Примерный перечень вопросов (”чек-лист“), изучаемых Центром в ходе осуществления контрольной деятельности по вопросам реализации технических мер по обеспечению защиты персональных данных.

1. Данный перечень вопросов (”чек-лист“) позволит операторам (уполномоченным лицам) самостоятельно подтвердить исполнение требований законодательства о персональных данных в части реализации технических мер по обеспечению технической защиты персональных данных, направлен на повышение эффективности принимаемых мер для их защиты, а также на недопущение наиболее типичных нарушений при реализации этих мер.

Перечень является примерным и неисчерпывающим. При осуществлении контрольных мероприятий Центром могут изучаться и иные вопросы с учетом специфики бизнес-процессов конкретного оператора (уполномоченного лица), а также мер, принятых им в рамках риск-ориентированного подхода.

2. Технические меры по обеспечению защиты персональных данных не должны быть формальными.

В этой связи при оценке их эффективности изучается не только содержание документов оператора (уполномоченного лица), свидетельствующих о принятых мерах по обеспечению защиты персональных данных, но и их фактическая реализация (например, в ходе анализа его информационных ресурсов (систем), используемых средств защиты информации и т.д.).

3. При проведении плановой или внеплановой проверок изучаются следующие вопросы:

№	Объект контроля	Пояснение
1	Назначение лица (подразделения), ответственного за информационную безопасность.	Проверяется наличие приказа о назначении такого лица (создании структурного подразделения), должностная инструкция (положение о структурном подразделении).
2	Прохождение обучения лицом, в обязанности которого входит обеспечение информационной безопасности.	Проверяется прохождение обучения по образовательной программе повышения квалификации руководящих работников и специалистов по вопросам технической и (или) криптографической защиты информации (наличие свидетельства о повышении квалификации).
3	Перечень информационных ресурсов (систем), содержащих персональные данные, собственником (владельцем) которых является оператор (уполномоченное лицо), а также категорий персональных данных,	Проверяется факт ведения перечня таких ресурсов (систем) и правильность категорирования обрабатываемой в них информации посредством анализа баз данных информационных ресурсов (систем) или иных инструментов. Дополнительно запрашивается оборотно-сальдовая ведомость нематериальных активов оператора (уполномоченного лица) для проверки полноты и актуальности перечня.

	подлежащих включению в данные ресурсы (системы).	
4	Информационные ресурсы (системы), связанные с предметом деятельности оператора (уполномоченного лица), в которых обрабатываются персональные данные. Документы, определяющие порядок функционирования информационных ресурсов (систем), техническая документация в отношении таких ресурсов.	Проверяется избыточность обработки персональных данных в информационных ресурсах (системах) оператора (уполномоченного лица). Проверяется объем передаваемых персональных данных в соответствии с технической документацией для глобальных (смежных) информационных ресурсов (систем).
5	Типовые для операторов (уполномоченных лиц) информационные ресурсы (системы) (кадровый учет, бухгалтерское обеспечение и т.д.), в которых обрабатываются персональные данные.	Проверяется отсутствие избыточности персональных данных, обрабатываемых в информационных ресурсах (системах) для целей ведения хозяйственной деятельности оператора (уполномоченного лица) (трудовые отношения, бухгалтерский учет и т.д.).
6	Порядок осуществления видеонаблюдения.	Проверяется соответствие законодательству мест установки камер и зон их охвата, прав доступа к записям, сроков их хранения и информирование субъектов.
7	Официальные интернет-ресурсы.	Проверяются: аккаунты оператора (уполномоченного лица) в мессенджерах или социальных сетях на факты распространения персональных данных работников и иных лиц без правовых оснований; обработка cookie-файлов; размещение документов, определяющих политику обработки персональных данных оператора (уполномоченного лица); использование форм обратной связи; обработка персональных данных в личных кабинетах пользователей (при их наличии); принадлежность доменного имени.
8	Порядок доступа к персональным данным, в том числе обрабатываемым в информационном ресурсе (системе) (далее – порядок доступа).	Проверяется соблюдение порядка доступа ко всем информационным ресурсам (системам), используемым у оператора (уполномоченного лица), а также систематизированным местам хранения документов, содержащих персональные данные, и производится сверка технологических ролей (прав) доступа работников в информационных ресурсах (системах) на соответствие указанному в порядке доступа. Также анализируется учет представителей уполномоченных лиц, имеющих доступ к информационным ресурсам (системам), собственником (владельцем) которых является проверяемый оператор (уполномоченное лицо).

9	Местонахождение систем хранения данных и (или) передача персональных данных на территории других стран.	Проверяется используемая инфраструктура (местонахождение, взаимодействие между системами, передача третьим лицам и т.д.).
10	Аттестат соответствия системы защиты информации информационной системы требованиям по защите информации.	При наличии аттестата проверяется соответствие реального состава и структуры объектов информационной системы общей схеме системы защиты информации (проверка наличия средств защиты информации, сертификатов на них, сверка серийных номеров). Проверка внешних маршрутов и подключений. При отсутствии аттестата изучается объем выполненных требований по кибербезопасности объектов информационной инфраструктуры государственных органов и иных организаций, определенных приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 25 июля 2023 г. № 130.
11	Привлекаемые уполномоченные лица по направлению информационных технологий.	Проверяются доступы работников уполномоченных лиц к информационным ресурсам (системам) оператора (уполномоченного лица) на предмет соответствия прав доступа для выполнения возложенных обязанностей.
12	Выборочное изучение персональных электронных вычислительных машин работников на предмет обработки персональных данных в нарушение установленного порядка.	Проверяются хранимые на компьютерах работников и в файловых хранилищах документы/скан-копии/фотографии, содержащие персональные данные на предмет избыточности, а также сроки их хранения.
13	Техническая организация рабочих мест удаленных работников.	Проверяется использование служебных устройств на предмет использования средств защиты информации (при организации рабочих мест) и учет рабочего времени для удаленных работников.
14	Система контроля и управления доступом.	Проверяется обработка такой системой персональных данных на избыточность и на сроки хранения учетной информации о работниках.
15	Методы и средства контроля удаления или блокирования персональных данных уполномоченными лицами при отсутствии оснований для обработки.	Проверяются методы прекращения обработки персональных данных (как техническое, так и документационное обеспечение) уполномоченными лицами и способы контроля такой деятельности со стороны оператора (уполномоченного лица).
16	Использование служебных SIM-карт.	Проверяется наличие (отсутствие) функционала установления местонахождения работников, предоставляемого операторами (уполномоченными лицами) электросвязи по заключенным договорам на услуги электросвязи.

4. Иные вопросы технической защиты персональных данных.

№	Ситуация	Пояснение
1	Получение Центром информации о критической уязвимости информационного ресурса (системы) оператора (уполномоченного лица) (например, код подтверждения регистрации передается в открытом виде в теле HTTP-ответа).	Как правило, проводится внеплановая проверка по конкретному вопросу обеспечения технической защиты персональных данных, связанного с критической уязвимостью. По результатам такой проверки выносится требование о приостановке обработки персональных данных в указанном информационном ресурсе (системе) до устранения критической уязвимости.
2	Получение Центром информации о возможной ”утечке“ персональных данных.	Как правило, Центр информирует оператора (уполномоченного лица) о возможном инциденте. По результатам проведения расследования оператор (уполномоченное лицо) направляет уведомление о нарушении системы защиты персональных данных либо информационное письмо об отсутствии факта ”утечки“.