Министерство образования Республики Беларусь

Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ»

Факультет компьютерных систем и сетей

Кафедра гуманитарных дисциплин

РЕФЕРАТ  
На тему: «Информация ограниченного распространения»

Выполнил: студент 3 курса

группы №250541

Власов Р. Е.

Проверил:

\_\_\_\_\_\_\_\_\_

МИНСК 2025

План

1. Персональные данные
2. Гриф и степень секретности информации
3. Служебная информация ограниченного распространения

4. Шифрование фразы

**1. Персональные данные**

Персональные данные (ПД) — любая информация, относящаяся к идентифицированному физическому лицу или физическому лицу, которое может быть идентифицировано

**1.1 Персональные данные  как разновидность информации ограниченного распространения**

В белорусском праве персональные данные занимают особое место среди сведений ограниченного распространения. С одной стороны, они образуют «неприкосновенное ядро» частной жизни, а с другой — активно циркулируют в цифровых сервисах, системах гос‑управления и коммерческого оборота. Именно поэтому защита ПД рассматривается не только как элемент кибербезопасности, но и как способ гарантировать базовые конституционные права граждан.

**1.2. Что такое персональные данные**

Действующий Закон РБ № 99‑З «О защите персональных данных» определяет ПД как любую информацию об идентифицированном либо потенциально идентифицируемом человеке. В перечень входят как «обычные» сведения (ФИО, контакты, адрес), так и «специальные» — расовая и национальная принадлежность, здоровье, политические взгляды, биометрия, генетика и т. д. Именно специальные ПД порождают наибольшие риски для личности и потому находятся под более строгими ограничениями — к примеру, без письменного согласия субъекта их обрабатывать нельзя, за исключением узкого круга случаев, прямо обозначенных в законе.

**1.3. Почему персональные данные относятся к информации ограниченного распространения**

C практической точки зрения любой набор ПД обладает тремя чувствительными свойствами:

* Однозначно связывает сведения с конкретным человеком. Утечка телефона либо скана паспорта сразу подводит злоумышленника к реальной персоне.
* Хранит «следы поведения». Клиентские базы, медицинские карты, записи видеонаблюдения фиксируют поведение и привычки, а их разглашение порождает угрозу дискриминации или преследования.
* Часто содержит коммерческую ценность. Рынок спам‑рассылок, таргет‑рекламы и социальной инженерии питается именно ПД.

Чтобы не «парализовать» цивильный обмен данными, законодатель разрешает распространять ПД только в пределах, необходимых для достижения конкретной, заранее обозначенной цели. За рамками такой цели данные превращаются в информацию ограниченного распространения, и доступ к ним должен либо прекращаться, либо строго регламентироваться.

**1.4. Ключевые принципы обработки**

Закон 99‑З закрепляет семь фундаментальных идей, которые образуют «этический каркас» работы с ПД: законность, прозрачность, целевое ограничение, минимизация, точность, ограничение хранения и конфиденциальность. На практике это означает, что оператор:

1. Чётко формулирует основания обработки. Чаще всего — согласие субъекта, но возможны и контракт, закон, жизненно важные интересы и пр.
2. Собирает только нужное. Скан паспорта не должен храниться в системе лояльности, если достаточно номера телефона.
3. Хранит данные не дольше, чем нужно. Большинство внутренних политик устанавливают «минимальный жизненный цикл»: после окончания договора или услуги сведения подлежат обезличиванию либо уничтожению.
4. Защищает конфиденциальность. Используются шифрование, разграничение прав, журналы аудита; доступ — исключительно по роли.

Эти принципы делают ПД «гибридной» категорией: они не столь секретны, как государственные тайны, но и не свободны к публичному обороту, как новостной контент.

**1.5. Жизненный цикл и практические этапы защиты**

* Сбор. Человек подписывает согласие в мобильном приложении, заполняет анкету или отправляет резюме. В этот момент субъект должен получить «паспорт обработки» — кто, зачем и как долго будет держать его ПД.
* Хранение. Данные размещаются либо на серверах в Беларуси, либо в государствах, признанных обеспечивающими «достаточный уровень защиты». С 1 января 2024 г. сведения о таких ресурсах обязаны вноситься в государственный Реестр операторов ПД, который ведёт Национальный центр защиты персональных данных (НЦЗПД).
* Использование. Сотрудник банка видит вашу кредитную историю, врач — электронную карту, маркетолог — агрегированные профили без прямой идентификации (псевдонимизация).
* Передача. Трансграничный экспорт ПД возможен лишь после проверки, соответствует ли иностранная юрисдикция белорусским стандартам защиты, либо при наличии отдельного разрешения НЦЗПД.
* Удаление/обезличивание. Файлы стираются без возможности восстановления, бумажные носители шредируются; резервные копии очищаются синхронно.

