МЕРЫ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Рекомендовано учебно-методическим объединением в сфере дополнительного образования взрослых по группе специальностей 0421 Право

Под редакцией А. А. Гаева, М. А. Городецкой

Минск
РИВШ
2025

УДК 34.03:004.056(075.9)
ББК 67.04:16.82я73
М52

А в т о р ы :

А. И. Гавриленко, Д. Н. Гайкевич, В. И. Диско, Н. С. Журов,
М. Г. Коршекевич, В. В. Кузуро

Р е ц е н з е н т ы :

директор Института управленческих кадров
Академии управления при Президенте Республики Беларусь,
кандидат юридических наук *С. В. Апанасевич*;

главный советник экспертно-правового управления
Государственного секретариата Совета Безопасности Республики Беларусь,
кандидат юридических наук, доцент *М. А. Дубко*;

декан факультета повышения квалификации и переподготовки
Института информационных технологий
Белорусского государственного университета информатики
и радиоэлектроники, кандидат экономических наук, доцент *А. И. Ящук*

Меры по обеспечению защиты персональных данных:
М52 учебное пособие / А. И. Гавриленко, Д. Н. Гайкевич, В. И. Диско [и др.]; под общ. ред. А. А. Гаева, М. А. Городецкой. – Минск: РИВШ, 2025. – 78 с.

ISBN 978-985-586-919-2.

В учебном пособии дается общая характеристика требований законодательства о персональных данных в отношении системы мер по защите персональных данных, разъясняется суть риск-ориентированного подхода, заложенного в Законе о персональных данных, подробно излагается содержание законодательных требований по реализации мер по обеспечению защиты персональных данных, предлагаются возможные варианты их реализации на практике. Особое внимание уделено типичным ошибкам, которые допускают операторы (уполномоченные лица) при реализации требований законодательства о персональных данных.

Адресовано слушателям, проходящим повышение квалификации в Национальном центре защиты персональных данных Республики Беларусь по учебным программам «Защита персональных данных» и «Защита персональных данных в банках и небанковских кредитно-финансовых организациях». Может быть полезным для преподавателей, обучающихся учреждений высшего образования, учреждений дополнительного образования взрослых.

УДК 34.03:004.056(075.9)
ББК 67.04:16.82я73

ISBN 978-985-586-919-2

СОДЕРЖАНИЕ

СПИСОК ИСПОЛЬЗОВАННЫХ СОКРАЩЕНИЙ

абз.	– абзац
ГИР (С)	– государственный информационный ресурс (система)
ГИР Реестр операторов	– государственный информационный ресурс «Реестр операторов персональных данных»
Закон о персональных данных	– Закон Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных» (с изм. и доп. Закона Республики Беларусь от 1 июня 2022 г. № 175-З)
Закон об информации, информатизации и защите информации	– Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» (с изм. и доп. Закона Республики Беларусь от 10 октября 2022 г. № 209-З)
ИР	– информационный ресурс
ИР (С)	– информационный ресурс (система)
ИС	– информационная система
ОАЦ	– Оперативно-аналитический центр при Президенте Республики Беларусь
п.	– пункт
подп.	– подпункт
Положение о порядке технической и криптографической защиты информации	– Положение о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденное приказом ОАЦ от 20 февраля 2020 г. № 66
политика	– документ, определяющий политику оператора (уполномоченного лица) в отношении обработки персональных данных

Приказ директора Центра от 15 ноября 2021 г. № 12	– приказ директора Национального центра защиты персональных данных Республики Беларусь от 15 ноября 2021 г. № 12 «О классификации информационных ресурсов (систем)»
Приказ директора Центра от 15 ноября 2021 г. № 13	– приказ директора Национального центра защиты персональных данных Республики Беларусь от 15 ноября 2021 г. № 13 «Об уведомлении о нарушениях систем защиты персональных данных»
Приказ ОАЦ № 94	– приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 1 июня 2022 г. № 94 «О государственном информационном ресурсе «Реестр операторов персональных данных»
ст.	– статья
Указ № 422	– Указ Президента Республики Беларусь от 28 октября 2021 г. № 422 (с изм. и доп. Указа Президента Республики Беларусь от 5 февраля 2024 г. № 46) «О мерах по совершенствованию защиты персональных данных»
Центр (если не указано иное)	– Национальный центр защиты персональных данных Республики Беларусь
ч.	– часть

ПРЕДИСЛОВИЕ

Закон о персональных данных, установивший обязанность операторов (уполномоченных лиц) принять необходимые меры по обеспечению защиты персональных данных, вступил в силу в Беларуси более трех лет назад, в ноябре 2021 г. Однако на практике вопросы принятия (реализации) необходимых мер по защите персональных данных все еще остаются актуальными, о чем свидетельствуют проводимые Центром контрольные мероприятия.

Реализация мер по обеспечению защиты персональных данных представляет собой одно из ключевых направлений, нацеленных на соблюдение законодательства о персональных данных. Более того, реализация таких мер позволяет обеспечить баланс интересов субъектов персональных данных и лиц, осуществляющих их обработку.

Учебное пособие подготовлено в рамках проводимой Центром работы по правовому просвещению и разъяснению законодательства о персональных данных.

Издание ориентировано в первую очередь на слушателей, проходящих повышение квалификации по учебным программам «Защита персональных данных» и «Защита персональных данных в банках и небанковских кредитно-финансовых организациях», разработанным и утвержденным в Национальном центре защиты персональных данных Республики Беларусь.

При этом об актуальности подготовленного учебного пособия свидетельствует опыт организации образовательного процесса в учреждениях высшего образования, учреждениях дополнительного образования взрослых, в учебно-тематических планах и учебных программах которых с появлением и развитием законодательства о персональных данных стали появляться соответствующие учебные занятия и (или) дисциплины. Учитывая сказанное, издание может стать полезным как для преподавателей, так и для обучающихся указанных учреждений образования.

С учетом практико-ориентированного характера издания оно может использоваться как руководство при выстраивании на практике системы защиты персональных данных и быть востребованным среди руководителей и работников, ответственных за осуществление внутреннего контроля за обработкой персональных данных.

Учебное пособие подготовлено в дополнение к разработанным в Центре постатейному комментарию к Закону Республики Беларусь «О защите персональных данных» (2023) и учебному пособию «Защита персональных данных», получившему гриф Министерства образования в 2024 г.

Структурно издание состоит из предисловия, раскрывающего его актуальность; четырнадцати параграфов, в которых дается общая характеристика требований законодательства о персональных данных в отношении системы мер по защите персональных данных, разъясняется суть риск-ориентированного подхода, заложенного в Законе о персональных данных, а затем подробно излагается содержание законодательных требований по реализации мер по обеспечению защиты персональных данных, предлагаются возможные варианты их реализации на практике. Особое внимание уделено типичным ошибкам, которые допускают операторы (уполномоченные лица) при реализации требований законодательства о персональных данных.

Для более удобного восприятия представленного в учебном пособии текста он сопровождается QR-кодами, ведущими читателя на интернет-сайты, содержащие необходимые (описываемые по тексту) формы документов, разъяснения, рекомендации и т. п. Кроме того, в завершении каждого параграфа приводятся тезисы о лучших практиках и типичных нарушениях при применении законодательства о персональных данных.

Важной частью учебного пособия является предлагаемая читателю библиография, включающая перечень нормативных правовых актов, разъяснений и рекомендаций Национального центра защиты персональных данных, научных и научно-практических публикаций (статьи, научные труды, материалы) по заявленной тематике. Она будет полезна при самостоятельном изучении отдельных вопросов защиты персональных данных, подготовке учебно-программной документации, проведении научных исследований.

Выражаем надежду, что издание будет полезным читателю!

§ 1. ОБЩАЯ ХАРАКТЕРИСТИКА МЕР ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

В нынешних реалиях персональные данные признаются ценным активом, который нуждается в не меньшей охране, чем материальные активы организации. Недостаточно внимательное отношение к работе с личной информацией, пренебрежение мерами защиты персональных данных могут повлечь несанкционированный доступ к ним, утечку, распространение этих сведений и причинение гражданам других неблагоприятных для них последствий (манипулирование, мошенничество, угрозы и т. п.), а также значительные репутационные и материальные издержки организаций.

Проводимый Центром анализ реализуемых юридическими лицами мероприятий по защите обрабатываемых ими персональных данных показывает, что многие нарушения обусловлены незнанием или ошибочным представлением о допустимых пределах использования и хранения таких данных, неосведомленностью о положениях нормативных правовых актов, регулирующих эти вопросы, и в целом нереализацией предусмотренных законодательством обязательных мер по обеспечению защиты персональных данных[1].

Обеспечение защиты персональных данных включает принятие правовых, организационных и технических мер (п. 1 ст. 17 Закона о персональных данных) (рис. 1).

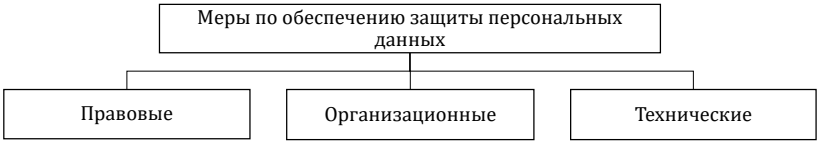

Рис. 1. **Меры по обеспечению защиты персональных данных**

К правовым мерам относится разработка и принятие (издание, установление) оператором совокупности документов по вопросам защиты персональных данных (издание политик, принятие поло-

[1] Специалист по защите персональных данных в организации: задачи, функции, образование. Подробный гайд для операторов. – URL: https://cpd.by/specialist-po-zashhite-personalnyh-dannyh-v-organizacii-zadachi-funkcii-obrazovanie-podrobnyj-gajd-dlja-operatorov/. – Дата публ.: 28.07.2023 (дата обращения: 01.04.2025).

жения о порядке осуществления внутреннего контроля за обработкой персональных данных, установление и поддержание в актуальном состоянии перечня уполномоченных лиц, разработка форм согласий субъектов персональных данных и т. п.).

Организационные меры охватывают мероприятия по разграничению доступа к персональным данным, в том числе обрабатываемым в информационном ресурсе (системе), ознакомлению и обучению работников и иных лиц положениям законодательства о персональных данных, политик, осуществлению внутреннего контроля за обработкой персональных данных, ведению реестра обработок персональных данных и т. п.

Под техническими мерами понимаются мероприятия, направленные на осуществление технической и криптографической защиты персональных данных.

Вместе с тем распределение мер по обеспечению защиты персональных данных на три указанные группы является достаточно условным. Так, например, п. 2 и 3 ст. 5 Закона о персональных данных предусмотрена возможность получения согласия не только в письменной форме, в виде электронного документа, но и в иной электронной форме, например посредством проставления субъектом персональных данных соответствующей отметки на интернет-ресурсе (абз. 2 п. 3 ст. 5). Реализация согласия в такой форме потребует от лица, привлеченного для этой цели, определенных знаний и умений в IT-сфере, в связи с чем такая мера может быть отнесена в большей степени к техническим мерам, чем к правовым.

Закон о персональных данных не содержит исчерпывающего перечня мер, принятие которых безусловно свидетельствует о выполнении оператором (уполномоченным лицом) обязанности по обеспечению защиты персональных данных. Определение такого перечня не представляется возможным в связи с многообразием и спецификой сфер деятельности операторов (уполномоченных лиц), масштабов обработки персональных данных, ее способов, категорий персональных данных, потенциальных рисков, связанных с обработкой персональных данных, и иных обстоятельств. С учетом этого каждый оператор (уполномоченное лицо) должен самостоятельно определить состав и перечень мер, необходимых и достаточных для выполнения им обязанностей по обеспечению защиты персональных данных, с учетом тех, соблюдение которых обязательно для всех операторов (уполномоченных лиц) (п. 3 ст. 17 Закона о персональных данных).

Таким образом, установленная в Законе о персональных данных модель определения достаточности мер по обеспечению защиты персональных данных обусловлена риск-ориентированным подходом, что позволяет оператору (уполномоченному лицу) гибко подходить к вопросу защиты персональных данных с учетом специфики своей деятельности и иных важных факторов.

При этом оператор (уполномоченное лицо) не полностью свободен в выборе упомянутых мер, поскольку п. 3 ст. 17 Закона о персональных данных и подп. 3.5 и 3.6 п. 3 Указа № 422 закрепляют ряд из них, которые носят обязательный характер.

В частности, п. 3 ст. 17 Закона о персональных данных определены следующие обязательные меры по обеспечению защиты персональных данных:

1) назначение оператором (уполномоченным лицом), являющимся государственным органом, юридическим лицом Республики Беларусь, иной организацией, структурного подразделения или лица, ответственного за осуществление внутреннего контроля за обработкой персональных данных (далее, если не определено иное, – ответственный за контроль);

2) издание оператором (уполномоченным лицом), являющимся юридическим лицом Республики Беларусь, иной организацией, индивидуальным предпринимателем, политик;

3) ознакомление работников оператора (уполномоченного лица) и иных лиц, непосредственно осуществляющих обработку персональных данных, с положениями законодательства о персональных данных, в том числе с требованиями по защите персональных данных, политиками, а также обучение указанных работников и иных лиц в порядке, установленном законодательством (далее, если не определено иное, – ознакомление и обучение);

4) установление порядка доступа к персональным данным, в том числе обрабатываемым в информационном ресурсе (системе);

5) осуществление технической и криптографической защиты персональных данных в порядке, установленном ОАЦ, в соответствии с классификацией информационных ресурсов (систем), содержащих персональные данные.

Специалистами справедливо отмечается, что обязательные меры по обеспечению защиты персональных данных, предусмотренные п. 3 ст. 17 Закона о персональных данных, составляют «сердцевину» мероприятий, принимаемых оператором для обра-

ботки персональных данных в соответствии с требованиями Закона о персональных данных[2].

Кроме того, отдельные меры по обеспечению защиты персональных данных прямо не названы в законодательстве, однако вытекают из обязанностей оператора, предусмотренных ст. 16 Закона о персональных данных. В частности, указанной статьей предусматриваются обязанности:

• уведомлять Центр о нарушениях систем защиты персональных данных незамедлительно, но не позднее трех рабочих дней после того, как оператору стало известно о таких нарушениях;

• прекращать обработку персональных данных, а также осуществлять их удаление или блокирование (обеспечивать прекращение обработки персональных данных, а также их удаление или блокирование уполномоченным лицом) при отсутствии оснований для обработки персональных данных, предусмотренных Законом о персональных данных и иными законодательными актами; и т. д.

Как уже отмечалось ранее, ряд мер по обеспечению защиты персональных данных, носящих обязательный характер, нашел отражение не только в Законе о персональных данных, но и в Указе № 422.

Согласно подп. 3.5 п. 3 Указа № 422 операторы, являющиеся государственными органами, юридическими лицами Республики Беларусь, иными организациями, устанавливают и поддерживают в актуальном состоянии:

а) перечень информационных ресурсов (систем), содержащих персональные данные, собственниками (владельцами) которых они являются;

б) категории персональных данных, подлежащих включению в такие ресурсы (системы):

• общедоступные персональные данные;

• специальные персональные данные (кроме биометрических и генетических персональных данных);

• биометрические и генетические персональные данные;

• персональные данные, не являющиеся общедоступными или специальными;

в) перечень уполномоченных лиц, если обработка персональных данных осуществляется уполномоченными лицами;

г) срок хранения обрабатываемых персональных данных.

---

[2] *Диско, В. И.* Типичные нарушения законодательства о персональных данных / В. И. Диско // Юстиция Беларуси. – 2024. – № 10. – С. 11–14.

