Об утверждении Требований к обеспечению безопасности и защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных

В соответствии со статьей 21 Закона Кыргызской Республики «Об информации персонального характера», статьями 10 и 17 конституционного Закона Кыргызской Республики «О Правительстве Кыргызской Республики» Правительство Кыргызской Республики постановляет:

1. Утвердить Требования к обеспечению безопасности и защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных (далее – Требования),согласно приложению.
2. Государственному комитету информационных технологий и связи Кыргызской Республики по согласованию с Государственным комитетом национальной безопасности Кыргызской Республики в недельный срок разработать и утвердить:

- Типовой перечень угроз безопасности персональных данных при обработке персональных данных в информационных системах, содержащий все виды и типы предполагаемых угроз;

- методику определения угроз безопасности в информационных системах персональных данных;

- форму перечня видов угроз.

1. Министерствам, государственным комитетам, административным ведомствам, иным государственным органам, органам местного самоуправления (по согласованию) в месячный срок:

- разработать и утвердить отраслевые перечни угроз безопасности персональных данных при обработке персональных данных в информационных системах, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки;

- принять исчерпывающие меры по обеспечению выполнения настоящего постановления.

1. Контроль за исполнением настоящего постановления возложить на отдел строительства, транспорта и коммуникаций и отдел обороны, правопорядка и чрезвычайных ситуаций Аппарата Правительства Кыргызской Республики.
2. Настоящее постановление вступает в силу со дня официального опубликования.

Премьер-министр

С.Дж.Исаков

Приложение

Требования

к обеспечению безопасности и защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных

1. **Общие положения**

1. Настоящие Требования устанавливают уровни защищенности персональных данных при их обработке в информационных системах, критерии угроз безопасности персональных данных, вошедших в перечень угроз, а также требования к обеспечению безопасности и защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных, в соответствии со статьей 21 Закона Кыргызской Республики «Об информации персонального характера».
2. Используемые в настоящих Требованиях понятия употребляются в значениях, определенных законами Кыргызской Республики
«Об информации персонального характера» и «Об электронном управлении».
3. Положения настоящих Требований обязательны для применения государственными органами, органами местного самоуправления, юридическими лицами с участием государства и/или муниципальных образований, а также организациями, финансируемыми из республиканского и местных бюджетов, являющимися владельцами и/или операторами государственных/муниципальных информационных систем, а также иных элементов, входящих в состав государственной инфраструктуры электронного управления, в которых обрабатываются персональные данные, а также всеми держателями (обладателей) массивов персональных данных.

2. **Уровни защищенности персональных данных при их обработке в информационных системах**

4. При обработке персональных данных устанавливаются следующие уровни защищенности в информационных системах:

1. синий;
2. зеленый;
3. желтый;
4. красный.

5. Выбор уровня защищенности персональных данных, обеспечение которого необходимо при их обработке в конкретной информационной системе персональных данных, осуществляется держателем (обладателем) массива персональных данных в следующем порядке:

1. уполномоченный государственный орган по персональным данным разрабатывает и

утверждает Типовой перечень угроз безопасности персональных данных при обработке персональных данных в информационных системах (далее – Типовой перечень), содержащий все виды и типы предполагаемых угроз, а также методику определения угроз безопасности в информационных системах персональных данных (далее – Методика определения угроз);

2. министерства, государственные комитеты, административные ведомства, а также иные государственные органы, органы местного самоуправления на основании Типового перечня, Методики определения угроз разрабатывают и утверждают обязательные для исполнения подведомственными держателями (обладателями) массива персональных данных ведомственные акты об определении перечня угроз безопасности персональных данных при обработке персональных данных в информационных системах, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки;
3. держатель (обладатель) массива персональных данных, исходя из конкретных условий работы с персональными данными, ценности защищаемой информации и стоимости мер по ее защите, а также с учетом уровня технического развития, утверждает собственный перечень угроз безопасности персональных данных (далее – перечень угроз) по форме, утвержденной уполномоченным государственным органом по персональным данным.