**1.6. Риск‑ландшафт: от инсайдеров до биг‑даты**

Исследования НЦЗПД показывают, что к 2024 году количество жалоб граждан выросло почти втрое, а самые частые нарушения остаются прежними: обработка без правовых оснований, проблемы с получением согласия и «бумажный» DPO, которому не дают реальных полномочий.  К этой «классике» добавились угрозы эпохи больших данных: повторная идентификация при объединении разных баз, злоупотребления нейросетями для генерации портретов и фишинг‑кампании, использующие слитые e‑mail и логины.

**1.7. Инструменты защиты**

Белорусский регулятор предпочитает «риск‑ориентированный» подход: меры соотносятся с масштабом, природой и контекстом обработки. На практике это выражается в трёх уровнях:

* Организационном — назначение ответственного (DPO), утверждение политики обработки, регулярные тренинги, внутренний аудит.
* Техническом — шифрование (TLS 1.3, AES‑256), сегментированные сети, SIEM и DLP‑системы, двуфакторная аутентификация, маскирование полей в рабочих интерфейсах.
* Правовом — договоры с подрядчиками, оценка импакта (DPIA) для чувствительных операций, регистрация в Реестре и уведомление НЦЗПД об инцидентах.

**1.8. Контроль и ответственность**

Надзор осуществляет НЦЗПД, который с конца 2021 г. проводит плановые, внеплановые и камеральные проверки. В 2024 году их было 47, и нарушение нашли в каждой. Штрафы по ст. 23.7 КоАП достигают 200 базовых величин; дополнительно возможен гражданский иск о возмещении морального вреда или дисциплинарные санкции вплоть до увольнения. Несмотря на жёсткие пределы, регулятор по‑прежнему отдаёт предпочтение предписаниям и рекомендациям, оставляя наказание «тяжёлой артиллерией» на случай явного игнорирования требований.

**1.9. Вывод**

Персональные данные — это «нервная система» цифрового общества; их защита формирует доверие как к государственным e‑сервисам, так и к бизнес‑экосистеме. Ограничение распространения ПД не сводится к запретам: оно заставляет операторов строить прозрачные процессы, а субъектов — активнее пользоваться своими правами доступа и контроля. В результате выигрывают обе стороны: организации получают устойчивую репутацию, граждане — уверенность, что их цифровой образ не выйдет из‑под контроля.

**2. Гриф и степень секретности информации**

Гриф секретности – реквизит, проставляемый на носителе государственных секретов и (или) сопроводительной документации к нему, свидетельствующий о степени секретности содержащихся на этом носителе государственных секретов

Носитель государственных секретов – материальный объект, на котором государственные секреты содержатся в виде символов, образов, сигналов и (или) технических решений и процессов, позволяющих их распознать и идентифицировать

Степень секретности – показатель важности государственных секретов, определяющий меры и средства защиты государственных секретов

Вопрос засекречивания сведений в Беларуси регулирует специальный Закон «О государственных секретах» № 170‑З от 19 июля 2010 г. Он вводит двухуровневую систему тайн — государственную и служебную — и связывает степень секретности (то есть тяжесть возможного ущерба) с конкретным «грифом», который проставляется на каждом носителе документа.

**2.1. Откуда берётся секректность**

Закон начинается с понятия государственные секреты — это сведения, разглашение которых может повлечь вред обороноспособности, внешней безопасности, разведывательным интересам, экономической устойчивости или международным обязательствам государства. Внутри этой категории сразу выделяются две «подкатегории»:

* Государственная тайна — наносит тяжкий (критический) вред.
* Служебная тайна — наносит существенный (но не критический) вред.

Такое разделение позволяет не «засекречивать всё подряд»: чем ниже потенциальный урон, тем мягче режим и короче срок ограничения.

**2.2. Скаляр вреда: степени секретности**

Закон устанавливает три формальных ступени — по сути, шкалу тяжести последствий утечки:

A screenshot of a computer

Description automatically generated

Сравнить их легко по вопросу: «Что случится, если файл попадёт в руки постороннего?». При «особой важности» речь идёт о критическом кризисе, при «совершенно секретно» — о тяжёлом, но управляемом повреждении, при «секретно» — о заметном осложнении работы государства.

**2.3. Гриф секретности: зачем он нужен и как выглядит**

Гриф — это визуальный ярлык на самом носителе (бумага, флешка, сервер), который сообщает пользователю два факта:

1. перед ним секретный документ,

2. какова его степень секретности.