Подпунктом 3.6 п. 3 Указа № 422 устанавливается обязанность операторов вносить в создаваемый Центром ГИР Реестр операторов сведения об информационных ресурсах (системах), содержащих персональные данные, а также обеспечивать актуализацию соответствующих сведений. Виды информационных ресурсов (систем), сведения о которых подлежат внесению в реестр, а также перечень включаемых в него сведений и срок их внесения в реестр определяются ОАЦ (см. подробнее об этом в § 12).

Для удобства операторов (уполномоченных лиц) при организации работы по приведению их деятельности в соответствие с требованиями Закона о персональных данных разработан и размещен на официальном сайте Центра соответствующий пошаговый алгоритм действий (доступен для скачивания в разделе «Правовая основа/Методологические документы»).

В настоящем учебном пособии читателю предлагается рассмотреть меры по обеспечению защиты персональных данных в следующем порядке:

1) назначение оператором (уполномоченным лицом), являющимся государственным органом, юридическим лицом Республики Беларусь, иной организацией, ответственного за контроль (абз. 2 п. 3 ст. 17 Закона о персональных данных);

2) выявление, фиксация и анализ бизнес-процессов, в которых обрабатываются персональные данные;

3) издание оператором (уполномоченным лицом), являющимся юридическим лицом Республики Беларусь, иной организацией, индивидуальным предпринимателем, политик;

4) ознакомление работников оператора (уполномоченного лица) и иных лиц, непосредственно осуществляющих обработку персональных данных, с положениями законодательства о персональных данных, в том числе с требованиями по защите персональных данных, политик, а также обучение указанных работников и иных лиц в порядке, установленном законодательством;

5) внесение изменений в должностные обязанности лиц, обрабатывающих персональные данные;

6) установление порядка доступа к персональным данным, в том числе обрабатываемым в информационном ресурсе (системе) (абз. 5 п. 3 ст. 17 Закона о персональных данных);

7) осуществление технической и криптографической защиты персональных данных в порядке, установленном ОАЦ, в соответствии с классификацией информационных ресурсов (систем), со-

держащих персональные данные (абз. 6 п. 3 ст. 17 Закона о персональных данных);

8) установление и поддержание в актуальном состоянии перечня информационных ресурсов (систем), содержащих персональные данные, собственниками (владельцами) которых является оператор, а также категорий персональных данных, подлежащих включению в данные ресурсы (системы);

9) установление и поддержание в актуальном состоянии перечня уполномоченных лиц, если обработка персональных данных осуществляется такими лицами;

10) внесение операторами сведений об информационных ресурсах (системах), содержащих персональные данные, в ГИР Реестр операторов, а также обеспечение актуализации соответствующих сведений;

11) обеспечение учета фактов предоставления персональных данных третьим лицам;

12) уведомление Центра о нарушениях систем защиты персональных данных.

В то же время следует учитывать, что полное и исчерпывающее осуществление данных мер еще не означает надлежащее построение системы защиты персональных данных в организации. При обработке персональных данных необходимо также принимать во внимание иные требования, предъявляемые к ней Законом о персональных данных (например, ст. 4, п. 3 ст. 8).

Формальный подход к реализации законодательных требований в сфере защиты персональных данных, в том числе утверждение шаблонов документов без их адаптации к конкретным бизнес-процессам оператора, не обеспечит такую защиту. Как показывает анализ проводимой Центром контрольной деятельности, многие из выявляемых им на практике нарушений при реализации обязательных мер по обеспечению защиты персональных данных носят типичный характер, поскольку допускаются операторами (уполномоченными лицами) вне зависимости от масштабов обработки персональных данных, сфер их деятельности, а также имеющихся ресурсов.

В соответствии с положениями Указа № 422 Центр при осуществлении контроля в обязательном порядке делает вывод о достаточности принятых мер для защиты персональных данных и их соответствии требованиям законодательства о персональных данных. При этом нередко в актах, оформляемых по итогам про-

веденных проверок, приходится констатировать недостаточность принятых оператором мер по обеспечению защиты персональных данных в связи с формальным подходом к их реализации. К сожалению, обобщение результатов контрольной деятельности свидетельствует порой о значительном разрыве между положениями локальных правовых актов оператора и фактическим положением дел в отношении обработки персональных данных.

Важно понимать, что принятые единожды решения, с учетом изменения законодательства, бизнес-процессов и т. п., подлежат регулярному пересмотру и актуализации с целью повышения их эффективности.

§ 2. НАЗНАЧЕНИЕ ОТВЕТСТВЕННОГО ЗА ОСУЩЕСТВЛЕНИЕ ВНУТРЕННЕГО КОНТРОЛЯ ЗА ОБРАБОТКОЙ ПЕРСОНАЛЬНЫХ ДАННЫХ

Внутренний контроль за обработкой персональных данных (далее – внутренний контроль) можно назвать одним из основных инструментов обеспечения надлежащего соблюдения обязанностей, возложенных на операторов (уполномоченных лиц) Законом о персональных данных. Его реальное осуществление помогает организации выявить риски, связанные с защитой персональных данных, и предотвратить возможные нарушения законодательства о персональных данных, в том числе их утечку.

Назначение ответственного за контроль (также имеет наименование DPO (англ.) – Data Protection Officer) в соответствии с абз. 2 п. 3 ст. 17 Закона о персональных данных является одной из обязательных мер по обеспечению защиты персональных данных.

При этом в соответствии с Законом о персональных данных обязанность по назначению ответственного за контроль возложена на государственные органы, юридические лица Республики Беларусь и иные организации. Операторы (уполномоченные лица) из числа физических лиц, включая индивидуальных предпринимателей, адвокатов, нотариусов, ремесленников, репетиторов, медиаторов и т. п., такое лицо назначать не обязаны.

На ответственного за контроль возлагаются организационные, консультативные, контрольные, информационно-образовательные и иные функции, связанные с проведением комплексной работы по обеспечению соблюдения законодательства о персональных данных (рис. 2).

Рис. 2. **Функции ответственного за контроль**

К *организационным функциям* ответственного за контроль относятся:

• изучение и анализ процессов обработки персональных данных;

• определение рисков, связанных с процессами обработки персональных данных, выработка предложений по их минимизации;

• разработка и поддержание в актуальном состоянии документов в сфере обработки персональных данных и т. д.

Консультативные функции включат в себя:

• консультирование руководителей, иных работников организации;

• взаимодействие с уполномоченными лицами по вопросам обработки и защиты персональных данных;

• согласование локальных правовых актов, договоров на предмет их соответствия законодательству о персональных данных и т. д.

К *контрольным функциям* относятся:

• проведение проверок по соблюдению требований законодательства о персональных данных и локальных правовых актов оператора (уполномоченного лица) в структурных подразделениях организации для выявления нарушений и предупреждения их совершения;

• контроль за своевременным внесением работниками изменений в персональные данные, которые являются неполными, устаревшими или неточными, прекращением обработки персональных данных, а также осуществлением их удаления или блокирования при отсутствии оснований для обработки персональных данных, предусмотренных законодательными актами;

• контроль за предоставлением персональных данных третьим лицам и ведением учета таких фактов;

• уведомление руководства о выявленных нарушениях законодательства о персональных данных;

• проведение расследований по фактам нарушений работниками требований обработки персональных данных.

К *информационно-образовательным функциям* такого лица относятся:

• ознакомление работников и иных лиц, непосредственно осуществляющих обработку персональных данных, с законодательством о персональных данных, в том числе с требованиями по защите персональных данных, политиками;

• организация прохождения обучения с контролем знаний работников, осуществляющих обработку персональных данных, по вопросам обработки и защиты персональных данных в порядке, установленном законодательством;

• определение оптимальных форм обучения работников, исходя из их должностных обязанностей.

Осуществление *иных функций* ответственного за контроль предусматривает:

• рассмотрение (участие в рассмотрении) заявлений и жалоб субъектов персональных данных по вопросам обработки персональных данных;

• принятие необходимых мер по восстановлению их нарушенных прав;

• обеспечение взаимодействия с Центром[3].

Соответствующие функции перечислены в Едином квалификационном справочнике должностей служащих «Должности служащих для всех видов деятельности», утвержденном постановлением Министерства труда Республики Беларусь от 30 декабря 1999 г. № 159, при описании квалификационной характеристики *специалиста по внутреннему контролю за обработкой персональных данных*.

В соответствии с квалификационной характеристикой соответствующий специалист должен иметь высшее образование. Вместе с тем, принимая во внимание стоящие перед ответственным за контроль задачи, он должен назначаться с учетом знания законодательства о персональных данных и практики его применения, понимания бизнес-процессов оператора (уполномоченного лица), в которых обрабатываются персональные данные, наличия представления об используемых оператором (уполномоченным лицом) информационных системах, их защите, а также способности выполнять упомянутые функции.

Примерная должностная инструкция для специалиста по внутреннему контролю

Примерная должностная инструкция для специалиста по внутреннему контролю размещена на сайте Центра в разделе «Портфель оператора». Данная инструкция может быть использована и при составлении должностной инструкции ответственного за

[3] Постатейный комментарий к Закону Республики Беларусь «О защите персональных данных» // Методологические документы. Официальный сайт Национального центра защиты персональных данных Республики Беларусь. – URL: https://cpd.by/pravovaya-osnova/metodologicheskiye-dokumenty-rekomendatsii/postatejnyj-kommentarij-k-zakonu-respubliki-belarus-o-zashhite-personalnyh-dannyh/ (дата обращения: 01.04.2025).

контроль, занимающего иную должность (в случае, если функции ответственного за контроль возложены на неосвобожденного работника).

Закон о персональных данных не предусматривает конкретных вариантов или критериев его назначения, что объясняется разнообразием условий функционирования и возможностей операторов (уполномоченных лиц).

На практике возможны следующие модели назначения ответственного за контроль:

- создание отдельного структурного подразделения;
- назначение освобожденного работника;
- возложение дополнительных функций на одного из работников;
- возложение дополнительных функций на нескольких работников;
- возложение дополнительных функций на существующее структурное подразделение (рис. 3)[4].

При этом выбор модели назначения ответственного за контроль должен осуществляться исходя:

- из специфики деятельности оператора;
- масштабов обработки персональных данных;
- возможности эффективно выполнять возлагаемые функции и т. п[5].

Создание отдельного структурного подразделения либо назначение освобожденного работника целесообразно в случаях:

- масштабной обработки персональных данных;
- обработки биометрических и генетических персональных данных;
- привлечения значительного числа уполномоченных лиц;
- системного осуществления трансграничной передачи персональных данных;

---

[4] Защита персональных данных: учеб. пособие / А. А. Гаев, С. В. Задиран, М. Г. Коршекевич [и др.]; под общ. ред. М. Г. Коршекевича, М. А. Городецкой. – Минск: РИВШ, 2024. – С. 63.

[5] Постатейный комментарий к Закону Республики Беларусь «О защите персональных данных» // Методологические документы. Официальный сайт Национального центра защиты персональных данных Республики Беларусь. – URL: https://cpd.by/pravovaya-osnova/metodologicheskiye-dokumenty-rekomendatsii/postatejnyj-kommentarij-k-zakonu-respubliki-belarus-o-zashhite-personalnyh-dannyh/ (дата обращения: 01.04.2025).

• повышенного риска нарушения прав субъектов персональных данных (обработки значительного объема специальных персональных данных, персональных данных несовершеннолетних и др.).

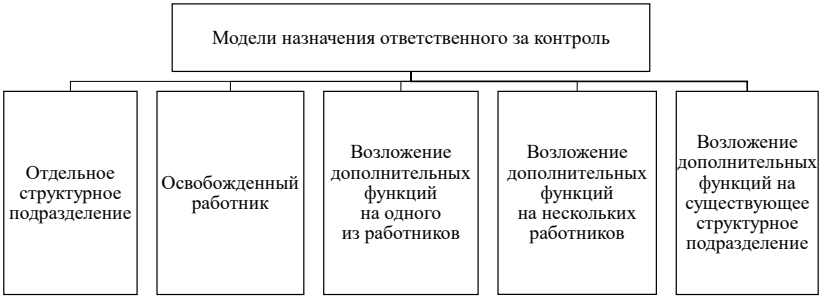

Рис. 3. **Модели назначения ответственного за контроль**

Возложение дополнительных функций на одного из работников. Данный вариант назначения ответственного за контроль не должен привести к формальному изданию приказа о возложении обязанностей на работника без фактического осуществления им упомянутых функций. Кроме того, непосредственная обработка персональных данных не должна быть основной задачей деятельности такого лица (следует исключить конфликт интересов, т. е. совпадение контролера и контролируемого в одном лице).

В связи с этим назначение ответственного за контроль из числа руководителей организации (их заместителей), а также структурных подразделений или работников, основные функции которых связаны с обработкой большого объема персональных данных (например, кадровые и бухгалтерские службы, структурные подразделения по работе с обращениями граждан и т. п.), допустимо, только если иным образом невозможно обеспечить реализацию соответствующей меры (например, иные работники не обладают достаточным уровнем квалификации).

Более того, такой работник должен иметь не только глубокие знания законодательства о персональных данных, но также объективную возможность выполнять соответствующие функции с учетом уже имеющихся должностных обязанностей.

На практике для эффективного осуществления внутреннего контроля за обработкой персональных данных также важным является выстраивание надлежащей коммуникации со всеми работниками (структурными подразделениями).

Возложение дополнительных функций на нескольких работников. На практике, как правило, данная модель реализуется посредством возложения дополнительных функций на двух работников:

• на одного (например, юрисконсульт) – в части организационных и правовых мер;

• на другого (например, специалист, ответственный за обеспечение защиты информации) – в части реализации технических мер (мероприятий по осуществлению технической и криптографической защиты персональных данных).

При таком варианте требуется четкое распределение функций между указанными лицами, исключение дублирования в их деятельности. Кроме того, у назначенных работников также должна быть объективная возможность выполнять соответствующие функции с учетом уже имеющихся должностных обязанностей.

Как было отмечено ранее, в рамках осуществления внутреннего контроля допускается *возложение дополнительных функций на ранее созданное структурное подразделение*, специализирующееся на выполнении иных задач. В этой связи необходимо учитывать, что выбор подразделения, на которое будет возложено осуществление такого контроля, должен зависеть от ряда факторов, первоочередным из которых является наличие или отсутствие обработки значительного количества персональных данных.

В качестве дополнительных критериев выбора следует выделить степень осведомленности и компетентности работников такого подразделения в вопросах защиты персональных данных (например, достаточный уровень знаний ими законодательства, требований, предъявляемых к обработке персональных данных в конкретных бизнес-процессах); их загруженность с учетом основной работы. Допускается также ситуация, когда лишь отдельные направления внутреннего контроля передаются структурному подразделению (например, контроль соблюдения мер технической и криптографической защиты персональных данных).

Вместе с тем ответственность за достаточность предпринимаемых таким структурным подразделением мер в рамках внутреннего контроля не должна «размываться». Это означает, что за осуществление внутреннего контроля, его эффективность в первую очередь отвечает руководитель такого подразделения (начальник управления, заведующий сектором и др.). Такой руководитель в рамках распределения обязанностей между работниками подразделения определяет конкретных работников, реализующих соот-

ветствующую функцию подразделения (в том числе обязанности таких работников по осуществлению внутреннего контроля, которые закрепляются в их должностных инструкциях).

При этом следует учитывать, что выбор оператором (уполномоченным лицом) любой модели назначения ответственного за контроль должен обеспечить эффективный, действенный контроль за обработкой персональных данных в рамках оператора и достаточность принимаемых мер для защиты персональных данных.

