**Приложение 1**

**Замечания и предложения ОЮЛ «Национальная телекоммуникационная ассоциация Казахстана» (НТА)**

**к проекту постановления Правительства Республики Казахстан «О внесении изменений и дополнений в постановления**

**Правительства Республики Казахстан от 3 сентября 2013 года № 909 «Об утверждении Правил осуществления собственником**

**и (или) оператором, а также третьим лицом мер по защите персональных данных» и от 12 июля 2019 года № 501**

**«О мерах по реализации Указа Президента Республики Казахстан от 17 июня 2019 года № 24 «О мерах по дальнейшему**

**совершенствованию системы государственного управления Республики Казахстан»**

**Общие замечания:**

1. Необходимо пояснение – отсылочная норма на порядок, устанавливаемый Правительством РК по соблюдению необходимых мер по защите ПД подразумевает новый порядок или это отсылка на ПП РК № 909?

 2. В пояснительной записке к Проекту(к примеру, п. 3 и 7), полагаем, должны иметь дополнительные пояснения, которые могут быть использованы и операторами в дальнейшем при разъяснении Проекта, так как любой доступ к ограниченным ПД может иметь резонанс как с сертификатом безопасности.

 3. НТА и операторы неоднократно предлагали исключить резервное копирование или доступ к базам, которые регулируются ЗРК «О связи». К примеру, база данных об абонентах (доступ органов ОРД), база БДИК (EMEI), база MNP (переносимость номеров). Поэтому доступ ГТС предлагается ограничить к этим базам с указанным обоснованием.

 4. Полный доступ ГТС ко всем объектам информатизации выглядит нецелесообразным и в связи с тем, что функции, описанные в Проекте согласно ЗРК«Об информатизации», выполняет оперативный центр информационной безопасности (ОЦИБ). Так, в соответствии с п.1 ст. 7-2 Закона «Об информатизации», ОЦИБ осуществляет деятельность по обнаружению, оценке, прогнозированию, локализации, нейтрализации и профилактике угроз ИБ информационно-коммуникационной инфраструктуры, объектов информатизации, подключенных к ОЦИБ; принимает меры по минимизации угроз ИБ, незамедлительно информирует владельца информационно-коммуникационной инфраструктуры, а также Национальный координационный центр информационной безопасности (ГТС) о факте инцидента информационной безопасности.

4. Проверки-обследования согласно Проекту могут проводиться до 2-х раз в месяц, что также не способствует гос. политике по развитию бизнеса и восстановлению экономического роста (п.2, 13 Пояснительной записки к Проекту).

 5. Считаем, что поправки, устанавливаемые Проектом, необходимо рассматривать вместе с указанным порядком по проведению обследования, а также необходимо разъяснения необходимости в этом со стороны разработчиков, т.к. в ЗРК «Об информатизации» указаны процессы по ИБ, в т.ч. по аудиту информ.систем, который в соответствии с Правилами проведения аудита информационных систем включает подведение результатов инструментального обследования и т.д.

 6.  Доступа к ограниченной информации у ГТС, исходя из целей поправок в Проекте, быть не должно. Кроме того, приведенное обоснование в Проекте не связано с приведением в соответствие с п.1 ст.22 ЗРК «О персональных данных и их защите». Такой доступ может быть описан на уровне законов, а не Правил. Также если говорить о таком обследовании, то скорее это должно проводится не ГТС, а аккредитованными испытательными лабораториями в соответствии ЗРК «О техническом регулировании» (ст.49 ЗРК «Об информатизации»).

7. Считаем, что для целостности и всесторонности позиции НТА и операторов связи по Проекту необходимо совместно с Проектом представить проект Правил регулятора, которым планируется описать порядок доступа ГТС к инфраструктуре.

**СРАВНИТЕЛЬНАЯ ТАБЛИЦА**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Структурный элемент** | **Действующая редакция** | **Предлагаемая редакция разработчика** | **Обоснование разработчика** | **Замечания/позиция НТА** |
| **Постановление Правительства Республики Казахстан от 3 сентября 2013 года № 909**  **«Об утверждении Правил осуществления собственником и (или) оператором, а также третьим лицом мер по защите персональных данных»**  **Правила осуществления собственником и (или) оператором, а также третьим лицом мер по защите персональных данных** | | | | | |
|  | Пункт 3 | 3. Собственник и (или) оператор, а также третье лицо обязаны принимать необходимые меры по защите персональных данных, обеспечивающие:  1) предотвращение несанкционированного доступа к персональным данным;  2) своевременное обнаружение фактов несанкционированного доступа к персональным данным, если такой несанкционированный доступ не удалось предотвратить;  3) минимизацию неблагоприятных последствий несанкционированного доступа к персональным данным. | 3. Собственник и (или) оператор, а также третье лицо обязаны принимать необходимые меры по защите персональных данных **в соответствии с порядком, определяемом Правительством Республики Казахстан и** обеспечивающие:  1) предотвращение несанкционированного доступа к персональным данным;  2) своевременное обнаружение фактов несанкционированного доступа к персональным данным, если такой несанкционированный доступ не удалось предотвратить;  3) минимизацию неблагоприятных последствий несанкционированного доступа к персональным данным.  **4) предоставление доступа государственной технической службе к объектам информатизации, использующих, хранящих, обрабатывающих и распространяющих персональные данные ограниченного доступа, содержащиеся в электронных информационных ресурсах, для осуществления обследования обеспечения защищенности процессов хранения, обработки и распространения персональных данных ограниченного доступа, содержащихся в электронных информационных ресурсах в порядке, определяемом уполномоченным органом.** | В целях приведения в соответствие с пунктом 1 статьи 22 Закона Республики Казахстан «О персональных данных и их защите». | Не согласны и против внесения в пункт 3 Правил осуществления собственником и (или) оператором, а также третьим лицом мер по защите персональных данных подпункта 4) в предложенной редакции по следующим основаниям:  1) в статье 22 Закона РК «О персональных данных и их защите», отсутствует норма касательно обязательства собственника и (или) оператора сбора персональных данных по предоставлению доступа к объектам информатизации, использующих, хранящих, обрабатывающих и распространяющих персональные данные ограниченного доступа;  2) ни в Законе РК «О персональных данных и их защите», ни в Законе РК «Об информатизации» нет норм, которые наделяли бы ГТС функцией по осуществлению обследования обеспечения защищенности процессов хранения, обработки и распространения персональных данных ограниченного доступа, содержащихся в электронных информационных ресурсах;  3) согласно статье 56 Закона РК «Об информатизации», собственники и владельцы информационных систем, получившие электронные информационные ресурсы, содержащие персональные данные, собственник и (или) оператор базы, содержащей персональные данные, а также третьи лица обязаны принимать меры по их защите, т.е. осуществляют это самостоятельно в соответствии с законодательством Республики Казахстан о персональных данных и их защите. |