# Методические рекомендации по организации безопасности персональных данных в соответствии с требованиями Закона КР №58 «Об информации персонального характера»

# Оглавление

Правовые основы методических рекомендаций....3
Терминология....6
Процесс управления персональными данными....8
Самооценка и регистрация Держателя массива персональных данных....9
Пример определения рейтинга безопасности....12
Требования к уровню защищённости....14
Согласие Субъекта ИПХ....21
Перечень типовых идентификаторов ИПХ....21
Форма получения согласия на обработку ИПХ....23
Внедрение режима обработки персональных данных....25
Цель защиты персональных данных....26
Необходимость соответствия при хранении данных в облаке, за рубежом или у сервис-провайдера, в дата-центре....27
Документация....28
Разработка частной модели угроз....30
Цель....31
A1 Описание информационной системы....32
A2 Классификация уязвимостей....32
A3 Определение глобального уровня исходной защищённости $Y_1$....33
A4 Модель нарушителя....36
A6 Угрозы....38
A7 Оценка опасности угроз....39
A8 Вероятность реализации $Y_2$....40
A9 Актуальность угрозы....42
A10 Управление угрозами информационной безопасности....43
A11 Результат....44

# Правовые основы методических рекомендаций

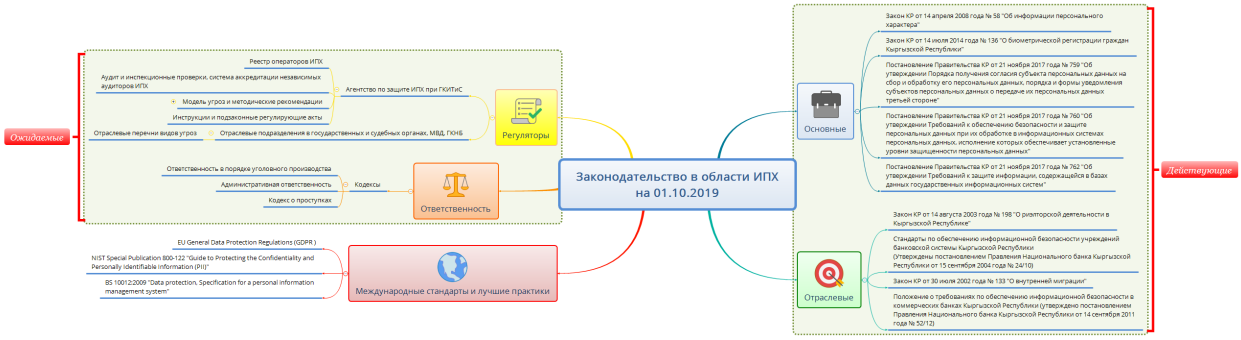
Выпущенная в 2017 году последняя редакция Закона КР «Об информации персонального характера» отличается своей зрелостью и полностью отвечает современным требованиям в области защиты персональных данных. Не секрет, что большинство аналогичных законов и инициатив, предпринимаемых в мире в области защиты персональных данных, являются различными интерпретациями единой сущности. Российские, американские или европейские законы в этой сфере буквально повторяют друг друга, описывая различными словами идентичные по сути требования и методики. Последняя редакция Закона КР «Об информации персонального характера» вобрала в себя весь накопленный мировой опыт в этой сфере и является своевременным ответом на возрастающие угрозы в области обеспечения безопасности персональных данных граждан.

Обеспечение безопасности персональных данных в Кыргызской республике базируется на следующей правовой базе:

1. Закон Кыргызской Республики от 14 апреля 2008 года № 58 «Об информации персонального характера»
2. Постановление Правительства Кыргызской Республики от 21 ноября 2017 года № 759 «Об утверждении Порядка получения согласия субъекта персональных данных на сбор и обработку его персональных данных, порядка и формы уведомления субъектов персональных данных о передаче их персональных данных третьей стороне»
3. Постановление Правительства Кыргызской Республики от 21 ноября 2017 года № 760 «Об утверждении Требований к обеспечению безопасности и защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищённости персональных данных»
4. Приказы, издаваемые уполномоченным государственным органом по персональным данным, об утверждении:
   - Типового перечня угроз безопасности персональных данных при обработке персональных данных в информационных системах, содержащий все виды и типы предполагаемых угроз;
   - Методики определения угроз безопасности в информационных системах персональных данных;
   - Формы перечня видов угроз.
5. Отраслевые перечни угроз безопасности персональных данных при обработке персональных данных в информационных системах, эксплуатируемых при осуществлении соответствующих видов деятельности, с учётом содержания персональных данных, характера и способов их обработки, разрабатываемые и

утверждаемые министерствами, государственными комитетами, административными ведомствами и иными государственными органами, и органами местного самоуправления в дополнение к приказам ГКИТиС.

На момент составления настоящих методических рекомендаций в нормативно-правовом поле Кыргызской республики в области обеспечения охраны персональных данных действовали исключительно нормативные акты, перечисленные в пп. 1—3. Ожидается, что пп. 4, 5 будут разработаны и утверждены после создания уполномоченного органа по персональным данным.




Несмотря на сложившуюся относительную нормативно-правовую несостоятельность, обеспечение безопасности персональных данных является важным компонентом общей системы обеспечения информационной безопасности как коммерческой организации, так и государственного учреждения.

Коммерческие организации обязаны защищать персональные данные своих работников, контрагентов и клиентов наряду с прочими мерами информационной безопасности — это прямо проистекает из предпринимаемого комплекса мер ИБ. Угроза утечки, потери или умышленной модификации персональных и иных данных могут напрямую повлиять на устойчивость бизнеса, а в случае с грубыми нарушениями — привести к его полной ликвидации. В условиях общемировой глобализации коммерческие компании Кыргызской республики могут столкнуться, — если уже не столкнулись — с необходимостью обеспечения безопасности персональных данных в соответствии с зарубежными требованиями. К примеру, GDPR — General Data Protection Regulations, аналог Закона КР «Об информации персонального характера» — устанавливает требования, подобные тем, что описаны в Законе и подзаконных актах и распространяется на все без исключения организации в любой стране мира, если они занимаются обработкой и хранением персональных данных граждан Евросоюза. При этом размер штрафных санкций в форме ответственности за их несоблюдение в случае нарушения прав граждан Евросоюза может достигать рекордных 20 млн. евро. Очевидно, что исполнение требований Закона КР — с небольшой адаптацией под евронормы — позволит местным компаниям свободно осуществлять свою

деятельность как на территории РФ и Евросоюза, так и в связи с необходимостью обработки и хранения персональных данных граждан этих стран.

Что же касается государственных органов, то защита персональных данных, особенно таких чувствительных, как национальность, история болезни или принадлежность тому или иному политическому, религиозному течению, является принципиальной основой обеспечения национальной безопасности страны.