Ключевым аспектом, который должен быть также учтен вне зависимости от выбранной модели назначения ответственного за контроль, является обеспечение его независимости в осуществлении внутреннего контроля, что вытекает из сущности данного института. Без соблюдения этого условия соответствующая обязательная мера не может быть должным образом реализована.

Независимость ответственного за контроль может быть достигнута во многом за счет:

• обеспечения его непосредственной подчиненности руководителю организации или его заместителю;

• недопущения вмешательства в его деятельность со стороны иных должностных лиц (структурных подразделений);

• наделения ответственного за контроль полномочием принимать по вопросам, входящим в его компетенцию, решения, обязательные для исполнения работниками и иными лицами, непосредственно осуществляющими обработку персональных данных;

• предоставления достаточных ресурсов для выполнения своих задач;

• закрепления обязательного согласования с ответственным за контроль документов, касающихся вопросов обработки персональных данных (договоры, локальные правовые акты и др.), а также наделения его правом инициирования внесения изменений в такие документы.

Важно, чтобы такое лицо (структурное подразделение) имело достаточные ресурсы (организационные, временные и т. п.) для исполнения своих функций[6].

В организации должен быть разработан и утвержден порядок осуществления внутреннего контроля, включающий в том числе и план проведения внутреннего контроля. Такой локальный правовой акт должен иметь своей целью не столько выявление нару-

[6] *Диско, В. И.* Типичные нарушения законодательства о персональных данных / В. И. Диско // Юстиция Беларуси. – 2024. – № 10. – С. 11–14.

Примерное Положение о порядке осуществления внутреннего контроля

шений, сколько их предупреждение. Иными словами, работники оператора (уполномоченного лица), зная порядок проведения внутреннего контроля, его период, объекты, подлежащие контролю, могут провести анализ своей деятельности и исключить нарушения до их выявления соответствующим лицом (структурным подразделением).

Отметим, что в связи с назначением ответственного за контроль ни оператор, ни уполномоченное лицо, ни их работники, непосредственно осуществляющие обработку персональных данных, не освобождаются от ответственности, предусмотренной законодательными актами, за допущенные ими нарушения.

Типичные ошибки:

1. Отсутствие лица (структурного подразделения), ответственного за контроль.

2. Отсутствие утвержденного в организации порядка осуществления внутреннего контроля.

3. Фактическое непроведение внутреннего контроля, что подтверждается отсутствием документов о его проведении (планов проведения, докладных записок, отчетов по итогам проведения).

4. Формальное возложение обязанностей по осуществлению внутреннего контроля на работника, который не имеет знания законодательства о персональных данных (предполагающего, как правило, наличие юридического образования) и практики его применения.

§ 3. ВЫЯВЛЕНИЕ, ФИКСАЦИЯ И АНАЛИЗ БИЗНЕС-ПРОЦЕССОВ, В КОТОРЫХ ОБРАБАТЫВАЮТСЯ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

С целью обеспечения эффективного контроля за обработкой персональных данных оператором (уполномоченным лицом) рекомендуется провести инвентаризацию и систематизацию процессов обработки персональных данных и в дальнейшем поддерживать их учет в актуальном состоянии. Это может быть обеспечено с помощью ведения реестра обработки персональных данных или иной формы систематизации процессов обработки (далее, если не указано иное, – реестр).

Эта мера не предусмотрена в качестве обязательной для реализации операторами (уполномоченными лицами). Вместе с тем отсутствие такого реестра порождает сложность в реализации положений ст. 4 и 17 Закона о персональных данных и прав субъектов персональных данных (например, права на получение информации, касающейся обработки персональных данных).

Кроме того, учет всех процессов обработки персональных данных посредством реестра служит фундаментом для создания надлежащей системы защиты персональных данных в организации, упрощает издание политик, подготовку договоров с уполномоченными лицами, локальных правовых актов, организационно-распорядительной документации, реализацию мер по технической защите персональных данных.

На практике нередко реестр обработки персональных данных рассматривается как основа для организации внутреннего контроля и обучения работников[7].

В этой связи для большинства операторов (уполномоченных лиц) целесообразно принятие локального правового акта (например, положения) о реестре обработки персональных данных, в котором следует определить:

[7] По итогам митапа «Внутренний контроль за обработкой персональных данных: анализ практики и перспективы развития» // Ilex. – URL: https://cpd.by/opublikovany-tezisy-po-itogam-mitapa-vnutrennij-kontrol-za-obrabotkoj-personalnyh-dannyh-analiz-praktiki-i-perspektivy-razvitija/. – Дата публ.: 23.11.2023 (дата обращения: 01.04.2025).

• порядок взаимодействия профильных структурных подразделений со структурным подразделением или лицом, ответственным за контроль, по вопросам ведения реестра;

• механизм актуализации реестра;

• форму реестра;

• порядок его применения в служебной (трудовой) деятельности работников и структурных подразделений (в том числе ответственность за поддержание соответствующих разделов реестра в актуальном состоянии с учетом их компетенции и функциональных обязанностей).

Примерное положение о реестре

В самом реестре в отношении каждого самостоятельного процесса обработки персональных данных целесообразно указать следующую информацию:

• цель обработки персональных данных;

• подразделение (лицо), ответственное за конкретную обработку;

• категории лиц, чьи персональные данные обрабатываются (клиенты, работники, бывшие работники, соискатели на трудоустройство, стороны гражданско-правовых договоров (клиенты, контрагенты), посетители интернет-сайта и др.);

• категории обрабатываемых персональных данных (отражается конкретный перечень персональных данных);

• правовые основания обработки (указывается конкретное правовое основание, предусмотренное Законом о персональных данных, а при применении в качестве правового основания абз. 20 или 21 ст. 6 либо абз. 17 или 18 п. 2 ст. 8 Закона о персональных данных дополнительно отражается конкретный структурный элемент законодательного акта и (или) принятого в его развитие акта законодательства);

Примерная форма реестра

• источник получения персональных данных;

• категории получателей персональных данных;

• срок хранения персональных данных.

Структура реестра может быть определена оператором (уполномоченным лицом) самостоятельно.

Примерная форма реестра размещена на официальном сайте Центра и доступна для ознакомления и скачивания по предлагаемому QR-коду.

Важно не только создать реестр, но и поддерживать его в актуальном состоянии. Поэтому после выявления и фиксации новых бизнес-процессов, в которых обрабатываются персональные данные, или изменения действующих бизнес-процессов реестр необходимо дополнять или изменять, а также проводить систематический анализ обработки на предмет соответствия требованиям законодательства о персональных данных.

В частности, деятельность по актуализации реестра следует проводить по следующим направлениям:

• формулирование конкретных целей обработки персональных данных;

• определение правовых оснований для обработки персональных данных исходя из ее цели;

• оценка соразмерности и неизбыточности обрабатываемых персональных данных по отношению к цели обработки;

• обеспечение соответствия получаемых согласий на обработку персональных данных требованиям ст. 5 Закона о персональных данных, если обработка осуществляется на основании согласия;

• определение сроков хранения персональных данных исходя из целей обработки, а также с учетом возможности дальнейшей трансформации правового основания и возникновения у оператора (уполномоченного лица) обязанности хранить персональные данные в рамках сроков, определенных в постановлении Министерства юстиции Республики Беларусь от 24 мая 2012 г. № 140 «О перечне типовых документов», иных актах законодательства. В случае, если сроки хранения не установлены законодательством, установление (уточнение) соответствующего срока осуществляется оператором с учетом п. 8 ст. 4 Закона о персональных данных;

• обеспечение наличия правовых оснований для предоставления персональных данных уполномоченным лицам (договор, решение государственного органа, акт законодательства), а также иным лицам (самостоятельным операторам, сооператорам и т. п.).

При отсутствии правовых оснований для обработки, превышении срока хранения, избыточности обрабатываемых персональных данных такие данные подлежат удалению. В случае отсутствия технической возможности удаления персональных данных необхо-

димо принять меры по недопущению дальнейшей обработки персональных данных, включая их блокирование.

Лучшие практики:

1. Вовлечение в процесс ведения реестра руководителей (работников) структурных подразделений организации после их ознакомления (обучения) с положениями законодательства о персональных данных.

2. Назначение во всех структурных подразделениях работника, ответственного за предоставление сведений в реестр (его ведение, ревизию) в части, касающейся деятельности каждого из структурных подразделений.

3. Поддержание реестра в актуальном состоянии, внесение в него (учет) новых целей обработки, исключение неактуальных.

Типичные ошибки:

1. Отсутствие реестра или формальный подход к его составлению.

2. Несоответствие реестра фактическому положению дел в рамках обработки персональных данных.

3. Некорректное определение правовых оснований для обработки персональных данных.

4. Неучет бизнес-процессов, в которых организация выступает уполномоченным лицом.

§ 4. УДАЛЕНИЕ (БЛОКИРОВАНИЕ) ПЕРСОНАЛЬНЫХ ДАННЫХ

Под *удалением* персональных данных понимаются действия, в результате которых становится невозможным восстановить персональные данные в ИР (С), содержащих персональные данные, и (или) в результате которых уничтожаются материальные носители персональных данных (абз. 15 ст. 1 Закона о персональных данных).

В соответствии с абз. 7 п. 1 ст. 16 Закона о персональных данных оператор обязан прекращать обработку персональных данных, а также осуществлять их удаление или блокирование (обеспечивать прекращение обработки персональных данных, а также их удаление или блокирование уполномоченным лицом) при отсутствии оснований для обработки персональных данных, предусмотренных Законом о персональных данных и иными законодательными актами. Возникновение такой обязанности включает и случаи, когда субъект персональных данных реализует свое право на отзыв согласия на обработку персональных данных или заявляет требование о прекращении обработки персональных данных.

Кроме того, указанная обязанность оператора обусловлена требованием к обработке персональных данных, установленным п. 8 ст. 4 Закона о персональных данных.

Механизм удаления такой информации в значительной степени зависит от того, в каком виде и в каких документах содержатся персональные данные.

Процедура уничтожения документов, содержащих персональные данные, включенных в номенклатуру дел с установленными сроками хранения, предусмотрена:

- Законом Республики Беларусь от 25 ноября 2011 г. № 323-З «Об архивном деле и делопроизводстве»;
- главой 16 Инструкции по делопроизводству в государственных органах, иных организациях, утвержденной постановлением Министерства юстиции Республики Беларусь от 19 января 2009 г. № 4;
- Инструкцией о порядке работы с электронными документами в государственных органах, иных организациях, утвержденной постановлением Министерства юстиции Республики Беларусь от 6 февраля 2019 г. № 19, и др.

Порядок удаления информации из информационных систем (ресурсов) в законодательстве не определен, за исключением отдельных ГИР (С).

Поэтому оператор в целях выполнения соответствующей обязанности при отсутствии правового регулирования вправе самостоятельно определить порядок удаления персональных данных, например в локальном правовом акте, определяющем порядок функционирования ИР (С).

При этом составление акта об удалении персональных данных целесообразно только в случаях разового удаления персональных данных, например на основании заявления субъекта персональных данных, требования Центра, в иных случаях, когда необходимо подтвердить факт совершения этого действия.

В случае автоматического удаления персональных данных из ИР (С) в документе, определяющем порядок удаления персональных данных, достаточно указать сроки хранения этой информации. Примером подобного удаления является осуществление записи изображения посредством системы видеонаблюдения в циклическом режиме, когда самые старые записи заменяются новыми.

В иных случаях оператору следует создавать лог-файлы и настраивать их ведение таким образом, чтобы в эти файлы вносились записи об удалении персональных данных, но без информации, позволяющей идентифицировать физических лиц (например, запись сведений о дате удаления и объеме удаленных сведений).

Удаление персональных данных из ИР (С) должно осуществляться таким образом, чтобы их восстановление было невозможным. Например, простое «*перемещение в корзину*» не является надлежащим выполнением обязанности по удалению персональных данных.

При этом сама по себе возможность применения специальных технических средств по восстановлению информации не рассматривается как невыполнение оператором обязанности по удалению персональных данных.

При отсутствии технической возможности удаления персональных данных оператор обязан принять меры по недопущению дальнейшей обработки персональных данных, включая их блокирование (ч. 2 п. 2 ст. 10, ч. 2 п. 2 ст. 13 Закона о персональных данных).

Блокирование персональных данных определено как прекращение доступа к персональным данным без их удаления (абз. 3 ст. 1 Закона о персональных данных). По своим последствиям блоки-

рование является равнозначным удалению и должно исключать использование, предоставление, распространение персональных данных и др.

В отличие от удаления персональных данных, когда либо сам носитель данных уничтожается, либо данные необратимо стираются или иным образом удаляются (без возможности их восстановления), при блокировании персональные данные сохраняются. При этом администратором ресурса (системы) ограничивается доступ к таким данным, и в дальнейшем они хранятся без возможности их использования, предоставления, распространения и т. п.

Вместе с тем блокирование может применяться и в иных случаях, например при наличии жалобы на неправомерную обработку, на оценку ситуации, по которой требуется время. В этой связи блокирование позволяет исключить продолжение потенциально незаконной обработки. По итогам рассмотрения жалобы обработка может быть продолжена либо данные будут удалены.

Лучшие практики:

1. Обеспечение подтверждения удаления персональных данных (например, в акте, содержащем информацию о дате удаления, перечне удаленных персональных данных, количестве субъектов персональных данных, чьи данные удалены).

2. Ревизия на систематической основе ответственным за контроль ИР (С), функционирующих в организации, на предмет обработки в них ПД, подлежащих удалению.

Типичные ошибки:

1. Сбор и хранение документов, содержащих персональные данные, «про запас».

2. По истечении срока хранения персональных данных использование обезличивания (либо блокирования) вместо удаления (при наличии возможности удаления).

3. Необоснованное дублирование персональных данных в различных информационных ресурсах (системах) одного и того же оператора.

§ 5. ИЗДАНИЕ ДОКУМЕНТОВ, ОПРЕДЕЛЯЮЩИХ ПОЛИТИКУ В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Обработка персональных данных должна носить прозрачный характер. В этих целях субъекту персональных данных в случаях, предусмотренных Законом о персональных данных, предоставляется соответствующая информация, касающаяся обработки его персональных данных (п. 6 ст. 4 Закона о персональных данных).

Реализация принципа прозрачности также лежит в основе обязанности оператора по изданию политики.

Соответствующая обязательная мера предусмотрена абз. 3 п. 3 ст. 17 Закона о персональных данных и позволяет исключить неосведомленность субъектов персональных данных относительно действий оператора с их персональными данными.

В целях формирования единообразных подходов к структуре и форме политики Центром разработаны Разъяснения по составлению документа, определяющего политику оператора (уполномоченного лица) в отношении обработки персональных данных (доступны по ссылке через QR-код).

Разъяснения по составлению документа, определяющего политику оператора (уполномоченного лица) в отношении обработки персональных данных (пункт 2)

Политика должна позволять субъектам персональных данных понимать, кем, как и для каких целей их персональные данные собираются, используются или иным образом обрабатываются, а также отражать имеющиеся у субъектов персональных данных права в контексте этой обработки и механизм их реализации.

Политика оператора должна быть написана простым, ясным и доступным языком без использования абстрактных и неоднозначных формулировок.

В зависимости от основных целей обработки персональных данных по отдельным бизнес-процессам целесообразно издать самостоятельные политики:

• политику в отношении обработки персональных данных работников, бывших работников;

• политику в отношении обработки персональных данных при осуществлении административных процедур (в отношении «внешнего» контура);

• политику в отношении обработки cookie-файлов;

• политику видеонаблюдения;

• политику в отношении обработки персональных данных в рамках программы лояльности;

• политику в отношении обработки персональных данных кандидатов на трудоустройство и др.