В перечень угроз держателем (обладателем) массива персональных данных в обязательном порядке включаются угрозы, определенные в актах, указанных в подпунктах 1 и 2 настоящего пункта, а также, по решению держателя (обладателя) массива персональных данных, и иные угрозы.

Перечень угроз подлежит пересмотру держателем (обладателем) массива персональных данных по мере изменения состава обрабатываемых персональных данных, условий и видов их обработки;

4. ассоциации, союзы и иные объединения держателей (обладателей) массивов персональных данных своими решениями вправе определить дополнительные угрозы безопасности персональных данных при обработке персональных данных в информационных системах, эксплуатируемых при осуществлении определенных видов деятельности членами таких ассоциаций, союзов и иных объединений, с учетом содержания персональных данных, характера и способов их обработки, наряду с угрозами безопасности персональных данных, определенными в ведомственных актах, указанных в подпункте 2 настоящего пункта.

3. **Критерии угроз безопасности, рейтинг угроз**

6. Каждому виду угроз безопасности персональных данных, вошедших в перечень угроз, разработанный держателем (обладателем) массива персональных данных, присваивается рейтинг в зависимости от следующих критериев в соответствии с Методикой определения угроз, указанной в подпункте 1 пункта 5 настоящих Требований:

№ п/п	**Критерий**	**Диапазон баллов**	**Оценка (баллов)**
1.	Актуальность угрозы безопасности персональных данных	0-1 балла	0 - неактуальна; 1 – актуальна.

2.	Возможное причинение вреда субъекту персональных данных, который может быть причинен в случае реализации угрозы	0-3 балла	0 - вред не может быть причинен (не влечет причинения убытков и морального вреда субъекту персональных данных); 1 - незначительный вред, легко компенсируемый держателем (незначительные затраты – менее 1 000 расчетных показателей, на ликвидацию/компенсацию последствий за причиненные убытки и моральный вред); 2 - значительный вред, который может быть компенсирован оператором (влечет значительные затраты – более 1 000 расчетных показателей, на ликвидацию/компенсацию последствий за прочиненные убытки и моральный вред); 3 - критический вред, не может быть компенсирован (влечет причинение убытков и морального вреда, которые не могут компенсированы)
3.	Объем обрабатываемых персональных данных, которые подвержены данной угрозе	1-3 балла	1 - незначительный объем (информационная система обрабатывает персональные данные в объеме, не превышающем 10 000 субъектов персональных данных); 2 - значительный объем (информационная система обрабатывает персональные данные в объеме, более 10 000 до 100 000 субъектов персональных данных); 3 - критический объем (информационная система обрабатывает персональные данные в объеме более 100 000 субъектов персональных данных)

4.	Содержание обрабатываемых персональных данных, которые подвержены данной угрозе	1-2 балла	1 - персональные данные, не относящиеся к специальным категориям; 2 - специальные категории персональных данных (в соответствии с частью 1 статьи 8 Закона Кыргызской Республики «Об информации персонального характера»), а также биометрические данные (в соответствии с частью 3 статьи 5 Закона Кыргызской Республики «О биометрической регистрации граждан Кыргызской Республики»)
5.	Продолжительность деятельности, к которой применима угроза	0-1 балла	0 - краткосрочная (обработка данных не более чем в течение 2 (двух) недель); 1 – долгосрочная

7. Рейтинг угрозы безопасности персональных данных определяется, как произведение баллов по каждому из критериев.
8. Уровни безопасности персональных данных в зависимости от угроз безопасности этих данных определяются для каждой информационной системы или группы информационных систем следующим образом:

1. «синий» – наличие угроз с рейтингом не более 1 балла;
2. «зеленый» – наличие угроз с рейтингом 2 балла (но не более);
3. «желтый» – наличие угроз с рейтингом от 3 до 6 баллов включительно (но не более);
4. «красный» – наличие угроз с рейтингом более 6 баллов.

