных вредоносных программных продуктов, полученных из сторонних источников и через интернет-приложения.
3. Повышение ответственности и добросовестности сотрудников учреждений, которые имеют доступ к персональным данным.

Однако, кроме цифровых уязвимостей, существующих в программном обеспечении органов внутренних дел, необходимо выделить и типы цифровых угроз:

- присутствие недекларированных возможностей в информационном обеспечении, установленном в информационных системах персональных данных;
- присутствие недокументированных возможностей в системном программном обеспечении, установленном в информационных системах персональных данных;
- угрозы, не связанные с наличием неявных возможностей во всех типах программного обеспечения [7].

Внедрение в деятельность правоохранительных органов автоматизированного документооборота указывает на необходимость помнить об обеспечении сохранности персональных данных путём использования проверенного и безопасного способа их хранения и использования. При реализации деятельности в органах внутренних дел, в которых в настоящее время активно ведётся электронный документооборот, необходимо уделять внимание проверке информационных ресурсов, на которых пользователи оставляют свои персональные данные, пользоваться исключительно лицензионным отечественным программным обеспечением, своевременно обновляя антивирусные программы, а также обеспечивать многоступенчатую систему аутентификации.

---

1. Обработка персональных данных в органах внутренних дел https://23.мвд.рф/document/13650184 // https://xn--b1amdelgbarlac.23.xn--b1aew.xn--p1ai/document/64283462

2. Кузнецова И. О., Нестеренко И. С., Нестеренко Г. А. Особенности сохранения персональных данных при использовании цифрового документооборота // Международный научно-исследовательский журнал. 2025. № 1. С. 8–15
3. Горлов А. П. Гулак М. Л., Лексиков Е. В. [и др.] Сущность комплексного подхода к разработке системы защиты информации // Информационная безопасность и защита персональных данных. Проблемы и пути их решения: Сборник материалов и докладов XV межрегиональной научно-практической конференции, Брянск, 28 апреля 2023 года / Под общ. ред. О.М. Голембиовской. Брянск: Брянский государственный технический университет, 2023. С. 83–87.
4. Ушаков Н.О., Сибикина И. В., Космачева И. М. Информационная безопасность в системах электронного документооборота // Техническая эксплуатация водного транспорта: проблемы и пути развития : Материалы Третьей международной научно-технической конференции, Петропавловск-Камчатский, 26 ноября 2020 года / Отв. за выпуск О.А. Белов. Петропавловск-Камчатский: Камчатский государственный технический университет, 2021. С. 70-74.
5. Security Week 2420: эксплуатация уязвимостей в ПО // https://habr.com/ru/companies/kaspersky/articles/814065/
6. Защита персональных данных в СЭД / https://searchinform.ru/resheniya/biznes-zadachi/zaschita-personalnykh-dannykh/realizaciya-zashchity-personalnyh-dannyh/perechen-personalnyh-dannyh-podlezhashchih-zashchite/zaschita-personalnykh-dannykh-v-sed/

1. Obrabotka personal`ny`x danny`x v organax vnutrennix del https://23.mvd.rf/document/13650184 // https://xn--b1amdelgbarlac.23.xn--b1aew.xn--p1ai/document/64283462
2. Kuzneczova I. O., Nesterenko I. S., Nesterenko G. A. Osobennosti soxraneniya personal`ny`x danny`x pri ispol`zovanii cifrovogo dokumentooborota // Mezhdunarodny`j nauchno-issledovatel`skij zhurnal. 2025. № 1. S. 8–15
3. Gorlov A. P. Gulak M. L., Leksikov E. V. [i dr.] Sushhnost` kompleksnogo podxoda k razrabotke sistemy` zashhity` informacii // Informacionnaya bezopasnost` i zashhita personal`ny`x danny`x. Problemy` i puti ix resheniya: Sbornik materialov i dokladov XV mezhregional`noj nauchno-prakticheskoj konferencii, Bryansk, 28 aprelya 2023 goda / Pod obshh. red. O.M. Golembiovskoj. Bryansk: Bryanskij gosudarstvenny`j texnicheskij universitet, 2023. S. 83–87.
4. Ushakov N.O., Sibikina I. V., Kosmacheva I. M. Informacionnaya bezopasnost` v sistemax e`lektronnogo dokumentooborota // Texnicheskaya e`kspluataciya vodnogo transporta: problemy` i puti razvitiya : Materialy` Tret`ej mezhdunarodnoj nauchno-texnicheskoj konferencii, Petropavlovsk-Kamchatskij, 26 noyabrya 2020 goda / Otv. za vy`pusk O.A. Belov. Petropavlovsk-Kamchatskij: Kamchatskij gosudarstvenny`j texnicheskij universitet, 2021. S. 70-74.
5. Security Week 2420: e`kspluataciya uyazvimostej v PO // https://habr.com/ru/companies/kaspersky/articles/814065/
6. Zashhita personal`ny`x danny`x v SE`D / https://searchinform.ru/resheniya/biznes-zadachi/zaschita-personalnykh-dannykh/realizaciya-zashchity-personalnyh-dannyh/perechen-personalnyh-dannyh-podlezhashchih-zashchite/zaschita-personalnykh-dannykh-v-sed/

Информация об авторе

Анна Дмитриевна Чаплыгина. Адъюнкт.
Московский университет МВД России имени В. Я. Кикотя.
117437, Россия, Москва, ул. Академика Волгина, д. 12.

Information about the author

Anna D. Chaplygina. Adjunct.
Kikot Moscow University of the Ministry of Internal Affairs of Russia.
117437, Russia, Moscow, Akademika Volgina Str., 12.

Статья поступила в редакцию 04.08.2025; одобрена после рецензирования 15.09.2025; принята к публикации 29.09.2025.

The article was received in the editorial office on 04.08.2025; approved after review on 15.09.2025; accepted for publication on 29.09.2025.