Центром разработан ряд примерных политик, которые могут быть использованы операторами (уполномоченными лицами) при реализации ими указанной меры.

В политику целесообразно включать следующую информацию (структурные элементы):

• общие положения;

• порядок и условия обработки персональных данных;

• об уполномоченных лицах;

• о трансграничной передаче персональных данных;

• права субъектов персональных данных и механизмы их реализации.

В политике указываются перечень осуществляемых оператором (уполномоченным лицом) действий с персональными данными, источник получения персональных данных, цели обработки персональных данных, а также иная информация в соответствии с Разъяснениями по составлению документа, определяющего политику оператора (уполномоченного лица) в отношении обработки персональных данных.

Политика Центра в отношении обработки cookie-файлов

Примерная политика видеонаблюдения для УДО, УСО

Примерная политика в отношении обработки персональных данных в процессе трудовой деятельности и при осуществлении административных процедур

Для обеспечения большей доступности и наглядности политики следует обеспечить соотношение целей и правовых оснований обработки, категорий субъектов персональных данных, чьи данные подвергаются обработке, перечня обрабатываемых персональных данных и конкретных сроков обработки в форме, удобной для восприятия субъектами персональных данных (например, в табличной форме (таблица 1 и 2)).

Кроме того, в случае значительного объема излагаемого материала и при наличии технической возможности целесообразно использовать многоуровневый подход (например, раскрытие на интернет-сайте раздела (рубрики) информации при нажатии на него).

Цели и правовые основания обработки персональных данных должны быть конкретными, законными и формулироваться до начала обработки персональных данных. Не допускается указание абстрактных или общих целей, которые не определяют пределов обработки и не позволяют субъекту персональных данных понять, для чего будут обрабатываться его персональные данные.

Например, не соответствуют критерию конкретности такие формулировки, как «совершенствование деятельности организации», «разработка новых услуг», «достижение общественно значимых целей», «реализация Устава» и т. п.

В случае если оператор поручает обработку персональных данных уполномоченному лицу (уполномоченным лицам), то в политике подлежит отражению следующая информация:

- наименование и местонахождение уполномоченного лица (уполномоченных лиц), а при невозможности указания данной информации из-за большого количества уполномоченных лиц, динамичности или краткосрочности договорных отношений – категории уполномоченных лиц;
- цели обработки персональных данных уполномоченным лицом.

При намерении осуществлять трансграничную передачу персональных данных в политике отражаются применительно к каждой цели передачи персональных данных:

- субъекты (категории субъектов) в иностранных государствах, которым персональные данные могут быть переданы;
- страны, на территории которых находятся такие субъекты (категории субъектов);
- передаваемые персональные данные;
- правовые основания для трансграничной передачи.

Таблица 1

Пример обеспечения соотношения целей и правовых оснований обработки, категорий субъектов персональных данных, чьи данные подвергаются обработке, перечня обрабатываемых персональных данных и конкретных сроков обработки

№ п/п	Цель обработки персональных данных	Категория субъектов персональных данных, чьи данные подвергаются обработке	Перечень обрабатываемых персональных данных	Правовые основания обработки персональных данных	Срок хранения персональных данных	Образующиеся документы (копии документов) и места их хранения	ИР (С)
1							
2							
3							
4							
5							
…							

Таблица 2

Пример обеспечения соотношения целей и правовых оснований обработки, категорий субъектов персональных данных, чьи данные подвергаются обработке, перечня обрабатываемых персональных данных и конкретных сроков обработки

	Оформление (прием на работу)	
	Категории субъектов персональных данных, чьи данные подвергаются обработке	Соискатели на трудоустройство, члены их семей
	Перечень обрабатываемых персональных данных	В соответствии со ст. 26 Трудового кодекса Республики Беларусь, п. 11 Декрета Президента Республики Беларусь от 15 декабря 2014 г. № 5 «Об усилении требований к руководящим кадрам и работникам организаций», иными законодательными актами
	Правовые основания обработки персональных данных	Обработка персональных данных при оформлении трудовых отношений (абз. 8 ст. 6, абз. 3 п. 2 ст. 8 Закона)
	Срок хранения персональных данных	После увольнения – 55 лет

Если трансграничная передача персональных данных не осуществляется, информация об этом также отражается в Политике.

Помимо издания политики на оператора (уполномоченное лицо) возложена обязанность по обеспечению неограниченного доступа к ней, в том числе с использованием глобальной компьютерной сети Интернет. При этом в случае отсутствия интернет-сайта у оператора создание его для целей размещения политики не требуется.

Реализация указанного требования должна осуществляться с учетом круга субъектов персональных данных, на которых она распространяется.

Так, политику в отношении «внешнего контура» (клиентов, контрагентов, граждан, направляющих обращения, и т. п.) следует разместить на интернет-сайте организации. При этом необходимо учитывать, что такая информация должна находиться на интернет-сайте на странице не ниже второго уровня (например, в меню на главной странице, в «футере» и т. п.). Дополнительно соответствующая информация может размещаться на иных интернет-ресурсах или распространяться другими способами.

При наличии у оператора (уполномоченного лица) нескольких интернет-сайтов следует публиковать политику на каждом из них (а в случае подготовки нескольких политик по отдельным направлениям – политику применительно к бизнес-процессу, связанному с данным интернет-сайтом).

Иной подход может быть применен к политике в отношении работников, бывших работников. Нет необходимости размещать такой документ в открытом доступе для неограниченного круга лиц. В этом случае допустимо опубликовать соответствующий документ на корпоративном портале (при его наличии), разместить его в сетевой папке, на информационных стендах, а также обеспечить доступ к нему заинтересованных лиц иными способами.

Отметим, что политика должна поддерживаться в актуальном состоянии. В случае, если в содержание политики вносятся существенные изменения, включая изменение целей обработки персональных данных, сроков их хранения, порядка реализации прав субъектов персональных данных, условий трансграничной передачи, они должны доводиться до сведения субъектов персональных данных до вступления в силу таких изменений.

Издание политики и, соответственно, обеспечение к ней неограниченного доступа необязательно для государственных органов и физических лиц, за исключением индивидуальных предприни-

мателей (абз. 8 и 16 ст. 1, абз. 3 п. 3 и п. 4 ст. 17 Закона о персональных данных). Однако реализация данной меры указанными операторами (уполномоченными лицами), в особенности государственными органами, уже стала распространенной практикой и приветствуется.

Лучшие практики:

1. Разработка и поддержание в актуальном состоянии политики (политик) для основных бизнес-процессов оператора. Размещение ее (их) на своем сайте в сети Интернет.

2. Составление нескольких политик в зависимости от специфики определенных бизнес-процессов.

3. Обеспечение удобства восприятия политики (политик) на сайте (например, раскрытие раздела (рубрики) информации при нажатии на него, возможность поиска по тексту и т. п.).

4. Доступность предыдущих редакций политики на сайте.

Типичные ошибки:

1. Отсутствие политики (политик), необеспечение неограниченного доступа к ней (ним), в том числе с использованием глобальной компьютерной сети Интернет.

2. Отсутствие в политике соотношения целей обработки, категорий субъектов персональных данных, чьи данные подвергаются обработке, перечня обрабатываемых персональных данных (в частности, изложение целей обработки, категорий субъектов персональных данных, перечня обрабатываемых сведений, правовых оснований в различных пунктах документа).

3. Отсутствие указания в политике всех бизнес-процессов, в ходе которых осуществляется обработка персональных данных.

4. Отсутствие политики по обработке персональных данных в трудовых отношениях либо отсутствие политики видеонаблюдения при его осуществлении.

5. Принятие одной политики в случае наличия значительного количества процессов по обработке либо изложение ее сложным юридическим или техническим языком, исключающим понимание его субъектами персональных данных, чьи данные обрабатываются в соответствии с этой политикой.

6. Указание слишком общих (неконкретных) целей обработки («обеспечение соблюдения законодательства», «осуществление своей деятельности в соответствии с Уставом»).

7. Неуказание сроков обработки персональных данных либо указание неконкретных сроков («не дольше, чем этого требуют

цели обработки персональных данных, кроме случаев, когда срок хранения персональных данных установлен законодательством», «согласие действует до момента отзыва этого согласия либо до момента, установленного законодательством»).

8. Отсутствие в политике информации об уполномоченных лицах, трансграничной передаче персональных данных, правах субъектов персональных данных.

9. Неуказание механизма реализации прав субъектов персональных данных, в том числе неуказание контактных данных лица, ответственного за контроль.

10. Дублирование положений Закона о персональных данных (например, ст. 1, 4 и 6) без их конкретизации применительно к деятельности оператора, приведение положений, изложенных с учетом подходов российского или европейского законодательства (например, «обработка персональных данных на основании легитимного интереса»).

11. Несоответствие положений политики (политик) реальным процессам.

12. Опубликование на разных страницах интернет-сайта разных версий политик по одним и тем же бизнес-процессам.

§ 6. ОЗНАКОМЛЕНИЕ И ОБУЧЕНИЕ РАБОТНИКОВ

В соответствии с абз. 4 п. 3 ст. 17 Закона о персональных данных одной из обязательных мер по обеспечению защиты персональных данных является ознакомление работников оператора (уполномоченного лица) и иных лиц, непосредственно осуществляющих обработку персональных данных, с положениями законодательства о персональных данных, в том числе с требованиями по защите персональных данных, политиками, а также обучение указанных работников и иных лиц в порядке, установленном законодательством.

Приступая к рассмотрению указанной меры, следует отметить, что она включает в себя два самостоятельных мероприятия: ознакомление и обучение.

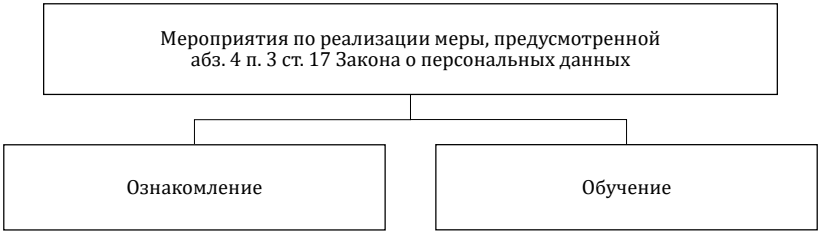

Рис. 4. **Мероприятия, направленные на реализацию меры, предусмотренной абз. 4 п. 3 ст. 17 Закона о персональных данных**

В любой организации большинство работников, выполняя возложенные должностные обязанности, осуществляют обработку персональных данных. Бывают ситуации, когда работники совершают правонарушения, незаконно распространяя или предоставляя такие данные по незнанию или из-за ошибочного представления о допустимых пределах их использования и хранения, неосведомленности о положениях нормативных правовых актов, регулирующих эти вопросы.

В связи с указанным важно ознакомить работников с законодательством о персональных данных и обучить правильному его применению[8].

[8] *Пырко, И. А.* Типичные нарушения при обработке персональных данных в трудовых отношениях. По итогам практической конференции / И. А. Пырко // Iiex. – Дата публ.: 10.10.2023 (дата обращения: 01.04.2025).

Реализация данной меры предусмотрена абз. 4 п. 3 ст. 17 Закона о персональных данных и направлена на формирование понимания работниками и иными лицами, непосредственно осуществляющими обработку персональных данных, сути возлагаемых на них обязанностей, связанных с обработкой персональных данных. Данная обязанность распространяется как на действующих, так и на вновь принятых работников.

Так, ознакомление осуществляется:

- с положениями законодательства о персональных данных (Закон о персональных данных, отдельные положения Указа № 422, иные акты законодательства, имеющие значение для выполнения функций по обработке персональных данных конкретным работником), в том числе требованиями по обеспечению защиты персональных данных (меры, предусмотренные ст. 17 Закона о персональных данных, а также иные меры, предусмотренные законодательством). Кроме того, целесообразно доводить информацию о мерах ответственности, предусмотренных Трудовым кодексом Республики Беларусь, Кодексом Республики Беларусь об административных правонарушениях и Уголовным кодексом Республики Беларусь);
- политикой (политиками).

Необходимо также ознакомить работников и иных лиц, непосредственно осуществляющих обработку персональных данных, и с иными документами (локальными правовыми актами) оператора (уполномоченного лица) по вопросам защиты персональных данных (например, с положениями о порядке осуществления внутреннего контроля, ведения реестра обработок персональных данных, политикой в процессе трудовой деятельности, порядком доступа к персональным данным, документами, регламентирующими порядок учета предоставления персональных данных третьим лицам, и т. п.).

Целесообразно обеспечить «адресный» характер ознакомления, то есть адаптировать его для разных категорий работников в зависимости от их функциональных обязанностей.

Например, для работников маркетингового подразделения актуальными являются соответствующие положения Закона Республики Беларусь от 10 мая 2007 г. № 225-З «О рекламе» (ст. 12 указанного Закона), а также Разъяснения Центра об обработке персональных данных при направлении рекламной рассылки с использованием абонентского номера, адреса электронной почты

Разъяснения Центра об обработке персональных данных при направлении рекламнои рассылки с использованием абонентского номера, адреса электронной почты

(с ними можно ознакомиться по ссылке через QR-код).

При этом ознакомление должно осуществляться в отношении:

• работников оператора (уполномоченного лица), непосредственно осуществляющих обработку персональных данных;

• иных лиц, непосредственно осуществляющих обработку персональных данных (лицами, которые работают в организации по гражданско-правовому договору и не являются уполномоченными лицами, практикантами).

Вместе с тем само по себе ознакомление может не иметь желаемого результата, в связи с чем данная мера дополняется законодательно установленным требованием о проведении обучения соответствующих лиц.

Подход к организации такого обучения, в том числе его периодичности, определен в подп. 3.3 п. 3 Указа № 422.

Категории лиц, обучаемых непосредственно в Центре, определены приказом ОАЦ от 12 ноября 2021 г. № 194 «Об обучении по вопросам защиты персональных данных».

К ним относятся лица, ответственные за контроль:

• в банках и небанковских кредитно-финансовых организациях;

• в страховых организациях;

• у операторов электросвязи (за исключением индивидуальных предпринимателей);

• в Республиканской и территориальных организациях по государственной регистрации недвижимого имущества, прав на него и сделок с ним;

• в Белорусской нотариальной палате, областных (Минской городской) нотариальных палатах;

• в риэлтерских организациях;

• в организациях здравоохранения;

• в организациях, осуществляющих гостиничное обслуживание;

• в организациях, осуществляющих туристическую деятельность;

• в организациях, оказывающих услуги по содействию в трудоустройстве;

• в организациях, осуществляющих обработку биометрических и (или) генетических персональных данных;

• в местных исполнительных и распорядительных органах (за исключением сельских (поселковых) исполнительных комитетов), их структурных подразделениях с правами юридического лица;

• у операторов (уполномоченных лиц), организующих и (или) осуществляющих обработку персональных данных не менее 10 тыс. физических лиц, за исключением персональных данных работников этих операторов (уполномоченных лиц) в процессе осуществления трудовой (служебной) деятельности.

Лица, непосредственно осуществляющие обработку персональных данных в названных организациях, могут пройти обучение как в Центре, так и у иных лиц, указанных в подп. 3.3 п. 3 Указа № 422, в том числе в самих организациях по месту выполнения трудовой функции.

Такие операторы (уполномоченные лица) ежегодно до 15 ноября обязаны обеспечить представление Центру информации о количестве лиц, ответственных за контроль, а также лиц, непосредственно осуществляющих обработку персональных данных, которым необходимо пройти обучение в Центре.