4. **Требования к защите персональных данных по уровням защищенности**

9. Установленные пунктом 8 настоящих Требований уровни защищенности персональных данных при их обработке в информационных системах персональных данных обеспечиваются выполнением следующих требований:

1. для «синего» уровня защищенности:

- принятием документа, определяющего политику держателя (обладателя) массива персональных данных в отношении обработки персональных данных, и доведением содержания данного документа до работников и контрагентов держателя (обладателя) массива персональных данных;
- назначением лица (лиц), ответственных за обеспечение безопасности персональных данных при их обработке в информационных системах и проведением их инструктажа по требованиям Закона Кыргызской Республики «Об информации персонального характера» и настоящих Требований;

- осуществлением внутреннего контроля соответствия обработки персональных данных требованиям Закона Кыргызской Республики «Об информации персонального характера», и настоящих Требований, иных документов, принятых по вопросам обработки персональных данных;
- включением в трудовые договоры и должностные инструкции работников держателя (обладателя) массива персональных данных их обязанностей в отношении обработки персональных данных, положений о неукоснительном соблюдении требований Закона Кыргызской Республики «Об информации персонального характера», и настоящих Требований, иных документов, принятых по вопросам обработки персональных данных;
- ведением (на бумажном носителе или в электронном виде) журнала учета машинных носителей персональных данных и списка лиц, в чьи должностные обязанности входит доступ к персональным данным;
- при каждом вводе персональных данных в систему обработки данных, а также при изменении или уничтожении таких данных – указанием лица, осуществившего ввод (изменение, уничтожение) таких данных, даты и времени совершения операции;
- созданием не реже одного раза в сутки резервной копии актуальных персональных данных, обрабатываемых в информационной системе персональных данных;

2. для «зеленого» уровня защищенности – требований, установленных для «синего» уровня защищенности, и дополнительно следующих требований:

- проектированием информационной системы и мер по ее развитию с учетом характера обрабатываемых в ней персональных данных и необходимости их защиты;
- оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы и перед значительными обновлениями (расширениями) информационной системы, проводимой уполномоченным государственным органом по персональным данным и/или аккредитованными органами оценки соответствия в области обеспечения требований безопасности персональных данных;
- применением шифровальных (криптографических) средств защиты информации, соответствующих техническим требованиям к таким средствам, для исключения несанкционированного доступа к персональным данным, их преднамеренного или случайного изменения или уничтожения;

3. для «желтого» уровня защищенности – требований, установленных для «зеленого» уровня защищенности, и дополнительно следующих требований:

- централизованным управлением системой защиты персональных данных, в том числе, путем создания структурного подразделения, ответственного за реализацию настоящих Требований;
- установлением системы контроля помещений, в которых установлена информационная система, позволяющей ограничить физический доступ к техническим средствам информационной системы только теми лицами, которым предоставлены соответствующие полномочия;
- ведением автоматического электронного журнала (лога), фиксирующего все операции с персональными данными, с обеспечением невозможности внесения изменений в данный журнал задним числом;
- обеспечением резервирования и высокой доступности информационной системы хранения и обработки персональных данных в реальном времени и автоматического электронного журнала, предусмотренного абзацем четвертым настоящего подпункта;
- наличием автоматической системы выявления и пресечения несанкционированного доступа к персональным данным, а также их случайного уничтожения или изменения;

4. для «красного» уровня защищенности – требований, установленных для «желтого» уровня защищенности, и дополнительно следующих требований:

- использованием только защищенных каналов связи при передаче персональных данных и (или) доступе к ним;
- защитой персональных данных от утечек по техническим каналам;
- применением средств защиты информации и/или информационных систем, прошедших в установленном порядке процедуру оценки соответствия в уполномоченном государственном органе по персональным данным и/или аккредитованном органе оценки соответствия в области обеспечения требований безопасности персональных данных;
- регулярным (не менее 1 раза в год) аудитом информационных систем держателя (обладателя) массива персональных данных автоматического электронного журнала (лога), фиксирующего все операции с персональными данными, уполномоченным государственным органом по персональным данным и/или аккредитованным органом оценки соответствия в области обеспечения требований безопасности персональных данных.