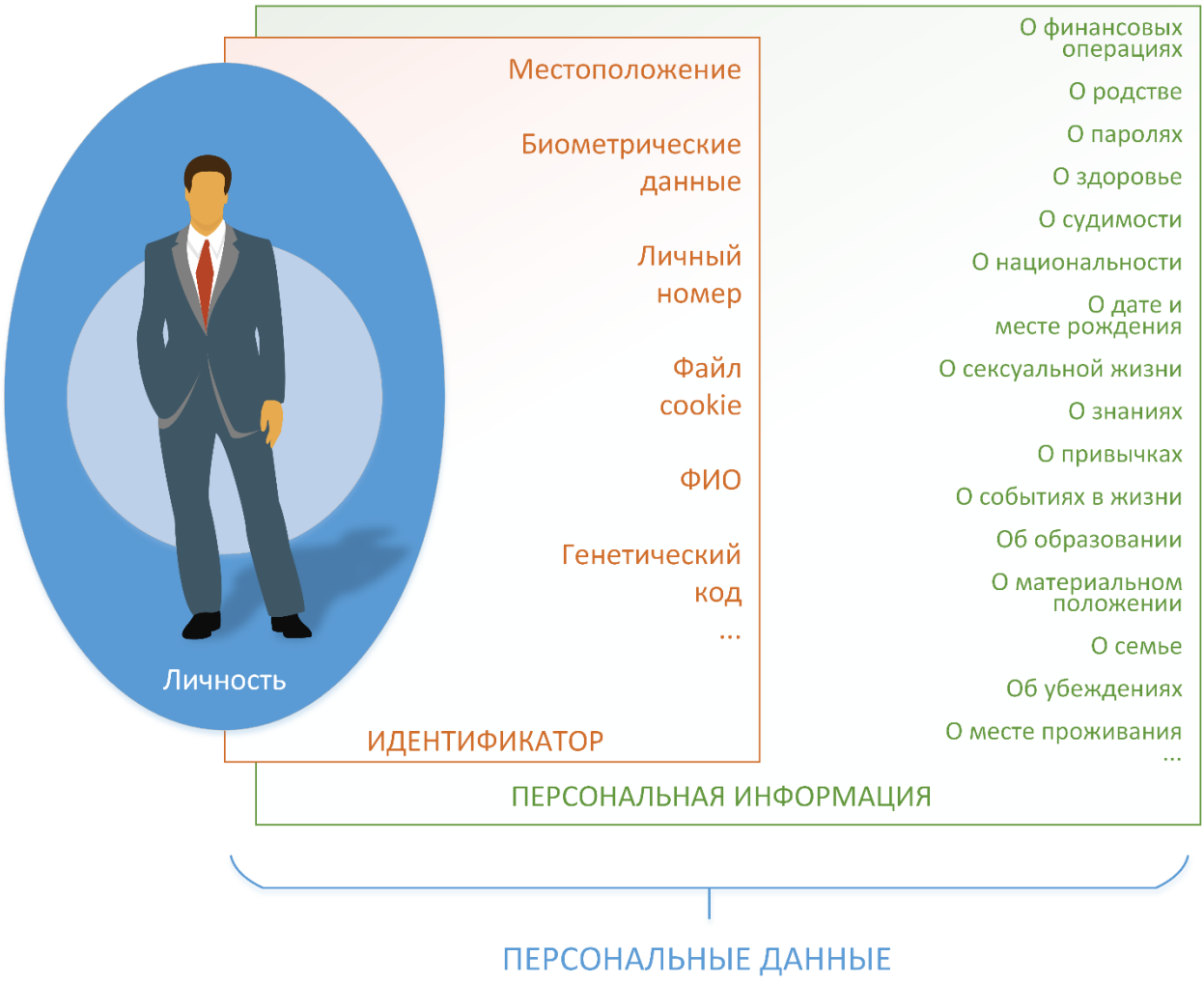
Учитывая общемировую тенденцию в сфере защиты персональных данных, коммерческие и государственные учреждения Кыргызской республики не могут оставаться вне этих процессов, чему в немалой степени способствуют уже принятые в правовом поле страны нормативно-правовые акты. В среднесрочном периоде ожидается создание полноценного государственного органа по защите персональных данных, внесение поправок об ответственности за нарушение Закона КР «Об ИПХ» в Административный или Уголовный кодекс, и доработка и утверждение подзаконных нормативно-правовых актов. После чего в стране будут созданы все необходимые условия для обеспечения правового режима охраны и защиты персональных данных.

Настоящие методические рекомендации составлены с учётом предстоящих нормативно-правовых новелл и должны послужить руководством к действию для широкого круга граждан, экспертов, ИТ-аудиторов, специалистов и руководителей, так или иначе вовлечённых в процесс обеспечения безопасности персональных данных.

# Терминология

Законодательством КР определяются следующие участники и характеристики процесса управления персональными данными:

**Информация персонального характера или ИПХ** — один идентификатор или свод (совокупность) двух и более идентификаторов персональных данных, позволяющие однозначно идентифицировать конкретного гражданина: ФИО, дата рождения, семейное положение, номер телефона, паспортные данные (персональный идентификационный номер (ПИН), номер, серия, дата и орган выдачи), «особые приметы» (кроме биометрических данных) и так далее. Список «и так далее» может быть бесконечно широким, если он в итоге позволяет однозначно идентифицировать конкретного гражданина.




**Специальные ИПХ** — особый вид персональных данных, указывающий на чувствительные характеристики ИПХ: национальность; сексуальная ориентация; биометрические данные; философские, религиозные или политические убеждения; диагноз, медицинские сведения или история болезни. Такие данные нельзя собирать

исключительно с целью выявления этих факторов за исключением случаев, когда Субъект дал информированное согласие для этого или когда получение согласия невозможно, но возникла неотложная необходимость обеспечения безопасности соответствующей группы лиц.

**Субъект ИПХ** — носитель и единственный законный владелец данных, лично предоставляющий временные права Держателю (обладателю) массива персональных данных на хранение, обработку или передачу третьим лицам собственных персональных данных.

**Держатель (обладатель) массива персональных данных (далее – держатель)** - органы государственной власти, органы местного самоуправления и юридические лица, на которые возложены полномочия определять цели, категории персональных данных и контролировать сбор, хранение, обработку и использование персональных данных в соответствии с настоящим Законом.

**Уполномоченный государственный орган по персональным данным (далее - уполномоченный государственный орган)** - государственный орган, уполномоченный Правительством Кыргызской Республики осуществлять функции и полномочия по обеспечению соответствия обработки персональных данных требованиям настоящего Закона, защите прав субъектов персональных данных (субъектов), регистрации держателей (обладателей) массива персональных данных, ведению Реестра держателей массивов персональных данных, другие задачи, функции и полномочия, предусмотренные настоящим Законом.