В случае, если оператор (уполномоченное лицо) не относится к категории субъектов, обязанных обеспечить прохождение обучения в Центре, он организует его прохождение в учреждениях образования, а также в иных организациях, которым предоставлено право реализации образовательной программы повышения квалификации руководящих работников и специалистов, в других организациях по образовательной программе обучающих курсов, у оператора (уполномоченного лица), то есть в самой организации, где работают лица, осуществляющие обработку персональных данных.

При прохождении обучения непосредственно у оператора (уполномоченного лица) он должен обеспечить изучение установленных требований в области защиты персональных данных, а также осуществление проверки знаний по вопросам защиты персональных данных в форме собеседования, опроса, тестирования и других формах контроля знаний, адаптированных к деятельности этого оператора (уполномоченного лица).

По результатам обучения лицо, его прошедшее, должно понимать содержание локальных правовых актов в области защиты персональных данных, а также как его персональные данные об-

рабатываются оператором (нанимателем) и каким образом он как работник оператора обрабатывает персональные данные граждан (клиентов, посетителей, коллег и иных лиц).

Согласно подп. 3.2 п. 3 Указа № 422 собственники (владельцы) информационных систем (указанные в ч. 1 п. 3 Положения о порядке технической и криптографической защиты информации) и владельцы критически важных объектов информатизации, а также организации, осуществляющие лицензируемую деятельность по технической и (или) криптографической защите информации, обеспечивают обучение в Центре не реже одного раза в три года своих работников и (или) иных лиц, в обязанности которых входит обеспечение информационной безопасности, по образовательной программе повышения квалификации руководящих работников и специалистов по вопросам технической и (или) криптографической защиты информации.

Кроме того, согласно абз. 3 этого подпункта указанные лица ежегодно до 15 ноября обязаны обеспечить представление в Центр информации о количестве работников и (или) иных лиц, в обязанности которых входит обеспечение информационной безопасности, для повышения их квалификации.

Лучшие практики:

1. Разработка программы обучения, построенной в простой доступной форме и адаптированной к специфике деятельности конкретных структурных подразделений организации (создание специальных программ, буклетов, иных разъяснительных материалов; индивидуализация процесса обучения для разных структурных подразделений с учетом специфики их деятельности).

2. Организация проверки знаний работников по итогам обучения с разъяснением сделанных ошибок при проверке знаний.

3. Организация обучения отдельных работников непосредственно в Центре.

4. Дополнительное повышение уровня осведомленности работников путем их участия в тематических семинарах, вебинарах, конференциях и т. п.

5. Использование технических средств обучения и контроля знаний.

6. Организация обучения ответственных за контроль вопросам технической защиты информации.

Типичные ошибки:

1. Нереализация рассматриваемой меры либо ознакомление с информацией лишь отдельных работников, которые обрабатывают персональные данные (например, только работников кадровой службы, бухгалтерии, службы маркетинга).

2. Формальный подход к реализации указанной меры (неэффективный способ ознакомления – размещение на информационных стендах организации либо рассылка посредством корпоративной почты с указанием на необходимость его самостоятельного изучения) без реального обучения с контролем знаний (в форме опроса, тестирования и других формах контроля знаний).

3. Ознакомление с неполным объемом требуемой информации. В частности, недопустимо ознакамливать либо только с положениями законодательства о персональных данных (в том числе с требованиями по защите персональных данных), либо только с политиками.

4. Осуществление ознакомления без обучения либо проведение обучения без ознакомления (например, только с законодательством о персональных данных).

§ 7. ВНЕСЕНИЕ ИЗМЕНЕНИЙ В ДОЛЖНОСТНЫЕ ОБЯЗАННОСТИ ЛИЦ, ОБРАБАТЫВАЮЩИХ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Исполнение обязанностей, возложенных Законом о персональных данных на оператора (уполномоченное лицо) при обработке персональных данных, осуществляется его работниками (лицами, работающими по трудовому договору (контракту)).

При этом они, независимо от выполняемых ими функций, обязаны соблюдать положения законодательства о персональных данных и локальных правовых актов по данным вопросам.

В целях надлежащего обеспечения защиты персональных данных, прав и свобод субъектов персональных данных, а также с учетом установленной Трудовым кодексом Республики Беларусь дисциплинарной ответственности за неисполнение или ненадлежащее исполнение работником своих трудовых обязанностей целесообразно предусмотреть в должностных инструкциях работников, осуществляющих обработку персональных данных, обязанность «соблюдать установленный законодательством о персональных данных и локальными правовыми актами порядок обработки персональных данных».

При необходимости в должностной инструкции должностные обязанности конкретных работников (например, работников, трудовая функция которых в основном связана с обработкой персональных данных в ИР (С), – работников кадровых, бухгалтерских служб, лиц, ответственных за функционирование ИР (С)) могут быть детализированы в части выполняемого функционала по обработке персональных данных, в том числе исходя из способов организации оператором выполнения обязанностей, предусмотренных ст. 16 Закона о персональных данных.

Принимая во внимание, что в должностной инструкции определяются конкретная трудовая функция (должностные обязанности) работника (служащего), а также его права и ответственность (ч. 2 п. 10 Общих положений Единого квалификационного справочника должностей служащих, утвержденных постановлением Министерства труда и социальной защиты Республики Беларусь от 2 января 2012 г. № 1), решение о необходимости детализации должностной инструкции с учетом выполняемых работником функций по реали-

зации Закона о персональных данных принимается нанимателем самостоятельно.

Например, в зависимости от трудовой функции работника в его должностную инструкцию могут быть включены обязанности:

• получать в необходимых случаях согласие субъекта персональных данных на обработку персональных данных;

• осуществлять контроль за соответствием срока обработки персональных данных заявленным целям, прекращать обработку персональных данных, а также обеспечивать их удаление или блокирование при отсутствии правовых оснований для обработки персональных данных;

• обеспечивать предоставление субъектам персональных данных информации, касающейся обработки их персональных данных, а также о предоставлении их персональных данных третьим лицам, за исключением случаев, предусмотренных Законом о персональных данных и иными законодательными актами;

• обеспечивать доступ к персональным данным в установленном порядке, вести учет такого доступа и случаев предоставления их третьим лицам.

§ 8. УСТАНОВЛЕНИЕ ПОРЯДКА ДОСТУПА К ПЕРСОНАЛЬНЫМ ДАННЫМ

Установление порядка доступа к персональным данным, в том числе обрабатываемым в ИР (С), предусмотрено абз. 5 п. 3 ст. 17 Закона о персональных данных.

При установлении порядка доступа к персональным данным операторам и уполномоченным лицам следует определить порядок предоставления такого доступа к персональным данным, обрабатываемым как в ИР (С), так и на бумажных носителях.

Доступ к персональным данным, отраженным в документах на бумажном носителе, можно ограничить посредством организации мест их хранения. Доступ к персональным данным, обрабатываемым в цифровом виде, может быть организован посредством конфигурирования программного обеспечения.

Важно понимать, что в отсутствие такого порядка доступ к персональным данным могут получить работники, должностные обязанности которых не связаны с обработкой персональных данных.

Закрепление порядка доступа к персональным данным целесообразно в одном документе. При этом отдельные его положения могут быть детализированы в иных документах, в том числе положениях об ИР (С), о видеонаблюдении, о контроле управления доступом в помещениях и на территории организации.

Примерное положение о порядке доступа к персональным данным, в том числе обрабатываемым в ИР (С)

Необходимо подчеркнуть, что порядок доступа к персональным данным должен основываться на принципе предоставления оптимального (разумно необходимого) уровня доступа к персональным данным исключительно в целях выполнения работником своих должностных обязанностей, а уполномоченными лицами – обязательств, определенных договором, решением государственного органа или актом законодательства.

При определении такого порядка следует учитывать, что могут возникнуть ситуации, когда необходимо предоставить временный доступ к персональным данным работнику (иному лицу), например в целях подготовки отчета, справки, проведения контроля, аудита. Механизм предоставления такого вре-

менного доступа также следует закрепить в порядке доступа к персональным данным.

Определение целей обработки и категорий персональных данных позволяет упростить распределение доступа к персональным данным относительно занимаемых должностей (оказываемых услуг, выполняемых работ). Однако нецелесообразно осуществлять определение порядка доступа к персональным данным на поименной основе в связи с движением кадров и изменениями бизнес-процессов.

Целесообразно периодически пересматривать содержание установленного порядка доступа с тем, чтобы оно соответствовало реальному положению дел. Частота такого пересмотра определяется оператором (уполномоченным лицом) самостоятельно и зависит от ряда обстоятельств (например, от создания новых должностей, изменения перечня должностных обязанностей работника, занимающего соответствующую должность, и др.).

Лучшие практики:

1. Определение порядка доступа и применение его на практике.

2. Участие должностного лица, ответственного за обеспечение защиты информации, в осуществлении контроля за соблюдением установленного порядка доступа.

Типичные ошибки:

1. Отсутствие порядка доступа к персональным данным.

2. Определение порядка доступа лишь применительно к ИР (С) (в частности, отсутствие порядка доступа к персональным данным на бумажных носителях).

3. Установление перечня лиц (должностей, структурных подразделений), осуществляющих обработку персональных данных, без указания бизнес-процессов, при реализации которых такой доступ необходим.

4. Несоответствие установленного порядка реальному положению дел по разграничению прав доступа к персональным данным, обрабатываемым в ИР (С).

§ 9. ОСУЩЕСТВЛЕНИЕ ТЕХНИЧЕСКОЙ И КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Частью 4 ст. 28 Закона об информации, информатизации и защите информации определено, что информация, распространение и (или) предоставление которой ограничено, которая не отнесена к государственным секретам, должна обрабатываться в информационных системах с применением системы защиты информации, аттестованной в порядке, установленном ОАЦ.

Это нормативное требование актуализировалось с принятием Закона о персональных данных, которым осуществление технической и криптографической защиты персональных данных в порядке, установленном ОАЦ, в соответствии с классификацией ИР (С), содержащих персональные данные, определено в качестве одной из обязательных мер по защите персональных данных (абз. 6 п. 3 ст. 17 Закона о персональных данных).

Требования, обязательные для выполнения собственниками (владельцами) ИС, обрабатывающими информацию, распространение и (или) предоставление которой ограничено, определены Указом Президента Республики Беларусь от 16 апреля 2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации». Например, закреплено требование об использовании средств защиты информации, имеющих сертификат соответствия, выданный в национальной системе подтверждения соответствия. Кроме того, установлено, что проводить мероприятия по осуществлению технической защиты информации должны ответственные сотрудники (подразделения) собственника (владельца) ИС либо организации, имеющие лицензию на осуществление данной деятельности.

Система защиты информации представляет собой совокупность правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности и доступности информации, распространение и (или) предоставление которой ограничено, в том числе и персональных данных.

Конкретные технические требования к защите информации, в том числе и персональных данных, определяются Положением о порядке технической и криптографической защиты информации. Новая редакция указанного Положения утверждена Приказом ОАЦ от 20 февраля 2020 г. № 66 (в ред. приказа ОАЦ от 10 декабря 2024 г. № 259).

Положение о порядке технической и криптографической защиты информации может не применяться:

• собственниками (владельцами) ИС, в которых обрабатываются только общедоступные персональные данные и (или) персональные данные, полученные после применения методов обезличивания, – в отношении таких ИС;

Положение о порядке технической и криптографической защиты информации

• операторами электросвязи – собственниками (владельцами) ИС, обеспечивающих управление технологическими процессами и предназначенных только для передачи персональных данных по технологическим сетям электросвязи, – в отношении таких ИС.

Работы по технической и криптографической защите информации включают:

• проектирование системы защиты информации;

• создание системы защиты информации;

• аттестацию системы защиты информации в соответствии с Положением о порядке аттестации систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденным приказом ОАЦ от 20 февраля 2020 г. № 66;

• обеспечение функционирования системы защиты информации в процессе эксплуатации информационной системы;

• обеспечение защиты информации в случае прекращения эксплуатации ИС.

В рамках комплекса мероприятий по технической и криптографической защите информации проводится аттестация системы защиты информации, которая представляет собой окончательную проверку корректности выполнения мероприятий по технической защите. Успешное прохождение данной проверки позволяет получить аттестат соответствия, срок действия которого составляет 5 лет.

Следует отметить, что Положением о порядке технической и криптографической защиты информации предусматривается также упрощенная процедура проектирования и аттестации системы защиты информации. Она применяется в случаях, когда ее функционирование предполагается на базе другой информационной системы, система защиты которой аттестована.

Конкретные требования к технической и криптографической защите персональных данных при их обработке в информационных системах зависят от класса информационной системы. Такая классификация, исходя из положений п. 5 ст. 17 Закона о персональных данных, устанавливается Центром.

В развитие указанной нормы издан приказ директора Центра от 15 ноября 2021 г. № 12.

Согласно приложению 1 к Положению о порядке технической и криптографической защиты выделены следующие классы типовых ИС:

Класс 4-ин – ИС, в которых обрабатываются персональные данные, за исключением специальных персональных данных, и которые не имеют подключений к сетям электросвязи общего пользования (открытым каналам передачи данных) (далее – открытые каналы передачи данных).

Класс 4-спец – ИС, в которых обрабатываются специальные персональные данные, за исключением биометрических и генетических персональных данных, и которые не имеют подключений к открытым каналам передачи данных.

Класс 4-бг – ИС, в которых обрабатываются биометрические и генетические персональные данные и которые не имеют подключений к открытым каналам передачи данных.

Класс 4-юл – ИС, в которых обрабатывается информация, составляющая коммерческую и иную охраняемую законом тайну юридического лица, распространение и (или) предоставление которой ограничено (за исключением сведений, составляющих государственные секреты, и служебной информации ограниченного распространения), и которые не имеют подключений к открытым каналам передачи данных.

Класс 4-дсп – ИС, в которых обрабатывается служебная информация ограниченного распространения и которые не имеют подключений к открытым каналам передачи данных.

Класс 3-ин – ИС, в которых обрабатываются персональные данные, за исключением специальных персональных данных, и которые подключены к открытым каналам передачи данных.

Класс 3-спец – ИС, в которых обрабатываются специальные персональные данные, за исключением биометрических и генетических персональных данных, и которые подключены к открытым каналам передачи данных.

Класс 3-бг – ИС, в которых обрабатываются биометрические и генетические персональные данные и которые подключены к открытым каналам передачи данных.

Класс 3-юл – ИС, в которых обрабатывается информация, составляющая коммерческую и иную охраняемую законом тайну юридического лица, распространение и (или) предоставление которой ограничено (за исключением сведений, составляющих государственные секреты, и служебной информации ограниченного распространения), и которые подключены к открытым каналам передачи данных.

Класс 3-дсп – ИС, в которых обрабатывается служебная информация ограниченного распространения и которые подключены к открытым каналам передачи данных.

В свою очередь, в приложении 3 к названному Положению применительно к данным классам типовых информационных систем установлены конкретные требования к системе защиты информации, которые подлежат включению в техническое задание на создание системы защиты информации. Такое задание должно быть создано на этапе проектирования системы защиты информации (п. 8 Положения о порядке технической и криптографической защиты информации).

Данные требования представлены в виде нескольких групп технических мер. К основным мерам относятся:

- необходимость осуществления защиты от вредоносного программного обеспечения, которое должно выявляться как на рабочих местах пользователей ИС, так и в сервисах обмена электронной почты;
- мониторинг событий информационной безопасности. Указанный мониторинг необходим для своевременного выявления инцидентов и позволяет минимизировать последствия от неправомерного воздействия на ИР (С);
- осуществление собственниками (владельцами) ИР (С) резервирования информации;
- разграничение доступа пользователей (что коррелирует с требованиями Закона о персональных данных);
- обеспечение безопасной настройки объектов и их непрерывного обновления до наиболее актуальных версий программного обеспечения.