Выглядит это буквально надписью заглавными буквами:

* «ОСОБОЙ ВАЖНОСТИ» или «СОВЕРШЕННО СЕКРЕТНО» — если документ относится к государственной тайне;
* «СЕКРЕТНО» — если речь о служебной тайне.

Гриф печатают (или выводят штампом) в правом верхнем углу титульного листа, а затем дублируют на каждом листе через косую черту: «СЕКРЕТНО/экз. № \_\_\_».

**2.4. Кому решать, что именно засекретить**

Право отнести сведения к тайне принадлежит организации‑владельцу совместно с профильным госорганом и Межведомственной комиссией по защите государственных секретов при Совбезе. Каждое министерство утверждает Перечень сведений, подлежащих засекречиванию; его обязаны ежегодно пересматривать, чтобы исключить устаревшие позиции. Тем самым закон заставляет бюрократию «чистить чуланы» и не хранить лишнего под замком.

**2.5. Сроки засекречивания и рассекречивание**

* Государственная тайна может оставаться закрытой до 30 лет с момента присвоения степени; продление допускается, но только после спецэкспертизы.
* Служебная тайна держится до 10 лет. Если по истечении срока вред несоразмерен пользе засекречивания, сведения рассекречивают досрочно.

Таким образом, секретность — не «приговор навсегда», а динамичный режим, подлежащий постоянной переоценке.

**2.6. Допуск: три «формы» доступа для чиновников и инженеров**

Для работы с документами каждой ступени человек проходит проверку (ФСБ‑образный режим) и получает одну из трёх форм допуска:

* Форма № 1 — к сведениям «особой важности»;
* Форма № 2 — к «совершенно секретно»;
* Форма № 3 — к «секретно».

Проверка охватывает биографию, судимости, зарубежные поездки, финансовое состояние. Для форм № 1‑2 добавляется медкомиссия и опрос членов семьи; срок действия допуска — пять лет (с возможностью продления). Носители «высокой» формы могут временно ограничиваться в праве выезда за границу, что служит дополнительным инструментом защиты.

**2.7. Техника защиты носителей**

* Бумажные документы хранятся в сейфах 1‑го или 2‑го класса, учёт ведётся в специальных журналах, выдача — под подпись. При копировании гриф дублируют на каждом отпечатке.
* Электронные носители — на выделённых сегментах сети, отделённых межсетевыми экранами и крипто‑VPN; контролируются системы обнаружения утечек (DLP) и журналирование действий пользователей.
* Передача данных «особой важности» осуществляется только службой специальной связи либо через закрытые волоконные каналы с сертифицированным шифрованием.

**2.8. Ответственность за нарушения**

Административная: ст. 23.11 КоАП (штраф, конфискация носителя).

Уголовная: ст. 373–375 Уголовного кодекса — за разглашение государственной тайны (до семи лет лишения свободы).

При этом суд учитывает форму допуска, степень секретности и умысел: случайная потеря часто заканчивается штрафом, умышленная продажа сведений — реальным сроком.

**2.9. Почему это важно для информационной безопасности**

Гриф секретности — не бюрократическая формальность, а «маркер» уровня угрозы. Он задаёт:

1. глубину криптографической и физической защиты;

2. ширину воронки доступа (чем выше степень — тем меньше людей её получают);

3. масштаб аудита: документы «особой важности» проверяются чаще, хранение и уничтожение фиксируются актами.

В итоге система степеней и грифов работает как регулятор потоков данных: она старается удержать документы в пределах тех подразделений и технологий, где риск контролируем.

**3. Служебная информация ограниченного распространения**

Служебная информация ограниченного распространения — это сведения, касающиеся деятельности государственного органа, юридического лица, распространение и (или) предоставление которых могут причинить вред национальной безопасности Республики Беларусь, общественному порядку, нравственности, правам, свободам и законным интересам физических лиц, в том числе их чести и достоинству, личной и семейной жизни, а также правам и законным интересам юридических лиц и которые не отнесены к государственным секретам.

**3.1. Почему у неё особый режим**

Между публичными сведениями и государственной тайной в белорусской системе лежит «промежуточный слой» — служебная информация ограниченного распространения (СИОР). Её разглашение не создаст критического ущерба обороне, но способно повредить национальной безопасности, общественному порядку, интересам граждан и организаций. Поэтому СИОР получает собственный правовой режим: доступ к ней ограничивается, но масштаб бюрократии и затрат на защиту гораздо ниже, чем для данных с грифами «СОВЕРШЕННО СЕКРЕТНО» или «ОСОБОЙ ВАЖНОСТИ».  Основу этого режима задаёт статья 18‑1 Закона «Об информации, информатизации и защите информации» № 455‑З, принятого ещё в 2008 г., но многократно обновлённого за последние годы.