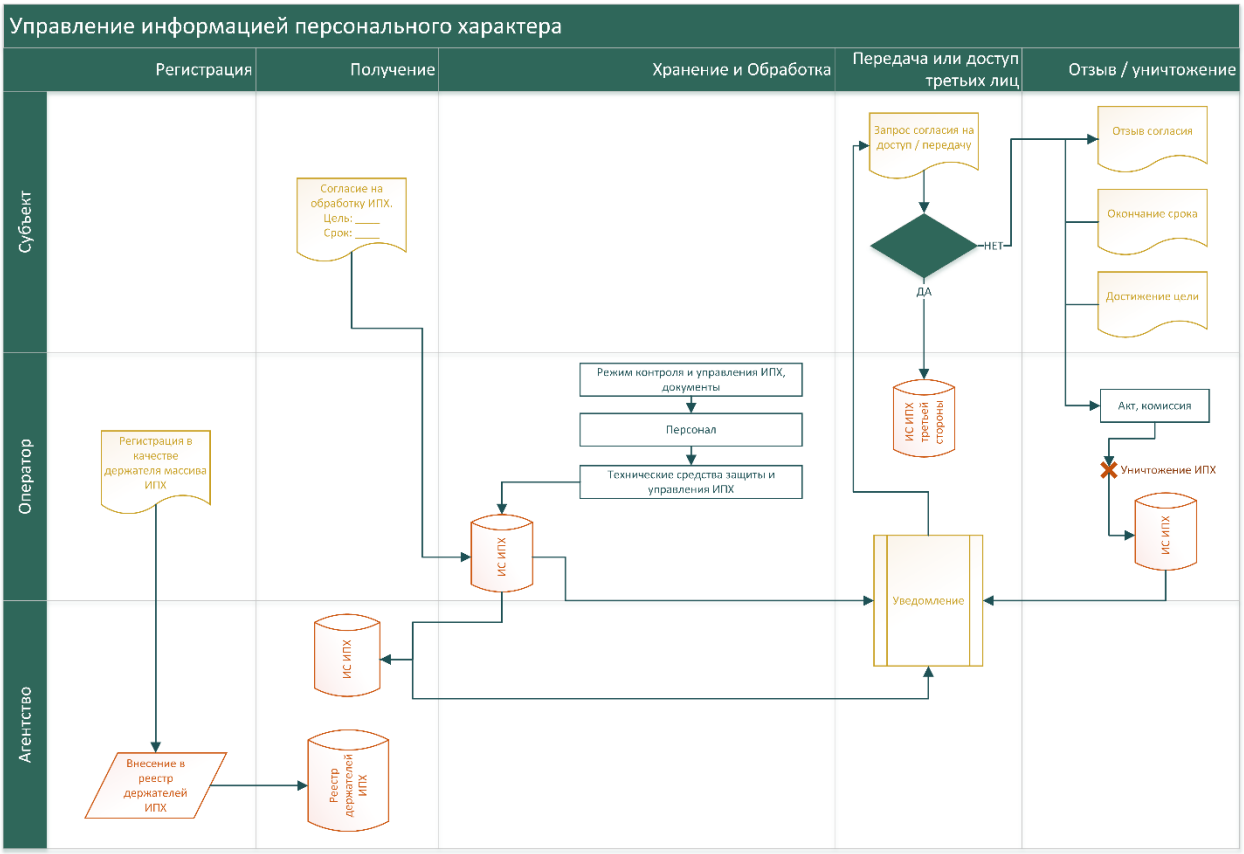
**Управление ИПХ** — процесс получения, хранения, обработки, передачи и уничтожения персональных данных, осуществляемых Держателем (обладателем) массива персональных данных в течение определённого срока и исключительно по согласию Субъекта на осуществление конкретных действий или достижения конкретной цели.

**Согласие Субъекта ИПХ** — явно выраженное, документально подтверждаемое согласие Субъекта ИПХ о передачи прав по Управлению ИПХ Держателю массива персональных данных на конкретный срок и для достижения конкретной цели.

**Отзыв согласия** — явно выраженное, документально подтверждаемое требование Субъекта ИПХ об отзыве ранее выданных прав на Управление ИПХ, от которого Держатель массива персональных данных не может уклониться, проигнорировать его или пренебречь им. Отзыв согласия наступает также автоматически по достижению ранее указанных срока или цели, установленных Субъекту ИПХ для Управления ИПХ.

**Информационная система ИПХ (ИС ИПХ)** — комплекс программно-аппаратных средств, применяемых Держателем массива персональных данных или уполномоченным государственным органом по персональным данным для Управления ИПХ в соответствии с требованиями.

## Процесс управления персональными данными




Таким образом, общий процесс управления ИПХ выглядит следующим образом:

1. Учреждение, занимающееся сбором и обработкой персональных данных, должно пройти в уполномоченном государственном органе по персональным данным процедуру регистрации в качестве держателя (обладателя) массива персональных данных. Однако, для получения этого статуса учреждение должно соответствовать требованиям Закона КР и подзаконных актов, внедрив необходимые организационно-технические меры по Управлению и Защите ИПХ.
2. После внесения в реестр и получения статуса держателя (обладателя) персональных данных, учреждение должно организовать прозрачный процесс получения информированного согласия от Субъекта.
3. Организация должна обеспечить информирование уполномоченного государственного органа по персональным данным и получение согласия Субъекта о любых случаях внесения изменений в ИПХ, о любых попытках доступа

к ИПХ, о необходимости передачи ИПХ для обработки третьему Оператору, а также об уничтожении ИПХ в связи с требованием Субъекта, истечением периода сбора (хранения) ИПХ или достижением ранее определённых целей.

## Самооценка и регистрация Держателя (обладателя) массива персональных данных

Прежде чем приступить к обработке персональных данных, Держатель (обладатель) массива персональных данных должен пройти процедуру самооценки для определения требуемого уровня защищённости как держателя (обладателя) массива персональных. Затем надлежит выполнить требования уполномоченного государственного органа по персональным данным и пройти процедуру регистрации в качестве держателя (обладателя) массива персональных данных. Отказ от регистрации или игнорирование требований Закона влекут за собой административную или уголовную ответственность.

Подзаконным актом, определяющим минимальный уровень в обеспечении защиты персональных данных, является Постановление Правительства Кыргызской Республики от 21 ноября 2017 года № 760 «Об утверждении Требований к обеспечению безопасности и защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищённости персональных данных». В рамках этого постановления определены четыре уровня безопасности, применимые к действующим и будущим Держателям (обладателям) массива персональных данных.