§ 10. УСТАНОВЛЕНИЕ И ПОДДЕРЖАНИЕ В АКТУАЛЬНОМ СОСТОЯНИИ ПЕРЕЧНЯ ИР (С), А ТАКЖЕ КАТЕГОРИЙ ПЕРСОНАЛЬНЫХ ДАННЫХ, ПОДЛЕЖАЩИХ ВКЛЮЧЕНИЮ В ДАННЫЕ ИР (С)

Согласно подпункту а) подп. 3.5 п. 3 Указа № 422 операторы, являющиеся государственными органами, юридическими лицами Республики Беларусь, иными организациями, устанавливают и поддерживают в актуальном состоянии перечень ИР (С), содержащих персональные данные, собственниками (владельцами) которых они являются.

Не подлежат включению в такой перечень ИР (С), если оператор не выступает собственником или владельцем по отношению к ним.

Категории персональных данных, подлежащих включению в такие ресурсы (системы), определены в подп. б) подп. 3.5 п. 3 Указа № 422 (рис. 5).

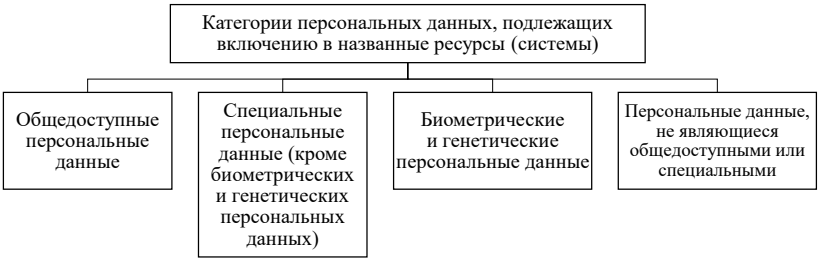

Рис. 5. **Категории персональных данных**

Приказом директора Центра от 15 ноября 2021 г. № 12 установлена классификация ИР (С). Так, определено, что ИР (С), содержащие персональные данные, в целях определения предъявляемых к ним требований по технической и криптографической защите персональных данных подразделяются на ИР (С), содержащие:

- общедоступные персональные данные;
- специальные персональные данные (кроме биометрических и генетических персональных данных);
- биометрические и генетические персональные данные;
- персональные данные, не являющиеся общедоступными или специальными.

Определение указанных категорий персональных данных содержится в ст. 1 Закона о персональных данных.

Общедоступные персональные данные – персональные данные, распространенные самим субъектом персональных данных либо с его согласия или распространенные в соответствии с требованиями законодательных актов (абз. 7 ст. 1 Закона о персональных данных).

Приказ директора Центра от 15 ноября 2021 г. № 12

Специальные персональные данные – персональные данные, касающиеся расовой либо национальной принадлежности, политических взглядов, членства в профессиональных союзах, религиозных или других убеждений, здоровья или половой жизни, привлечения к административной или уголовной ответственности, а также биометрические и генетические персональные данные (абз. 12 ст. 1 Закона о персональных данных).

Биометрические персональные данные – информация, характеризующая физиологические и биологические особенности человека, которая используется для его уникальной идентификации (отпечатки пальцев рук, ладоней, радужная оболочка глаза, характеристики лица и его изображение и др.) (абз. 2 ст. 1 Закона о персональных данных).

Генетические персональные данные – информация, относящаяся к наследуемым либо приобретенным генетическим характеристикам человека, которая содержит уникальные данные о его физиологии либо здоровье и может быть выявлена, в частности, при исследовании его биологического образца (абз. 4 ст. 1 Закона о персональных данных).

Примерная форма перечня ИР (С), содержащих персональные данные, и категории персональных данных, подлежащих включению в них

При реализации указанной меры следует учитывать, что к ИР (С), содержащим персональные данные, относятся в том числе корпоративная электронная почта, программное обеспечение для ведения бухгалтерского учета и отчетности, интернет-сайты организаций, автоматизированные системы контроля и управления доступом, системы видео-

наблюдения в организации, системы электронного документооборота и т. п.

Категории персональных данных, содержащиеся в ИР (С), предопределяют круг предъявляемых к данным ИР (С) требований по технической и криптографической защите персональных данных.

На практике ведение такого перечня осуществляется в виде таблицы, электронной формы и т. п. Порядок его ведения и форма утверждаются локальным правовым актом оператора.

Лучшие практики:

1. Включение в перечень дополнительных столбцов, облегчающих его ведение (например, отражающих назначение информационного ресурса, структурное подразделение, ответственное за его ведение, сведения о привлечении уполномоченных лиц).

2. Корреляция сведений перечня ИР(С), порядка доступа к персональным данным и реестра обработок персональных данных организации.

Типичные ошибки:

1. Отсутствие такого перечня либо установление операторами неполного перечня ИР (С), содержащих персональные данные, собственниками (владельцами) которых они являются.

2. Включение в перечень ресурсов, собственником (владельцем) которых является иное лицо.

3. Неуказание либо некорректное указание категорий персональных данных, обрабатываемых в конкретных ИР (С).

§ 11. УСТАНОВЛЕНИЕ И ПОДДЕРЖАНИЕ В АКТУАЛЬНОМ СОСТОЯНИИ ПЕРЕЧНЯ УПОЛНОМОЧЕННЫХ ЛИЦ

Ведение операторами, являющимися государственными органами, юридическими лицами Республики Беларусь, иными организациями, перечня уполномоченных лиц, если обработка персональных данных осуществляется уполномоченными лицами, предусмотрено подп. в) подп. 3.5 п. 3 Указа № 422.

Цель установления перечня уполномоченных лиц – систематизация и учет обработок персональных данных, поручаемых таким лицам.

В этой связи принципиально важным является определение статуса лиц, осуществляющих обработку персональных данных, до начала такой обработки. Оно должно осуществляться в каждом конкретном случае с учетом анализа конкретного бизнес-процесса, сопровождающегося обработкой персональных данных, исходя из фактических обстоятельств такой обработки независимо от того, как упомянутые лица названы, например, в договоре.

В соответствии с абз. 8 ст. 1 Закона о персональных данных оператор – государственный орган, юридическое лицо Республики Беларусь, иная организация, физическое лицо, в том числе индивидуальный предприниматель, самостоятельно или совместно с иными указанными лицами организующие и (или) осуществляющие обработку персональных данных.

Уполномоченное лицо – государственный орган, юридическое лицо Республики Беларусь, иная организация, физическое лицо, которые в соответствии с актом законодательства, решением государственного органа, являющегося оператором, либо на основании договора с оператором осуществляют обработку персональных данных от имени оператора или в его интересах (абз. 17 ст. 1 Закона о персональных данных).

До реализации указанной меры оператору следует надлежащим образом выстроить взаимодействие с уполномоченными лицами. Для этого необходимо квалифицировать его отношения с контрагентами, после чего обеспечить реализацию положений ст. 7 Закона о персональных данных.

Следует учитывать, что согласно п. 1 ст. 7 Закона о персональных данных в договоре между оператором и уполномоченным лицом,

акте законодательства либо решении государственного органа, являющегося оператором, должны быть определены:

- цели обработки персональных данных;
- перечень действий, которые будут совершаться с персональными данными уполномоченным лицом;
- обязанности по соблюдению конфиденциальности персональных данных;
- меры по обеспечению защиты персональных данных в соответствии со ст. 17 Закона о персональных данных.

Положения для включения в договор между оператором и уполномоченным лицом о поручении обработки персональных данных

Операторы и уполномоченные лица несут ответственность за непринятие правовых, организационных и технических мер по обеспечению защиты персональных данных от несанкционированного или случайного доступа к ним, изменения, блокирования, копирования, распространения, предоставления, удаления персональных данных, а также от иных неправомерных действий в отношении персональных данных.

Вместе с тем, если субъекту персональных данных причинен вред, в том числе моральный, действиями оператора или уполномоченного лица, то с учетом положений п. 3 ст. 7 Закона этот субъект в судебном порядке может обратиться с иском к оператору, который, в свою очередь, может требовать привлечения уполномоченного лица к ответственности за нарушение условий поручения по обработке.

Оператор также несет ответственность за случаи «утечки» персональных данных, допущенные уполномоченным лицом.

В этой связи операторам следует тщательно подходить к выбору уполномоченных лиц и привлекать к обработке персональных данных только тех из них, которые предоставляют достаточные гарантии принятия ими соответствующих правовых, организационных и технических мер для обеспечения обработки персональных данных в соответствии с требованиями Закона.

Иные особенности реализации указанной меры содержатся в разработанных Центром Рекомендациях о взаимоотношениях операторов и уполномоченных лиц при обработке персональных данных (ссылка доступна посредством перехода по QR-коду).

На практике ведение перечня уполномоченных лиц осуществляется в виде таблицы (таблицы 3, 4), электронной формы и др., который целесообразно установить локальным правовым актом оператора.

Рекомендации о взаимоотношениях операторов и уполномоченных лиц при обработке персональных данных

Типичные ошибки:

1. Отсутствие указанного перечня либо невключение в него всех уполномоченных лиц, осуществляющих обработку персональных данных по поручению оператора.

2. Указание вместо конкретных уполномоченных лиц категорий таких лиц.

3. Включение в него как уполномоченных лиц, так и самостоятельных операторов, которым осуществляется предоставление персональных данных.

4. Неактуализация такого перечня на периодической основе.

Таблица 3

Форма учета уполномоченных лиц

№ п/п	Уполномоченное лицо	Информационный ресурс (система)	Предмет договора
1			

Таблица 4

Форма учета уполномоченных лиц

№ п/п	Уполномоченное лицо	Перечень действий с персональными данными	Правовые основания поручения обработки (договор, решение госоргана, акт законодательства)	Цель обработки персональных данных	Перечень персональных данных	Дата направления запроса о принятии (реализации) мер по обеспечению защиты персональных данных и (или) об удалении персональных данных в рамках заключенного соглашения об обработке персональных данных	Дата получения ответа о принятии мер по обеспечению защиты персональных данных и (или) об удалении персональных данных в рамках заключенного соглашения об обработке персональных данных
1							
2							

§ 12. ВНЕСЕНИЕ СВЕДЕНИЙ В ГИР РЕЕСТР ОПЕРАТОРОВ

Подпунктом 3.6 п. 3 Указа № 422 с 1 января 2024 г. на операторов возложена обязанность вносить в создаваемый ГИР Реестр операторов сведения об ИР (С), в которых обрабатываются персональные данные, в случаях, когда такие ресурсы (системы) соответствуют критериям, предусмотренным подп. 1.1 п. 1 Приказа ОАЦ № 94, а также обеспечивать актуализацию соответствующих сведений.

Согласно названному подпункту Приказа ОАЦ № 94 ГИР Реестр операторов содержит информацию об ИР (С), посредством которых осуществляется:

ГИР Реестр операторов

- трансграничная передача специальных персональных данных, если на территории иностранного государства не обеспечивается надлежащий уровень защиты прав субъектов персональных данных, за исключением случаев, предусмотренных абз. 5–7 п. 1 ст. 9 Закона о персональных данных;
- обработка биометрических и (или) генетических персональных данных;
- обработка персональных данных более 100 тыс. физических лиц;
- обработка персональных данных более 10 тыс. физических лиц, не достигших возраста шестнадцати лет.

Необходимо отметить, что факт регистрации информационного ресурса (системы) в Государственном регистре информационных ресурсов или Государственном регистре информационных систем в порядке, предусмотренном постановлением Совета Министров Республики Беларусь от 26 мая 2009 г. № 673 «Об информационных ресурсах, информационных системах и государственных цифровых платформах», для цели внесения сведений в ГИР Реестр операторов значения не имеет.

Таким образом, если посредством ИР (С) оператора осуществляется обработка персональных данных, соответствующая одному и (или) нескольким критериям, предусмотренным подп. 1.1 п. 1 Приказа ОАЦ № 94, сведения о таком ИР (С) подлежат внесению в ГИР Реестр операторов.

Оценка соответствия ИР (С) критериям, предусмотренным подп. 1.1 п. 1 Приказа ОАЦ № 94, осуществляется оператором.

Рассмотрим на примерах.

Пример 1. В организации используется программный продукт организации «1С», в котором осуществляется хранение сведений более 100 тыс. физических лиц. Обработка персональных данных посредством такого информационного ресурса подпадает под критерий, предусмотренный абз. 4 подп. 1.1 п. 1 Приказа ОАЦ № 94. Таким образом, сведения о таком информационном ресурсе подлежат внесению в ГИР Реестр операторов.

Пример 2. Частная медицинская клиника осуществляет обработку сведений о здоровье клиентов посредством информационного ресурса, в котором хранятся результаты анализов, в том числе генетических, фото пациентов до и после хирургического вмешательства, стоматологические снимки. Поскольку в таком ИР обрабатываются генетические персональные данные (он соответствует критерию, предусмотренному абз. 3 подп. 1.1 п. 1 Приказа ОАЦ № 94), сведения о таком информационном ресурсе подлежат внесению в ГИР Реестр операторов независимо от количества физических лиц, персональные данные которых обрабатываются в этом ресурсе.

Пример 3. В организации используется система видеонаблюдения (ведется видеозапись в режиме реального времени), посредством которой осуществляется уникальная идентификация работников путем сопоставления с фото- и видеоизображениями работников, хранящимися в системе. С учетом того, что в ИС обрабатываются биометрические персональные данные (она соответствует критерию, предусмотренному абз. 3 подп. 1.1 п. 1 Приказа ОАЦ № 94), сведения о такой информационной системе подлежат внесению в ГИР Реестр операторов. Сведения о системах видеонаблюдения, посредством которых уникальная идентификация субъектов персональных данных не осуществляется, в ГИР Реестр операторов не вносятся.

Пример 4. В организации на компьютере в табличной форме ведется база данных клиентов с указанием фамилии, имени, отчества, адреса места жительства и контактного телефона. Список насчитывает персональные данные более 100 тыс. физических лиц. Сведения о таком ИР подлежат внесению в ГИР Реестр операторов, так как осуществляемая в нем обработка персональных данных соответствует критерию, предусмотренному абз. 4 подп. 1.1 п. 1 Приказа № 94.

Пример 5. Учреждение здравоохранения (детская поликлиника) обрабатывает персональные данные более 10 тыс. физических лиц,

не достигших возраста шестнадцати лет, посредством информационного ресурса. Сведения о таком информационном ресурсе подлежат внесению в ГИР Реестр операторов, так как осуществляемая в нем обработка персональных данных соответствует критерию, предусмотренному абз. 5 подп. 1.1 п. 1 Приказа № 94.

Важно отметить, что сведения об ИР(С) могут вноситься в ГИР Реестр операторов не только самим оператором, но и по его поручению уполномоченным лицом, то есть лицом, которое от имени или в интересах оператора обрабатывает персональные данные в соответствующем ресурсе (системе).

При этом при осуществлении оценки соответствия ИР (С) критериям, предусмотренным подп. 1.1 п. 1 Приказа № 94, учитывается количество физических лиц, персональные данные которых обрабатываются посредством такого информационного ресурса (системы), на момент внесения сведений в ГИР Реестр операторов.

Оператор или уполномоченное лицо в отношении ИР (С), созданного (созданной) после 1 января 2024 г., обязаны внести сведения в ГИР Реестр операторов в течение десяти рабочих дней после ввода его (ее) в постоянную эксплуатацию.