**3.2. Определение и перечень**

Закон описывает СИОР как сведения, которые могут причинить вред безопасности государства, нравственности или правам граждан, но при этом не отнесены к государственным секретам. Конкретный «скелет» заполняет Постановление Совмина № 783 от 12 августа 2014 г. с приложением‑перечнем. Среди типовых примеров — мобилизационные договоры, схемы охраны пограничных объектов, внутренние методики радиоэлектронной разведки, сводные данные о военной технике, а также служебные отчёты аудита, планы проверок и внутренние статистические сводки министерств.

При этом Постановление разрешает каждому ведомству выпускать собственный перечень: например, Минфин включает в него отчёты о небанковских организациях, а Минздрав — методики транспортировки препаратов крови. Такая гибкость позволяет поднять «заслон» ровно там, где находятся реальные уязвимости, а не закрывать административной бронёй весь документооборот.

**3.3. Как присваивается гриф «ДСП»**

Решение об отнесении сведений к СИОР принимает руководитель органа или уполномоченное им лицо. На документе в правом верхнем углу ставят надпись «ДЛЯ СЛУЖЕБНОГО ПОЛЬЗОВАНИЯ» (Times New Roman ≥ 12 pt) и номер экземпляра; одинаковая отметка появляется на обложке дела, сопроводительном письме и в электронном файле‑метаданных.

Важно: если в тексте только один абзац содержит СИОР, допускается подготовить два варианта — полный (для адресатов по компетенции) и извлечение. Это правило снижает риски, потому что «лишние» разделы не ходят по почте.

**3.4. Доступ, хранение, передача**

* Кто может читать. Доступ определяется списком допущенных; каждый экземпляр выдаётся под роспись, а любой выход сотрудника из проекта закрывает его права в информационной системе.
* Где хранится. Бумажные копии — в сейфах 2‑го класса; электронные — в выделенном сегменте сети под DLP‑и SIEM‑мониторингом. Шифрование (TLS 1.3 для транзита, AES‑256 на диске) и двухфакторная аутентификация обязательны, если документ содержит персональные данные или сведения о критической инфраструктуре.
* Как отправляется. Внутри ведомства — защищённым почтовым шлюзом или по VPN; наружу — только адресатам, указанным в решении об отнесении к СИОР, причём приоритет имеет извлечение, а не полный текст.
* Как копируется. Размножение ограничено: каждая копия получает свой порядковый номер и фиксируется в журнале учёта; сканирование без разрешения ИБ‑подразделения запрещено.

**3.5. Жизненный цикл документа**

Ограничение действует обычно до пяти лет; раз в пять лет перечни и грифа пересматриваются. Повод для досрочного снятия грифа — утрата актуальности или выявление необоснованного засекречивания (частый случай — публиковали такой же отчёт в Едином портале открытых данных). После отмены гриф зачеркивают, на полях ставят дату, номер распоряжения и рассылают уведомления всем адресатам.

**3.6. СИОР и коммерческая тайна — в чём разница**

Гриф «ДСП» существует параллельно с режимом коммерческой тайны (Закон «О коммерческой тайне» № 16‑З) и часто встречается в одних документах. Главное различие:

* СИОР защищает публичный интерес государства и общества;
* коммерческая тайна — имущественный интерес собственника информации.

Если отчёт одновременно содержит и секреты фирмы, и служебные сведения министерства, на нём проставляют два грифа или выпускают раздельные варианты.

**3.7. Ответственность за нарушение режима**

* Административная: КоАП, статья 23.8 — разглашение либо утрата СИОР по неосторожности (штраф 4–20 базовых величин).
* Уголовная: УК, статья 377 — хищение или уничтожение документов с служебной тайной (до трёх лет лишения свободы), статья 376 — незаконные средства для негласного получения такой информации.
* Дисциплинарная: выговор, лишение премии, увольнение.

При расследовании смотрят, была ли выполнена внутренняя политика ИБ: хранился ли журнал копий, шифровались ли файлы, действовали ли DLP‑правила. Если организация не ввела меры, предписанные Постановлением 783, регулятор может вынести предписание и отдельный штраф.

**3.8. Практическая значимость для специалиста ИБ**

Для безопасности‑менеджера гриф «ДСП» — это маркер уровня защиты:

* настраиваем правило DLP «Document.Tag = DSP → block external mail»;
* включаем обязательную маркировку водяным знаком на печать из СЭД;
* аудит доступа должен храниться не менее срока действия грифа плюс один год;
* инцидент‑репорт в 24 часа в ведомственный ИБ‑центр и руководителю.