Помимо уровней безопасности, Постановлением также определено, что Держатель (обладатель) массива персональных данных, исходя из конкретных условий работы с персональными данными, ценности защищаемой информации и стоимости мер по её защите, учитывая уровень собственного технического развития, должен разработать и утвердить собственный перечень угроз безопасности персональных данных по особой форме, утверждённый уполномоченным государственным органом по персональным данным. К моменту разработки Методических рекомендаций эта форма, как и базовый перечень угроз безопасности, находились в режиме согласования и утверждения, поэтому настоящие Методические рекомендации будут дополнены после утверждения соответствующих нормативов.

Тем не менее, модель угроз является отправной точкой при определении уровня защищённости организации, так как самооценка производится по каждому виду угроз отдельно согласно прилагаемой Таблице.

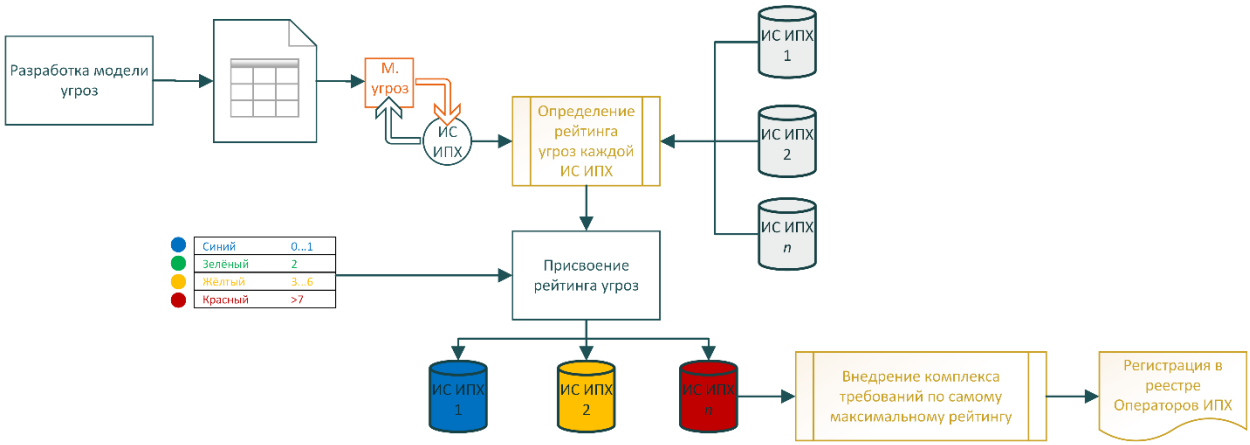
| № | Критерий | Оценка | Пояснение |
|---|---|---|---|
| *1* | Актуальность угрозы безопасности персональных данных | 0 | Угроза неактуальна |
| | | 1 | Угроза актуальна |
| *2* | Возможное причинение вреда субъекту персональных данных, который может быть причинён в случае реализации угрозы | 0 | Не влечёт причинения убытков и морального вреда субъекту персональных данных |
| | | 1 | Незначительный вред, легко компенсируемый держателем<br>Незначительные затраты — менее 1000 расчётных показателей на ликвидацию/компенсацию последствий за причинённые убытки и моральный вред |
| | | 2 | Значительный вред, который может быть компенсирован оператором<br>Значительные затраты — более 1000 расчётных показателей, на ликвидацию/компенсацию последствий за прочиненные убытки и моральный вред |
| | | 3 | Критический вред, не может быть компенсирован<br>Причинение убытков и морального вреда, которые не могут компенсированы |
| *3* | Объем обрабатываемых персональных данных, которые подвержены данной угрозе | 1 | Незначительный объем, до 10000 субъектов ИПХ |
| | | 2 | Значительный объем, от 10000 до 100000 субъектов ИПХ |
| | | 3 | Критический объем, свыше 100000 субъектов ИПХ |
| *4* | Содержание обрабатываемых персональных данных, которые подвержены данной угрозе | 1 | ИПХ, не относящиеся к специальным категориям |
| | | 2 | Специальные категории ИПХ, а также биометрические данные |
| *5* | Продолжительность деятельности, к которой применима угроза (срок обработки или хранения ИПХ) | 0 | Краткосрочная обработка данных до двух недель |
| | | 1 | Долгосрочная, свыше двух недель |

Общий рейтинг угрозы безопасности определяется путём элементарного арифметического произведения (умножения) оценочных баллов каждого из критериев. Рейтинг присваивается каждой информационной системе или их группе следующим образом:

- Синий — наличие угроз с рейтингом не более 1 балла;
- Зелёный — наличие угроз с рейтингом 2 балла;
- Жёлтый — наличие угроз с рейтингом от 3 до 6 баллов включительно;
- Красный — наличие угроз с рейтингом 7 и более баллов.

| | |
|---|---|
| Синий | 0…1 |
| Зелёный | 2 |
| Жёлтый | 3…6 |
| Красный | ≥7 |

Для каждого из уровней определены Требования к уровню защищённости организационно-технического окружения информационных систем в зависимости от присвоенного рейтинга. Ожидается, что после применения каждого вида угроз из модели к каждой информационной системе Держатель (обладатель) массива персональных данных сможет определить свой уровень угроз безопасности, после чего проведёт комплекс мероприятий и внедрение необходимых организационных и технических мер защиты на уровне не ниже, чем это определено Требованиями, и лишь после этого сможет приступить к процедуре регистрации в качестве держателя (обладателя) массива персональных данных.



## Пример определения рейтинга безопасности

Для иллюстрирования расчёта рейтинга угроз безопасности и определения уровня безопасности возьмём следующий пример.

Информационная система по обработке информации персонального характера в ОсОО «Мүйүздөр жана туяктар» хранит в себе порядка 80 тыс. единиц ИПХ следующего вида:

| Фамилия | Имя | Отчество | Дата рождения | Паспорт Серия | Паспорт № | ПИН | Пол |
|---|---|---|---|---|---|---|---|

Компьютер, на котором стоит ИС ИПХ, стоит в дальнем углу общего коридора, не имеет установленного пароля доступа и не обеспечен системой резервного копирования данных.

В отсутствие утверждённых Модели угроз и Методики, можно воспользоваться облегчённой экспертной оценкой. Исходя из вводных данных становится очевидным, что угроза безопасности является актуальной, так как к компьютеру имеется свободный доступа и нет пароля, а ущерб — значительным в силу того, что компании для ликвидации последствий в случае утери данных придётся оплатить стоимость восстановления каждой из 80 тыс. записей вручную из-за отсутствия резервного копирования. Компания управляет персональными данными, которые не относятся к специальным категориям. При этом сроки обработки персональных данных, а также в течение которых угроза безопасности будет сохранять свою актуальность, очевидно являются долгосрочными.