Сведения вносятся в ГИР Реестр операторов в электронном виде. Для этого необходимо пройти процедуру регистрации личного кабинета пользователя и аутентификации оператора. Аутентификация пользователей осуществляется через Единую систему идентификации физических и юридических лиц с использованием электронной цифровой подписи.

В случае отсутствия технической возможности доступа к ГИР Реестр операторов в целях соблюдения сроков, установленных Приказом ОАЦ № 94, сведения для внесения в ГИР Реестр операторов могут быть направлены в виде заявки посредством системы межведомственного документооборота или почтовой связи.

В ГИР Реестр операторов подлежат внесению следующие сведения:

- наименование ИР (С);
- местонахождение систем хранения данных и серверного оборудования, на которых размещается ИР (С);
- дата внесения сведений в ГИР Реестр операторов и их изменения;
- полное наименование (фамилия, собственное имя, отчество (если таковое имеется)), место нахождения (адрес места жительства (места пребывания)) и регистрационный номер в Едином

государственном регистре юридических лиц и индивидуальных предпринимателей (если таковой имеется) оператора;

Видеоинструкция по работе с ГИР Реестр операторов

• полное наименование (фамилия, собственное имя, отчество (если таковое имеется) и место нахождения (адрес места жительства (места пребывания) и регистрационный номер в Едином государственном регистре юридических лиц и индивидуальных предпринимателей (если таковой имеется) уполномоченного лица (если таковое имеется), осуществляющего обработку персональных данных в ИР (С) от имени оператора или в его интересах, в том числе по поручению которого вносятся сведения в ГИР Реестр операторов;

• фамилия, собственное имя, отчество (если таковое имеется), контактный номер телефона, адрес электронной почты руководителя структурного подразделения или лица, ответственного за контроль, назначенного оператором и (или) уполномоченным лицом;

• основания, предусмотренные для включения ИР (С) в ГИР Реестр операторов;

• количество субъектов персональных данных, персональные данные которых обрабатываются в ИР (С) на момент внесения информации в ГИР Реестр операторов;

• заявленные цели и правовые основания обработки персональных данных;

• срок хранения персональных данных;

• перечень иностранных государств, на территорию которых осуществляется трансграничная передача специальных персональных данных, если на их территории не обеспечивается надлежащий уровень защиты прав субъектов персональных данных.

Изменение сведений об ИР (С) или их исключение из ГИР Реестр операторов осуществляется оператором или уполномоченным лицом в течение десяти рабочих дней после ввода в постоянную эксплуатацию ИР (С) в измененном виде, после прекращения его (ее) эксплуатации или изменения иных сведений, внесенных в ГИР Реестр операторов.

Типичные ошибки:

1. Нарушение сроков внесения сведений в ГИР Реестр операторов.

2. Неполное указание сведений (например, при перечислении целей обработки персональных данных и перечня уполномоченных лиц).

3. Неактуализация сведений в 10-дневный срок.

§ 13. УЧЕТ ИНФОРМАЦИИ О ПРЕДОСТАВЛЕНИИ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕТЬИМ ЛИЦАМ

Установление порядка учета информации о предоставлении персональных данных третьим лицам и ведение такого учета является важной мерой, позволяющей исполнить должным образом обязанность оператора по предоставлению субъекту персональных данных информации, связанной с обработкой его персональных данных (абз. 5 п. 1 ст. 16 Закона о персональных данных).

Права субъектов персональных данных

Субъекты персональных данных в соответствии с Законом о персональных данных наделены широким кругом прав. Они являются действенным инструментом контроля за обработкой принадлежащих человеку персональных данных. В частности, субъект персональных данных вправе получать от оператора информацию о предоставлении своих персональных данных третьим лицам.

Право на получение информации о предоставлении своих персональных данных третьим лицам может быть реализовано субъектом персональных данных один раз в календарный год бесплатно.

Статья 14 Закона о персональных данных определяет порядок подачи субъектом персональных данных заявлений для реализации прав, связанных с обработкой персональных данных (далее – заявления субъектов персональных данных). Пунктом 1 указанной статьи Закона о персональных данных конкретизированы формы подачи заявлений субъектов персональных данных: письменная и в виде электронного документа, удостоверенного электронной цифровой подписью.

В свою очередь, п. 2 ст. 14 Закона о персональных данных закрепляет требования к содержанию заявлений субъектов персональных данных. Определенная законодателем информация, как правило, является достаточной для идентификации субъекта персональных данных, поэтому при ее наличии у оператора установление им дополнительных требований к содержанию заявлений

субъектов персональных данных не соответствует требованиям Закона о персональных данных[9].

Вместе с тем в случае отсутствия необходимости истребования в заявлении субъекта персональных данных о реализации его прав всех сведений, перечень которых предусмотрен п. 2 ст. 14 Закона о персональных данных, оператор, руководствуясь риск-ориентированным подходом, имеет право рассмотреть заявление субъекта, содержащее меньший объем сведений (например, в отсутствие в нем даты рождения субъекта персональных данных).

Оператор обязан в пятнадцатидневный срок после получения заявления субъекта персональных данных:

• предоставить ему информацию о том, какие персональные данные этого субъекта и кому предоставлялись в течение года, предшествовавшего дате подачи заявления, либо

• уведомить субъекта персональных данных о причинах отказа в ее предоставлении.

Информация о предоставлении персональных данных третьим лицам может не предоставляться, если обработка персональных данных осуществляется в соответствии с законодательством об исполнительном производстве, при осуществлении правосудия и организации деятельности судов общей юрисдикции, а также в случаях, предусмотренных п. 3 ст. 11 Закона о персональных данных:

• если персональные данные могут быть получены любым лицом посредством направления запроса в порядке, установленном законодательством, либо доступа к информационному ресурсу (системе) в глобальной компьютерной сети Интернет;

• если обработка персональных данных осуществляется:

• в соответствии с законодательством о государственной статистике;

• в соответствии с законодательством в области национальной безопасности, об обороне, о борьбе с коррупцией, о борьбе с терроризмом и противодействии экстремизму, о предотвращении легализации доходов, полученных преступным путем, финансирования террористической деятельности и финансирования распространения оружия массового поражения, о Государственной границе Республики Беларусь;

[9] Защита персональных данных: учеб. пособие / А. А. Гаев, С. В. Задиран, М. Г. Коршекевич [и др.]; под общ. ред. М. Г. Коршекевича, М. А. Городецкой. – Минск: РИВШ, 2024. – С. 63.

• в соответствии с законодательством об оперативно-розыскной деятельности, процессуально-исполнительным законодательством об административных правонарушениях, уголовно-процессуальным, уголовно-исполнительным законодательством;

• по вопросам ведения криминалистических учетов;

• в иных случаях, предусмотренных законодательными актами.

На практике указанная мера может быть реализована путем ведения электронной таблицы, журналов, если информация предоставлялась в письменном виде, систем логирования в ИР (С) и т. п.

Порядок такого учета целесообразно закрепить в локальном правовом акте.

Примерная форма учета представлена в таблице 5.

Таблица 5

Вариант установления порядка учета информации о предоставлении персональных данных третьим лицам

№ п/п	Субъект персональных данных	Перечень переданных персональных данных	Правовое основание предоставления персональных данных	Сведения о третьем лице	Сведения о способе передачи
1					

Вопросы доступа работников и иных лиц к информации о предоставлении персональных данных третьим лицам должны быть разрешены в документе, определяющем порядок доступа к персональным данным, в том числе обрабатываемым в ИР (С).

§ 14. УВЕДОМЛЕНИЕ ЦЕНТРА О НАРУШЕНИЯХ СИСТЕМ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Согласно абз. 8 п. 1 ст. 16 Закона о персональных данных оператор обязан уведомить Центр о нарушениях систем защиты персональных данных незамедлительно, но не позднее трех рабочих дней после того, как ему стало известно о таких нарушениях, за исключением случаев, предусмотренных Центром.

Под системой защиты персональных данных следует понимать совокупность правовых, организационных и технических мер, вытекающих из законодательства о персональных данных, предусмотренных локальными правовыми актами оператора, целью принятия которых является защита персональных данных, обрабатываемых оператором.

Порядок направления уведомления в Центр о нарушениях систем защиты персональных данных определен приказом директора Центра от 15 ноября 2021 г. № 13.

Согласно п. 1 этого приказа уведомление о нарушениях систем защиты персональных данных направляется оператором в Центр при нарушении систем защиты персональных данных, за исключением случаев, когда нарушение систем защиты не привело:

- к незаконному распространению, предоставлению персональных данных;
- изменению, блокированию либо удалению персональных данных без возможности восстановления доступа к ним.

При этом такое уведомление направляется и в ситуации, когда при названном нарушении оператор не может доказать отсутствие наступления подобных последствий.

Важно понимать, что нарушение системы защиты персональных данных – это не только утечка персональных данных (например, баз данных, содержащих пароли, логины, номера телефонов и др.).

Нарушение систем защиты персональных данных могут выражаться также:

- в несанкционированном доступе к документам, содержащим персональные данные;
- потере носителя информации, содержащего персональные данные;
- отправке документов, содержащих персональные данные, неверному получателю (например, на ошибочный электронный адрес).

Обязанность направления уведомления не зависит от количества лиц, затронутых нарушением.

Пунктом 2 приказа № 13 установлены сведения, которые подлежат отражению в уведомлении, а также форма такого уведомления – письменная либо в виде электронного документа. Так, уведомление должно содержать:

• фамилию, собственное имя, отчество (если таковое имеется), адрес места жительства (места пребывания) оператора (физического лица) или полное наименование и место нахождения оператора (государственного органа, юридического лица Республики Беларусь, иной организации), а также номер телефона, адрес электронной почты (при наличии) оператора;

• фамилию, собственное имя, отчество (если таковое имеется), должность лица, ответственного за контроль у оператора либо наименование соответствующего структурного подразделения (в отношении государственного органа, юридического лица Республики Беларусь, иной организации), его номер телефона и адрес электронной почты (при наличии);

• дату и время нарушения системы защиты персональных данных;

• дату и время, когда стало известно о произошедшем нарушении системы защиты персональных данных;

• нарушения системы защиты персональных данных;

• примерное количество субъектов персональных данных, затронутых нарушением;

• неблагоприятные последствия нарушения системы защиты персональных данных (потеря контроля над персональными данными, их хищение, нарушение прав и свобод субъектов персональных данных, чести, достоинства или деловой репутации, наступление убытков, разглашение охраняемой законом тайны, наступление иного существенного имущественного или иного вреда у субъектов персональных данных);

• меры, принятые или предлагаемые оператором для устранения нарушения системы защиты персональных данных.

Отметим, что обязанность оператора по уведомлению Центра о нарушениях систем защиты персональных данных не является отдельной мерой по обеспечению защиты персональных данных, однако она направлена на устранение (минимизацию) негативных последствий, связанных с незаконным распространением, предоставлением персональных данных, их изменением, блокирова-

нием либо удалением без возможности восстановления доступа к ним.

На практике одной из мер по устранению последствий нарушений систем защиты персональных данных либо их минимизации является информирование субъектов персональных данных о случившемся инциденте. Решение о таком информировании должно приниматься оператором с учетом риска потенциального нарушения прав субъектов персональных данных либо по требованию Центра.

Форма информирования может варьироваться в зависимости от специфики нарушения и количества затронутых субъектов персональных данных. Например, если нарушение касается участников программы лояльности или пользователей информационного ресурса (системы), возможными каналами информирования могут быть e-mail- и SMS-рассылка, уведомление в мобильном приложении, на интернет-сайте посредством информационного баннера и др.

Субъекты персональных данных должны быть информированы:

- о произошедшем нарушении;
- предпринятых оператором мерах по устранению последствий;
- рекомендуемых действиях по минимизации негативных последствий (например, прохождение процедуры перерегистрации, смены пароля, уделения особого внимания звонкам с незнакомых номеров, поступающим на электронный адрес письмам и т. п.).

При этом, если нарушение системы защиты персональных данных касается исключительно работников оператора, целесообразным является доведение сведений о нем лично этим работникам.

Необходимо отметить, что подп. 2.3 п. 2 приказа № 13 допускаются отзыв и изменение уведомления.

Так, если нарушение систем защиты персональных данных не подтверждается или не требует направления уведомления (соответствует условиям, предусмотренным ч. 2 п. 1 приказа № 13), оператор вправе отозвать его. Аналогичное право оператор имеет и в отношении внесения изменений в уведомление.

Отдельное значение в данном контексте приобретают вопросы обработки персональных данных при поручении такой обработки уполномоченному лицу (уполномоченным лицам).

В случае если оператор поручает ему (им) ведение бухучета, системное администрирование, оказание IT-поддержки, транс-

портные услуги, изготовление печатной продукции, SMS-рассылку и т. п., то в договоре между сторонами (дополнительном соглашении к нему) необходимо предусмотреть не только установленные п. 1 ст. 7 Закона о персональных данных положения, но и обязанность уполномоченного лица незамедлительно уведомлять оператора о нарушениях систем защиты персональных данных.

БИБЛИОГРАФИЯ

Нормативные правовые акты

1. О защите персональных данных: Закон Респ. Беларусь от 7 мая 2021 г. № 99-З: с изм. и доп. Закона Респ. Беларусь от 1 июня 2022 г. № 175-З) // ЭТАЛОН: информ.-поисковая система (дата обращения: 23.10.2024).

2. Об информации, информатизации и защите информации: Закон Респ. Беларусь от 10 ноября 2008 г. № 455-З: в редакции Закона Респ. Беларусь от 10 октября № 209-З // ЭТАЛОН: информ.-поисковая система (дата обращения: 23.10.2024).

3. О мерах по совершенствованию защиты персональных данных: Указ Президента Респ. Беларусь от 28 октября 2021 г. № 422: с изм. и доп. Указа Президента Респ. Беларусь от 5 февраля 2024 г. № 46 // ЭТАЛОН: информ.-поисковая система (дата обращения: 23.10.2024).

4. О некоторых мерах по совершенствованию защиты информации: Указ Президента Респ. Беларусь от 16 апреля 2013 г. № 196 // ЭТАЛОН: информ.-поисковая система (дата обращения: 23.10.2024).

5. О мерах по реализации Указа Республики Беларусь от 9 декабря 2019 г. № 449: приказ Оперативно-аналитического центра при Президенте Респ. Беларусь от 20 февраля 2020 г. № 66 (в ред. приказ Оперативно-аналитического центра при Президенте Респ. Беларусь от 10 декабря 2024 г. № 259) // ЭТАЛОН: информ.-поисковая система (дата обращения: 13.12.2024).

6. Об обучении по вопросам защиты персональных данных: приказ Оперативно-аналитического центра при Президенте Респ. Беларусь от 12 ноября 2021 г. № 194: в ред. от 23 ноября 2023 г. // ЭТАЛОН: информ.-поисковая система (дата обращения: 23.10.2024).

7. О государственном информационном ресурсе «Реестр операторов персональных данных»: приказ Оперативно-аналитического центра при Президенте Респ. Беларусь от 1 июня 2022 г. № 94 // ЭТАЛОН: информ.-поисковая система (дата обращения: 18.11.2024).

8. О классификации информационных ресурсов (систем): приказ директора Нац. центра защиты персональных данных Респ. Беларусь № 12 от 15 ноября 2021 г. № 12 // ЭТАЛОН: информ.-поисковая система (дата обращения: 18.11.2024).

9. Об уведомлении о нарушениях систем защиты персональных данных: приказ директора Нац. центра защиты персональных данных Респ. Беларусь от 15 ноября 2021 г. № 13 // ЭТАЛОН: информ.-поисковая система (дата обращения: 18.11.2024).