Такой подход позволяет соблюдать баланс: защищать реально чувствительные сведения, не превращая весь документооборот в зону тотального секрета, а значит — оставить организации гибкость и быстроту процессов.

**Итого.** Служебная информация ограниченного распространения — это эластичная «подушка безопасности» между открытым оборотом данных и жёсткой государственной тайной. Благодаря Закону 455‑З и Постановлению 783 каждая структура может гибко отнести уязвимые сведения к СИОР, присвоить гриф «ДСП», ввести доступ по ролям, шифрование и аудит, а после утраты актуальности — снять ограничения. Такой режим минимизирует риск утечек без излишней бюрократии и соответствует принципу «столько секретности, сколько нужно, но не больше».

**Шифрование фразы:**

“Безопасность всегда важнее скорости”  
Ключ – Власов

1) Присваиваем каждой букве индекс от 0 до 32:

2) Подготовка ключа:

Фразу разбиваем на буквы (пробелы и знаки препинания пропускаем при шифровании).

Длина фразы (без пробелов) — 30 символов.

Ключ «Власов» повторяем циклически, чтобы он был той же длины:

“В Л А С О В В Л А С О В В Л А С О В В Л А С О В В Л А С О В”

3) Преобразование букв в числа

Для каждого символа текста и ключа по отдельности находим индекс в алфавите.

Например, первые пять букв фразы «Безоп» и ключа «Власо»:

Б (1), Е (5), З (7), О (15), П (16)

В (2), Л (11), А (0), С (18), О (15)  
4) Сложение по модулю 33

Cᵢ = (Pᵢ + Kᵢ) mod 33

Где Pᵢ — индекс открытой буквы, Kᵢ — индекс буквы ключа, Cᵢ — индекс зашифрованной буквы.

Проделаем для первых трёх символов:

* + i=1: (1 + 2) mod 33 = 3 → индекс 3 = «Г»
  + i=2: (5 +11) mod 33 = 16 → индекс 16 = «П»
  + i=3: (7 + 0) mod 33 = 7  → индекс 7 = «З»

Так последовательно рассчитываем для всех 30 букв и переводим индексы Cᵢ обратно в буквы. В результате получается строка без пробелов, после этого для удобства добавляем пробелы:

ГРЗАЮВУЩОГБЮ ДЭЕФТВ ДЛЖЯУЖ УЦОВЭУФФ

Список используемых источников

1. Закон Республики Беларусь от 7 мая 2021 г. № 99‑З «О защите персональных данных» (в ред. от 11.01.2024) // Национальный правовой Интернет‑портал РБ, 14.05.2021, № 2/2837.
2. Закон Республики Беларусь от 10 ноября 2008 г. № 455‑З «Об информации, информатизации и защите информации» (в ред. от 13.07.2023) // НПИ‑портал РБ, 20.11.2008, № 2/1525.
3. Закон Республики Беларусь от 19 июля 2010 г. № 170‑З «О государственных секретах» (в ред. от 08.01.2023) // НПИ‑портал РБ, 27.07.2010, № 2/1716.
4. Указ Президента Республики Беларусь от 1 февраля 2010 г. № 60 «О мерах по совершенствованию использования национального сегмента сети Интернет» // НПИ‑портал РБ, 05.02.2010, № 1/11412.
5. Постановление Совета Министров Республики Беларусь от 15 октября 2021 г. № 638 «Об осуществлении отдельных положений Закона Республики Беларусь «О защите персональных данных»» // НПИ‑портал РБ, 19.10.2021, № 5/49837.
6. Приказ Оперативно‑аналитического центра при Президенте Республики Беларусь от 12 ноября 2021 г. № 194 «Об утверждении Инструкции о реестре операторов персональных данных» // НПИ‑портал РБ, 16.11.2021, № 8/37737.
7. Постановление Совета Министров Республики Беларусь от 12 августа 2014 г. № 783 «Об утверждении перечней сведений, составляющих служебную информацию ограниченного распространения, и порядке работы с ними» (в ред. от 05.12.2024) // НПИ‑портал РБ, 16.08.2014, № 5/39350.
8. Кодекс Республики Беларусь об административных правонарушениях: ст. 23.7, 23.8, 23.11 (ред. от 01.03.2025) // НПИ‑портал РБ.
9. Уголовный кодекс Республики Беларусь: ст. 373–377 (ред. от 15.01.2025) // НПИ‑портал РБ.
10. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements.
11. Сайт Национального правового Интернет‑портала Республики Беларусь – <pravo.by> (дата обращения: апрель 2025 г.).