В приведённом выше примере произведена оценка рейтинга угрозы безопасности исходя из:

- × актуальности угрозы безопасности — 1 балл.
- × объёма ИПХ в размере 80 тыс. единиц — 2 балла.
- × долгосрочного срока обработки ИПХ — 1 балл.
- × вероятного ущерба в размере свыше 100 тыс. сом — 2 балла.
- × хранения и обработки обычных ИПХ — 1 балл.

Таким образом: $1 \times 2 \times 1 \times 2 \times 1 = 4$, что соответствует «Жёлтому» уровню угрозы безопасности.

У компании «Мүйүздөр жана туяктар» определён Жёлтый рейтинг угрозы безопасности в отношении информационной системы, обрабатывающей персональные данные.

Для того, чтобы стать легитимным Держателем массива персональных данных, руководству компании надлежит выполнить необходимые требования, присущие «Жёлтому» уровню. Вместе с тем, выполняя все требования, компания сможет перейти на «Синий» уровень за счёт снижения размера вероятного ущерба до суммы ниже 100 тыс. сом, что может произойти сразу же после внедрения системы резервного копирования. Таким образом, при регистрации компании в реестре уполномоченного государственного органа по персональным данным информационная система будет рассматриваться с «Синим» уровнем угроз безопасности.

## Требования к уровню защищённости

| № | Требования | | | |
|---|---|---|---|---|
| | 0…1 | 2 | 3…6 | ≥ 7 |
| 1 | Разработка политики по управлению ИПХ | Разработка политики по управлению ИПХ | Разработка политики по управлению ИПХ | Разработка политики по управлению ИПХ |
| 2 | Доведение до сотрудников и контрагентов содержания политики | Доведение до сотрудников и контрагентов содержания политики | Доведение до сотрудников и контрагентов содержания политики | Доведение до сотрудников и контрагентов содержания политики |
| 3 | Назначение ответственных лиц за безопасность ИПХ | Назначение ответственных лиц за безопасность ИПХ | Назначение ответственных лиц за безопасность ИПХ | Назначение ответственных лиц за безопасность ИПХ |
| 4 | Включение в трудовые договора, должностные инструкций обязанностей в отношении ИПХ | Включение в трудовые договора, должностные инструкций обязанностей в отношении ИПХ | Включение в трудовые договора, должностные инструкций обязанностей в отношении ИПХ | Включение в трудовые договора, должностные инструкций обязанностей в отношении ИПХ |
| 5 | Осуществление контроля соответствия Управления ИПХ | Осуществление контроля соответствия Управления ИПХ | Осуществление контроля соответствия Управления ИПХ | Осуществление контроля соответствия Управления ИПХ |
| 6 | Ведение журнала учёта носителей ИПХ и списка лиц с доступом к ИПХ | Ведение журнала учёта носителей ИПХ и списка лиц с доступом к ИПХ | Ведение журнала учёта носителей ИПХ и списка лиц с доступом к ИПХ | Ведение журнала учёта носителей ИПХ и списка лиц с доступом к ИПХ |
| 7 | Логгирование действий при работе с ИПХ: лицо, операция, дата, время. | Логгирование действий при работе с ИПХ: лицо, операция, дата, время. | Логгирование действий при работе с ИПХ: лицо, операция, дата, время. | Логгирование действий при работе с ИПХ: лицо, операция, дата, время. |
| 8 | Ежедневное резервирование | Ежедневное резервирование | Ежедневное резервирование | Ежедневное резервирование |
| 9 | | Проектирование ИС с учётом требований ИПХ | Проектирование ИС с учётом требований ИПХ | Проектирование ИС с учётом требований ИПХ |
| 10 | | Аудит и оценка эффективности ИС до ввода в эксплуатацию или перед глобальным обновлением | Аудит и оценка эффективности ИС до ввода в эксплуатацию или перед глобальным обновлением | Аудит и оценка эффективности ИС до ввода в эксплуатацию или перед глобальным обновлением |
| 11 | | Применение средств криптографической защиты информации | Применение средств криптографической защиты информации | Применение средств криптографической защиты информации |
| 12 | | | Централизованное управление системой защиты ИПХ, вплоть до выделенного Департамента | Централизованное управление системой защиты ИПХ, вплоть до выделенного Департамента |
| 13 | | | Контроль и защита физического доступа в помещения обработки ИПХ | Контроль и защита физического доступа в помещения обработки ИПХ |
| 14 | | | Нефальсифицируемое логгирование всех событий с ИПХ | Нефальсифицируемое логгирование всех событий с ИПХ |
| 15 | | | Обеспечение высокой доступности ИС ИПХ в режиме реального времени | Обеспечение высокой доступности ИС ИПХ в режиме реального времени |
| 16 | | | Наличие системы обнаружения и предотвращения НСД | Наличие системы обнаружения и предотвращения НСД |
| 17 | | | | Использование только защищённых каналов связи |
| 18 | | | | Защита ИПХ от утечек по техническим каналам |
| 19 | | | | Применение сертифицированных С(К)ЗИ |
| 20 | | | | Ежегодный аудит ИС ИПХ |

Уровни защищённости персональных данных при их обработке в информационных системах ИПХ должны обеспечиваться выполнением требований, которые приведены в Таблице.

| R | № | ТРЕБОВАНИЕ | КОММЕНТАРИЙ |
|---|---|---|---|
| ● ● ● ● | 1 | Принятие документа, определяющего политику держателя (обладателя) массива персональных данных в отношении обработки персональных данных; | *Политика должна описывать конкретные сроки и цели сбора, обработки и хранения ИПХ, отражать приверженность руководства целям защиты ИПХ, определять нормы ответственности за несоблюдение требований политики и законов, декларировать строгое соблюдение требований в области защиты и информирования Субъекта о каждом случае изменения или доступа к экземпляру ИПХ; в Политике также должны отражаться все возможные случаи, когда Держатель должен и не должен передавать персональные данные третьим лицам, предоставлять им доступ.* |
| ● ● ● ● | 2 | Доведение содержания Политики до работников и контрагентов держателя (обладателя) массива персональных данных; | *Политика ИПХ не является секретным или сугубо внутренним документом — это своеобразный декларативный договор между Субъектом и Держателем массива персональных данных о совместном использовании персональных данных. Текст политики должен быть общедоступным, вплоть до публикации его на веб-сайте.* |
| ● ● ● ● | 3 | Назначение 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 других подзаконных актов; | *В каждой организации должно быть определено ответственное лицо, отвечающее за реализацию пунктов и положений Политики ИПХ. Офицер по защите персональных данных должен быть компетентным как с точки зрения знания нормативных актов, так и их технического или организационного применения. Это же лицо осуществляет контроль за соблюдением Политики в пределах всей организации и даёт рекомендации по внесению изменений в процессы, техническое оснащение или документацию. Допускается совмещение должности офицера по защите ИПХ с должностью офицера по информационной безопасности, но во избежание конфликта интересов это лицо не может замещать должность ИТ-специалиста (системного администратора), отвечающего за эксплуатацию ИС ИПХ.* |
| ● ● ● ● | 4 | Осуществление внутреннего контроля соответствия обработки персональных данных требованиям Закона Кыргызской Республики «Об информации персонального характера», и подчинённых подзаконных актов, иных документов, принятых по вопросам обработки персональных данных; | *Декларация Политики и внедрение соответствующих мер защиты без регулярного подтверждения, что все процессы работают и они работают должным образом, отрицательно сказывается на эффективности предпринятых мер защиты ИПХ. Контроль должен осуществляться на регулярной основе, ответственным за это лицом, с отчётом высшему руководству и с обязательным сохранением следов проверок.* |