Рекомендации и разъяснения Центра

1. Разъяснения законодательства о персональных данных (о копиях документов, удостоверяющих личность) // Нац. центр защиты персональных данных Респ. Беларусь. – URL: https://cpd.by (дата обращения: 19.01.2025).

2. Разъяснения законодательства о персональных данных (о праве субъекта персональных данных получать от оператора информацию о предоставлении своих персональных данных третьим лицам) (письмо Нац. центра защиты персональных данных Респ. Беларусь от 2 марта 2023 г. № 5–5/228) // Нац. центр защиты персональных данных Респ. Беларусь. – URL: https://cpd.by/pravovaya-osnova/metodologicheskiye-dokumenty-rekomendatsii/ (дата обращения: 19.01.2025).

3. Разъяснения законодательства о персональных данных (об объеме сведений, необходимом для оформления доверенности) // Нац. центр защиты персональных данных Респ. Беларусь. – URL: https://cpd.by (дата обращения: 19.01.2025).

4. Разъяснения законодательства о персональных данных (порядке осуществления видеонаблюдения в многоквартирных жилых домах) // Нац. центр защиты персональных данных Респ. Беларусь. – URL: https://cpd.by (дата обращения: 19.01.2025).

5. Разъяснения о применении законодательства о персональных данных в деятельности учреждений среднего специального и высшего образования / Нац. центр защиты персональных данных Респ. Беларусь. – URL: https://cpd.by (дата обращения: 22.07.2024).

6. Разъяснения о применении Закона Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных» в сфере образования (письмо от 24 августа 2022 г. № 05/196) // Нац. центр защиты персональных данных Респ. Беларусь. – URL: https://cpd.by (дата обращения: 19.01.2025).

7. Разъяснения о применении Закона Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных» в сфере образования (письмо от 17 марта 2023 г. № 5–13/93) // Нац. центр защиты персональных данных Респ. Беларусь. – URL: https://cpd.by (дата обращения: 19.01.2025).

8. Разъяснения об обработке персональных данных при осуществлении деятельности гаражных кооперативов и кооперативов, осуществляющих эксплуатацию автомобильных стоянок, товариществ собственников, организаций застройщиков, садоводческих товариществ // Нац. центр защиты персональных данных Респ. Беларусь. – URL: https://cpd.by (дата обращения: 19.01.2025).

9. Рекомендации по составлению документа, определяющего политику оператора (уполномоченного лица) в отношении обработки пер-

сональных данных // Нац. центр защиты персональных данных Респ. Беларусь. – URL: https://cpd.by/pravovaya-osnova/metodologicheskiye-dokumenty-rekomendatsii/ (дата обращения: 19.01.2025).

10. Рекомендации Центра о взаимоотношениях операторов и уполномоченных лиц при обработке персональных данных // Нац. центр защиты персональных данных Респ. Беларусь. – URL: https://cpd.by (дата обращения: 19.01.2025).

Литература

1. Защита персональных данных: учеб. пособие / А. А. Гаев, С. В. Задиран, М. Г. Коршевич [и др.]; под общ. ред. М. Г. Коршекевича, М. А. Городецкой. – Минск: РИВШ, 2024. – 124 с.

2. Постатейный комментарий к Закону Республики Беларусь «О защите персональных данных». – URL: https://cpd.by/pravovaya-osnova/metodologicheskiye-dokumenty-rekomendatsii/postatejnyj-kommentarij-k-zakonu-respubliki-belarus-o-zashhite-personalnyh-dannyh/ (дата обращения: 08.09.2024).

3. *Гавриленко, А. И.* К вопросу о реализации конституционного права на защиту персональных данных / А. И. Гавриленко // Современные новеллы Конституции Респ. Беларусь: сб. науч. ст. / БГУ, Юридический фак., Каф. конституционного права; [редкол.: Г. А. Василевич (отв. ред.) и др.]. – Минск: БГУ, 2023. – С. 22–25.

4. *Гавриленко, А. И.* Вынесение требования об устранении нарушений без проведения проверки / А. И. Гавриленко // Юрист. – 2024. – № 7. – С. 52–53.

5. *Гавриленко, А. И.* К вопросу о праве субъекта персональных данных на получение информации, касающейся обработки персональных данных / А. И. Гавриленко // Право.by. – 2024. – № 1. – С. 99–105.

6. *Гавриленко, А. И.* К вопросу о Реестре операторов персональных данных / А. И. Гавриленко // Актуальные проблемы развития правовых институтов в контексте глобальных вызовов: сб. науч. ст. / ГрГУ им. Янки Купалы; редкол.: С. Е. Чебуранова (гл. ред.) [и др.]. – Гродно: ГрГУ, 2024. – С. 112–115.

7. *Гавриленко, А.* Контрольная деятельность Национального центра защиты персональных данных / А. Гавриленко // Юрист. – 2024. – № 7. – С. 26–30.

8. *Гавриленко, А. И.* Актуальные вопросы правового регулирования обработки специальных персональных данных / А. И. Гавриленко // Право.by. – 2024. – № 5 (91). – С. 7–13.

9. *Гавриленко, А. И.* К вопросу о возрасте согласия на обработку персональных данных / А. И. Гавриленко // Актуальные проблемы гражданского права. – 2023. – № 2 (22). – С. 95–106.

10. *Гавриленко, А. И.* К вопросу о критериях согласия на обработку персональных данных / А. И. Гавриленко // Инновационный потенциал развития юридической науки и практики в современной мире: сб. науч. ст. / ГрГУ им. Янки Купалы; редкол.: С. Е. Чебуранова (гл. ред.) [и др.]. – Гродно, ГрГУ, 2023. – С. 83–86.

11. *Гавриленко, А. И.* К вопросу о праве субъекта персональных данных на получение информации, касающейся обработки персональных данных / А. И. Гавриленко // Право.by. – 2024. – № 1. – С. 99–105.

12. *Гавриленко, А. И.* Особенности реализации мер по обеспечению защиты персональных данных государственными органами в условиях цифровой трансформации / А. И. Гавриленко // VI Международный форум молодых управленцев «Теоретико-методологические и прикладные аспекты государственного управления»: сб. материалов / Академия управления при Президенте Респ. Беларусь; редкол.: В. Г. Швайко [и др.]; под науч. ред. О. Н. Солдатовой. – Минск: Академия управления при Президенте Респ. Беларусь, 2024. – С. 36–38.

13. *Гаев, А. А.* На защите персональных данных граждан. Три года Национальному центру защиты персональных данных Республики Беларусь / Гаев А. А. // Право.by. – 2024. – № 5 (91). – С. 5–6.

14. *Гаев, А. А.* Есть такая профессия – персональные данные защищать! / А. А. Гаев // Юрист. – 2023. – № 4. – С. 70–72.

15. *Гаев, А. А.* Национальному центру защиты персональных данных 1 год / Гаев А. А. // Юстиция Беларуси. – 2022. – № 11. – С. 20–22.

16. *Гайкевич, Д. Н.* Механизм действий ответственного лица (DPO) при осуществлении внутреннего контроля за обработкой персональных данных / Д. Н. Гайкевич // ilex: информ. правовая система. – Дата публ.: 29.04.2024 (дата обращения: 14.10.2024).

17. *Гайкевич, Д. Н.* Удаление (уничтожение) персональных данных / Д. Н. Гайкевич // ilex: информ. правовая система. – Дата публ.: 29.04.2024 (дата обращения: 15.10.2024).

18. *Городецкая, М. А.* О некоторых вопросах уголовной ответственности за нарушение законодательства о персональных данных / М. А. Городецкая // Практика осуществления правосудия и правоохранительной деятельности в контексте функционирования национальной правовой системы. – 2024. – С. 233–237.

19. *Городецкая, М. А.* Правовые основания обработки персональных данных в учреждениях высшего образования / М. А. Городецкая // Актуальные проблемы гражданского права. – 2023. – № 2 (22). – С. 16–31.

20. *Городецкая, М. А.* Согласие на обработку персональных данных несовершеннолетних: к вопросу о «возрасте цифрового согласия» / М. А. Городецкая // Правовая политика, наука, практика-2023: материалы Респ. науч.-практ. конф., Минск, 5 окт. 2023 / Нац. центр законо-

дательства и правовых исслед. Респ. Беларусь; редкол.: Е. В. Семашко [и др.]. – Минск: Кологрaд, 2023.

21. *Городецкая, М. А.* Защита персональных данных умерших лиц: сравнительно-правовое исследование / М. А. Городецкая // Право.by. – 2024. – № 5 (91). – С. 14–24.

22. Государственная политика информационной безопасности и информационное противоборство: учеб. пособие / В. Ю. Арчаков [и др.]; Акад. упр. при Президенте Респ. Беларусь. – 2-е изд., стер. – Минск: Академия управления при Президенте Республики Беларусь, 2021. – 228 с.

23. *Диско, В. И.* Типичные нарушения законодательства о персональных данных / В. И. Диско // Юстиция Беларуси. – 2024. – № 10. – С. 11–14.

24. *Захилько, К. С.* Минимальный перечень документов по вопросам защиты персональных данных в организации: актуально на 19 февр. 2024 г. / К. С. Захилько // ilex: информ. правовая система (дата обращения: 13.10.2024).

25. *Полещук, Д. Г.* Совершенствование уголовно-правовых средств охраны информационной безопасности: новые подходы и проблемные аспекты / Д. Г. Полещук // Юстиция Беларуси. – 2021. – № 11. – С. 10–16.

26. *Полещук, Д. Г.* Уголовная ответственность за незаконные действия с персональными данными: новое в законодательстве и правоприменении / Д. Г. Полещук // Ilex: информ. правовая система (дата обращения: 23.10.2024)

27. *Полещук, Д. Г.* Уголовная ответственность за незаконные действия с персональными данными: новеллы правового регулирования и направления их возможного практического применения / Д. Г. Полещук // Право в современном белорусском обществе: сб. науч. тр. / Нац. центр законодательства и правовых исслед. Респ. Беларусь, редкол.: Н. А. Карпович (гл. ред.) [и др.]. – Минск: Колорград, 2021. – Вып. 16. – С. 756–768.

28. *Полещук, Д. Г.* Уголовно-правовая охрана информационной безопасности: актуальные проблемы теории и практики / Д. Г. Полещук; под науч. ред. Д. В. Шаблинской; Нац. центр законодательства и правовых исследований Респ. Беларусь. – Минск: Колорград, 2022. – 239 с.

29. *Полещук, Д. Г.* Право на защиту персональных данных: конституционные основы и их реализация в законодательстве и правоприменении / Д. Г. Полещук // Конституционное право как фактор динамичного развития белорусского государства: история и современность: материалы Респ. науч.-практ. конф., Минск, 15 окт. 2021 г. / БГУ, юрид. фак. каф. конституционного права; [редкол.: Г. А. Василевич (отв. ред.), В. Е. Петухова, А. В. Шавцова]. – Минск: БГУ, 2021. – С. 215–219.

30. *Полещук, Д. Г.* Видеонаблюдение и видеосъемка как обработка персональных данных / Д. Г. Полещук // Актуальные проблемы гражданского права. – 2023 – № 2 (22) – С. 32–48.

31. *Пырко, И. А.* Использование видеонаблюдения в целях обеспечения общественной безопасности: зарубежный опыт и регулирование в Республике Беларусь / И. А. Пырко, Н. А. Швед // Актуальные проблемы гражданского права. – 2023. – № 2 (22). – С. 16–31.

32. *Пырко, И. А.* Типичные нарушения при обработке персональных данных в трудовых отношениях. По итогам практической конференции // Ilex: информ. правовая система. – Дата публ.: 10.10.2023 (дата обращения: 02.02.2025).

33. Руководство по обработке персональных данных в учреждении образования. Электронное пособие / Н. А. Швед; под ред. Е. Плехановой. – Минск: Информационное правовое агентство Гревцова, 2024. – 102 с.

34. *Саванович, Н. А.* Уголовная ответственность за незаконные действия с персональными данными / Н. А. Саванович. – URL: Режим доступа: https://pravo.by/novosti/novosti-pravo-by/2021/june/65098/ (дата обращения: 01.04.2024).

35. *Синюк, Е. В.* К вопросу об ограничении права знакомиться с материалами, непосредственно относящимися к рассмотрению обращений / Е. В. Синюк // Актуальные проблемы гражданского права. – 2023. – № 2 (22). – С. 104–113.

36. Типичные нарушения законодательства о персональных данных // Юрист. – 2023. – № 4. – С. 48–49.

37. Уголовно-правовая охрана информационной безопасности: актуальные проблемы теории и практики: монография / Д. Г. Полещук; под науч. ред. Д. В. Шаблинской; Нац. центр законодательства и правовых исследований Респ. Беларусь. – Минск: Колорград, 2022. – 239 с.

38. *Шакель, Н. В.* Права субъектов персональных данных и юридические возможности их защиты в Республике Беларусь / Н. В. Шакель // Весн. Гродз. дзярж. ун-та ім. Я. Купалы. – 2022. – Т. 12, № 3. – С. 14–19.

39. *Швед, Н. А.* Формируем перечень документов по защите персональных данных / Н. А. Швед // Директор школы, гимназии, лицея. – 2023. – № 3.

40. *Швед, Н. А.* Права субъектов персональных данных: что надо знать директору / Н. А. Швед // Директор школы, гимназии, лицея. – 2023. – № 8. – С. 20–23.

41. *Швед, Н. А.* Требования законодательства: какие меры должны быть приняты школами по защите персональных данных / Н. А. Швед // Настаўніцкая газета. – 2024. – 26 верасня.

42. *Швед, Н. А.* Уголовная ответственность за нарушение законодательства о персональных данных / Н. А. Швед // Юрист. – 2023. – № 12. – С. 45–48.

43. *Швед, Н. А.* Административная ответственность за нарушение законодательства о защите персональных данных / Н. А. Швед // Юрист. – 2023. – № 10. – С. 38–41.

44. *Швед, Н. А.* Гражданско-правовая ответственность за нарушение законодательства о персональных данных / Н. А. Швед // Юрист. – 2023. – № 11. – С. 35–38.

45. *Швед, Н. А.* Дисциплинарная ответственность за нарушение законодательства о персональных данных / Н. А. Швед // Юрист. – 2023. – № 7. – С. 39–42.

46. *Швед, Н. А.* Обеспечение защиты персональных данных как составляющая экономической безопасности / Н. А. Швед // Право национальной экономической безопасности: проблемы формирования и пути их решения: материалы Междунар. науч.-практ. кругл. стола, 27 июн. 2024 г. / Институт экономики НАН Беларуси, Белорусский государственный университет; редкол.: Е. Н. Гладкая [и др.]. – Минск: Право и экономика, 2024. – С. 38–42.

Учебное издание

Гавриленко Алексей Игоревич
Гайкевич Денис Николаевич
Диско Виталий Иванович и др.

МЕРЫ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Учебное пособие

Компьютерная верстка *К. А. Капустиной*
Редактор *А. И. Кизик*

Подписано в печать 13.06.2025. Формат 60×84/16.
Бумага офсетная. Ризография.
Усл. печ. л. 4,4. Уч-изд. л. 4,8. Тираж 200 экз. Заказ 53.

Издатель и полиграфическое исполнение:
государственное учреждение образования
«Республиканский институт высшей школы».
Свидетельство о государственной регистрации издателя,
изготовителя, распространителя печатных изданий
№ 1/174 от 12.02.2014.
Ул. Московская, 15, 220007, г. Минск.