| R | № | ТРЕБОВАНИЕ | КОММЕНТАРИЙ |
|---|---|---|---|
| | 5 | Включение 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; | *Каждый сотрудник должен осознавать важность обеспечения защиты ИПХ, что может быть достигнуто за счёт явного информирования сотрудников, инструктажей и внесением соответствующих положений в трудовые договора. Важно внести пункт о сообразной дисциплинарной и прочей, вплоть до уголовной, ответственности за несоблюдение внутренних и внешних требований о безопасности ИПХ.* |
| | 6 | Ведение (на бумажном носителе или в электронном виде) журнала учёта машинных носителей персональных данных и списка лиц, в чьи должностные обязанности входит доступ к персональным данным; | *Это требование является частным случаем генерального процесса управления информационными активами. Как и в случае с общим подходом, обязывающим ведение актуального реестра всех значимых информационных систем и активов, для обеспечения защиты ИПХ компании необходимо иметь представление, в каком количестве (количество копий, экземпляров), где и как хранятся персональные данные, кто имеет к ним доступ.* |
| | 7 | При каждом вводе персональных данных в систему обработки данных, а также при изменении или уничтожении таких данных - указание лица, осуществившего ввод (изменение, уничтожение) таких данных, даты и времени совершения операции; | *Требование к дизайну информационной системы. В большинстве случаев, исполнение этого требования реализовано по умолчанию — большинство современных и даже устаревших систем промышленного, корпоративного назначения обладают необходимым функционалом, фиксирующим доступ к тем или иным данным, включая персональные. В противном случае, если в используемой информационной системе фиксация логина, типа действий, даты и времени при изменении (вводе, удалении) данных не реализовано, то применение такой системы для обработки и хранения персональных данных должен быть исключено.* |
| | 8 | Создание не реже одного раза в сутки резервной копии актуальных персональных данных, обрабатываемых в информационной системе персональных данных; | *Создание резервных копий любых типов данных, не только персональных, является ярким примером лучших мировых практик, следование которым позволит достичь надлежащего уровня информационной безопасности, непрерывности деятельности и оперативного восстановления операций в случае их возможного прерывания. При организации процесса резервного копирования важно предусмотреть защиту систем хранения данных резервных копий, определить расписание, обозначить меры контроля успешности (или неуспешности) выполнения резервных копий в автоматизированном режиме, а также предусмотреть процедуры регулярного, не реже раза в месяц, тестирования резервных копий на предмет их консистентности и применимости.* |

| R | № | ТРЕБОВАНИЕ | КОММЕНТАРИЙ |
|---|---|---|---|
| ● ● ● | 9 | Проектирование информационной системы и мер по её развитию с учётом характера обрабатываемых в ней персональных данных и необходимости их защиты; | *Иначе это требование в мировой практике защиты персональных данных называется «Data Privacy by Design». Смысл этих требований заключается в том, чтобы применяемые информационные системы изначально были разработаны с учётом требований, обеспечивающих реализацию комплекса мер по защите персональных данных. В частном случае, это может потребовать глубокой переработки существующей информационной системы либо полного замещения на новую информационную систему, изначально отвечающую действующим требованиям. Благодаря существующей принципиальной схожести между Законом КР №58 и аналогичными европейскими (GDPR), российскими (152-ФЗ) и американскими (Privacy Act of 1974, Privacy Protection Act of 198, SP 800-122) законодательными инициативами, разрабатываемые в настоящее время промышленные зарубежные информационные системы заранее соответствуют самым жёстким требованиям к порядку обработки и хранения персональных данных.* |
| ● ● ● | 10 | Оценка 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; | *Требование обязывает Держателя массива персональных данных уведомлять уполномоченный государственный орган по персональным данным о происходящих изменениях с ИС ИПХ, после чего будет приниматься решение о необходимости проведения дополнительной очной или заочной (по документам разработчика) проверке о соответствии ИС настоящим требованиям.* |

| R | № | ТРЕБОВАНИЕ | КОММЕНТАРИЙ |
|---|---|---|---|
| ● ● ● | 11 | Применение 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; | *Применение алгоритмов шифрования с одной стороны полностью исключает возможности для компрометации персональных данных при несанкционированном доступе, с другой стороны накладывает существенные ограничения на порядок доступа к данным, находящимся в «горячем» доступе при работе в режиме реального времени. Разумеется, резервные копии и прочие «холодные» экземпляры массивов персональных данных надлежит шифровать в любом случае, вне зависимости от предъявляемых требований. При выборе решения для шифрования данных «горячего» доступа необходимо проводить комплексную оценку эффективности с учётом сильных и слабых сторон рассматриваемого решения. Например, шифрование с использованием так называемого «мастер-ключа» обладает существенными недостатками, когда вся информация в базе данных зашифрована алгоритмом любого уровня криптостойкости, но с использованием одного ключа. Существуют реализации, когда мастер-ключ вводится ответственным сотрудником каждый раз, когда информационная система запускается, но после этого все данные де-факто будут доступными в расшифрованном виде. Такой вариант применения шифрования считается недопустимым. В некоторых других реализациях такой же модели шифрования, мастер-ключ доступен практически любому сотруднику для исполнения своих должностных обязанностей, что также не отвечает требованиям обеспечения защиты ИПХ. При недостаточном обеспечении безопасности мастер-ключом может легко завладеть и злоумышленник и получить беспрепятственный к доступ к данным.* |
| ● ● | 12 | Централизованное управление системой защиты персональных данных, в том числе, путём создания структурного подразделения, ответственного за реализацию настоящих Требований; | *Этим требованием обеспечивается создание дополнительного контура защиты систем и процессов, так или иначе вовлечённых в процессы управления ИПХ. При таком подходе разумнее всего предусмотреть редизайн всех информационных систем таким образом, чтобы защищаемые персональные данные были выделены в качестве отдельной охраняемой (шифруемой) сущности, доступ к которым со стороны прикладных информационных систем осуществлялся опосредованно, через выделенный jump-сервер, с логгированием всех событий. При невозможности реализации такого способа обеспечения контролируемого доступа к данным, выделенный департамент по защите ИПХ должен обеспечить не менее эффективный контроль за доступом к персональным данным за счёт применения соответствующих административных, организационных и технических мер. Ожидается, что вертикаль подчинения такого департамента не будет приводить к конфликту интересов, когда его сотрудники будут поставлены перед фактом контролировать самих себя.* |

| R | № | ТРЕБОВАНИЕ | КОММЕНТАРИЙ |
|---|---|---|---|
| 🟡 🔴 | 13 | Установление системы контроля помещений, в которых установлена информационная система, позволяющей ограничить физический доступ к техническим средствам информационной системы только теми лицами, которым предоставлены соответствующие полномочия; | *Контроль физической безопасности является базовым требованием общей системы обеспечения информационной безопасности и по умолчанию реализуется в качестве одного из первых пунктов обеспечения ИБ на предприятии. Реализация этого пункта заключается в установлении дополнительных мер контроля при доступе к серверным помещениям: видеонаблюдение, автоматизированная фиксация входа за счёт установки электронных датчиков движения, открытия дверей и электронно-механических замков в рамках общей или частной системы контроля и управления доступом. Хорошей практикой является журналирование событий доступа в защищаемое помещение — ведение реестра записей о причинах посещений, — и регулярный контроль, что сотрудники не пренебрегают этой процедурой.* |
| 🟡 🔴 | 14 | Ведение автоматического электронного журнала (лога), фиксирующего все операции с персональными данными, с обеспечением невозможности внесения изменений в данный журнал задним числом; | *Реализация этого требования несмотря на кажущуюся сложность является вполне достижимой штатными средствами и инструментами. По усмотрению технических специалистов может быть выбран один из протоколов логгирования (syslogd, rsyslog) с обязательным сохранение реплики лог-записи на выделенный защищаемый лог-сервер, либо это может быть on-line репликация табличного пространства в базе данных, отвечающего за ведение журнала доступа, также на выделенный лог-сервер. Таким образом можно обеспечить нефальсифицируемую площадку с дубликатами логов всех произведённых действий со всех информационных систем, находящуюся под управлением офицеров по защите ИПХ.* |
| 🟡 🔴 | 15 | Обеспечение резервирования и высокой доступности информационной системы хранения и обработки персональных данных в реальном времени и автоматического электронного журнала, предусмотренного пунктом 14; | *Особо критичные информационные онлайн-системы надлежит эксплуатировать по модели кластера высокой доступности (HA-cluster), ноды которого должны быть географически отдалены друг от друга и обеспечены репликацией всех данных в режиме реального времени. Только такой способ на текущий момент гарантирует высокую доступность критически-важных данных и обеспечивает их сохранность при наступлении техно-, антропогенных катастроф практически любой разрушающей силы.* |
| 🟡 🔴 | 16 | Наличие автоматической системы выявления и пресечения несанкционированного доступа к персональным данным, а также их случайного уничтожения или изменения; | *Такие системы могут быть встроены в качестве дополнительного функционала прикладной информационной системы, либо воспроизведены в виде связного комплекса внешних организационных и технических решений, таких как включая системы мониторинга и резервирования логов, либо же могут быть отдельно-стоящими системами класса DLP (Data Leak Prevention, система предотвращения утечек данных), IDS/IPS (Intrusion Detection/Prevention System, система распознавания/предотвращения вторжений) и других.* |
| 🔴 | 17 | Использование только защищённых каналов связи при передаче персональных данных и (или) доступе к ним; | *Для исполнения этого требования необходимо обеспечить связность «клиент—сервер» или «сервер—сервер» с использованием одного из решений по организации защищённых туннелей передачи данных типа VPN L2 с шифрованием или VPN L3.* |

| R | № | ТРЕБОВАНИЕ | КОММЕНТАРИЙ |
|---|---|---|---|
| ● | 18 | Защита персональных данных от утечек по техническим каналам; | *Снятие информации с технического канала связи — съём специальными техническими средствами характеристик электромагнитных или других физических полей, возникающих при передаче информации по сетям связи, включая слаботочные Ethernet-соединения и оптические каналы. Для исполнения этого требования надлежит исключить передачу данных ИПХ в незашифрованном виде по любым каналам связи, даже в пределах защищаемого периметра обработки ИПХ: по сетям связи Ethernet (U(S)TP, Optical Fiber), по телефону (в т. ч. голосом), радиоканалу (Wi-Fi, GSM), факсом или с использованием материальных носителей (на бумаге, флэшках, съёмных магнитных, лазерных, твердотельных дисках).* |
| ● | 19 | Применение 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; | *Исполнение этого требования возможно при наличии утверждённого реестра проверенных и рекомендуемых к использованию моделей средств защиты информации.* |
| ● | 20 | Регулярный (не менее 1 раза в год) аудит 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. | *Как и в случае регулярным контролем для «сине-зелёных» систем, проведение регулярного независимого внешнего аудита информационных систем с «красным» рейтингом угроз безопасности позволяет получить известную степень уверенности и независимое подтверждение тому, что все необходимые требования соблюдены, сопутствующие процессы выполняются регулярно, а контрольные меры являются эффективными.* |

# Согласие Субъекта ИПХ

Процесс управления ИПХ всегда начинается с получения согласия гражданина как субъекта персональных данных. Согласие на обработку персональных данных выражается гражданином лично или через доверенное лицо без принуждения, осознанно и в форме, позволяющей подтвердить факт его получения — как правило, в письменной форме. Согласие в форме электронного документа может быть принято в качестве нормативного и легитимного только в случае, если оно подписано электронной подписью, как это определяется законодательством КР. Иные формы получения согласия, например, в виде «галочки» напротив пункта веб-сайта «Я согласен с обработкой своих персональных данных», в законодательстве не определены и являются нелегитимными.

Без явно выраженного, документально подтверждаемого согласия гражданина дальнейшее хранение и обработка персональных данных запрещается.

**Если учреждение к моменту вступления Закона об ИПХ в силу уже накопило определённый свод (массив) персональных данных, оно должно провести соответствующую работу по приведению внутренних норм и техсредств в соответствие с требуемым режимом управления ИПХ, в том числе и с помощью настоящих методических рекомендаций.**

Порядок получения и форма согласия Субъекта ИПХ регулируется Постановлением Правительства Кыргызской Республики от 21 ноября 2017 года № 759 «Об утверждении Порядка получения согласия субъекта персональных данных на сбор и обработку его персональных данных, порядка и формы уведомления субъектов персональных данных о передаче их персональных данных третьей стороне».

## Перечень типовых идентификаторов ИПХ

В соответствии с требованиями, Держатель массива персональных данных обязан определить каждый идентификатор персональных данных отдельно и, в случае необходимости, каждый раз запрашивать согласие Субъекта на обработку нового идентификатора ИПХ. Среди наиболее распространённых идентификаторов можно отметить следующие:

- фамилия, имя и отчество (прежние фамилия, имя, отчество, дата, место и причина изменения (в случае изменения);
- дата и место рождения;
- сведения о гражданстве (в том числе предыдущее гражданство, иные гражданства);
- сведение о семейном составе, семейном положении;
- сведения об образовании (наименование и год окончания образовательной организации, наименование и реквизиты документа об образовании,

квалификация, направление подготовки или специальность по документу об образовании);

- сведения о наличии учёной степени;
- информация о владении иностранными языками, уровне владения;
- спортивное звание, спортивный разряд;
- адрес места жительства (места пребывания);
- номер контактного телефона или сведения о других способах связи;
- вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;
- идентификационный номер налогоплательщика;
- персональный идентификационный номер;
- номер страхового свидетельства обязательного пенсионного страхования;
- реквизиты полиса обязательного медицинского страхования;
- отношение к воинской обязанности, сведения по воинскому учёту (для граждан, пребывающих в запасе, и лиц, подлежащих призыву на военную службу);
- семейное положение, состав семьи;
- сведения о трудовой деятельности (включая военную службу, работу по совместительству, предпринимательскую деятельность и т.п.);
- государственные награды, иные награды и знаки отличия (кем награждён и когда);
- информация о наличии либо отсутствии судимости;
- сведения о доходах, расходах, об имуществе и обязательствах имущественного характера;
- личная фотография.

## Форма получения согласия на обработку ИПХ

Типовая форма получения согласия для государственных (муниципальных) органов Кыргызской республики выглядит следующим образом:

**Согласие субъекта персональных данных на сбор и обработку его персональных данных**

г. Бишкек 25 декабря 2019 г.

Я, Козубеков Эрмек Бактыбекович
(фамилия, имя, отчество)

проживающий по адресу: г. Бишкек, ул. Ю. Абдрахманова, д. 1 «а», кв. 13

Документ, удостоверяющий личность: ID-паспорт серия AN № 1234567
(вид документа)

выдан 15/10/2012 МКК 50-55
(дата выдачи) (кем выдан)

свободно, осознанно, по своей воле даю согласие ЗАГС Октябрьского р-на ДРНАГС ГРС при ПКР
(наименование, адрес собственника или владельца информационной системы, ФИО обработчика)

- на обработку (любая операция или набор операций, выполняемых независимо от способов держателем (обладателем) персональных данных либо по его поручению, автоматическими средствами или без таковых, в целях сбора, записи, хранения, актуализации, группировки, блокирования, стирания и разрушения персональных данных),

а также на:

- передачу персональных данных (предоставление держателем (обладателем) персональных данных третьим лицам в соответствии с Законом Кыргызской Республики "Об информации персонального характера" и международными договорами;
- с трансграничную передачу персональных данных (передача держателем (обладателем) персональных данных держателям, находящимся под юрисдикцией других государств) следующих персональных данных:

1. Фамилия, Имя и Отчество
2. Дата и место рождения
3. Сведения о гражданстве
4. Номер контактного телефона
5. Номер паспорта
6. Персональный идентификационный номер
7. Личная фотография
8. Семейное положение и состав семьи

Вышеуказанные персональные данные предоставляю для обработки в целях предоставления мне государственной (муниципальной) услуги Регистрация рождения
(указать наименование услуги)

Я ознакомлен(а) с тем, что:

1) согласие на обработку персональных данных действует с даты подписания настоящего согласия в течение всего срока предоставления мне государственной (муниципальной) услуги и хранения данных об оказанной услуге в соответствии с законодательством Кыргызской Республики;

2) согласие на обработку персональных данных может быть отозвано на основании письменного заявления в произвольной форме;

3) в случае отзыва согласия на обработку персональных данных обработка моих персональных данных полностью или частично может быть продолжена в соответствии со статьями 5 и 15 Закона Кыргызской Республики «Об информации персонального характера».

Дата начала обработки персональных данных: 25 декабря 2019 года
(число, месяц, год)

"25" декабря 2019г.

ЭБКозубеков
Подпись

Козубеков Э. Б.
ФИО

При разработке собственной формы получения согласия необходимо обязательно отразить следующие важные положения:

- правовые основания обработки персональных данных;
- цели обработки персональных данных;
- способы обработки персональных данных;
- наименование и место нахождения держателя (обладателя) массива персональных данных,
- сведения о лицах (за исключением работников держателя (обладателя), которые имеют доступ к персональным данным или которым могут быть переданы

персональные данные на основании договора с держателем (обладателем) массива персональных данных или на основании закона;

- исчерпывающий список обрабатываемых персональных данных, относящиеся к соответствующему субъекту персональных данных;
- источник получения персональных данных, если они получены не от Субъекта;
- сроки обработки персональных данных;
- сроки хранения персональных данных после окончания срока обработки (окончания предоставления услуг, прекращения договора);
- информацию об осуществлённой или о предполагаемой передаче персональных данных третьим лицам, включая факты трансграничной передачи.

# Внедрение режима обработки персональных данных

Важно отметить, что наличие утверждённых формализованных документов, учитывающих необходимые аспекты управления информацией персонального характера, необходимо для того, чтобы донести до всех задействованных сторон цели и задачи режима защиты персональных данных, продемонстрировать их важность и обязательность применения. Система документации, регулирующая те или иные области защиты ИПХ, необходима для обоснования введения защитных мер в организации, применения адекватных мер ответственности в случае умышленного или случайного пренебрежения ими.

Поэтому начало внедрения происходит с разработки полного комплекта документов с последующем внедрением предусмотренных в документах организационных и организационно-технических мер. Разработка, утверждение высшим руководством и поддержание в актуальном состоянии документов в области защиты персональных данных позволяют получить уверенность, что все стороны процессов защиты ИПХ находятся в едином регуляционном поле и способствуют достижению всех утверждённых целей в области обеспечения надлежащего уровня информационной безопасности в соответствии с требованиями законодательства.

Поддержание документации в актуальном состоянии, отражающем реальные условия функционирования информационных систем, обрабатывающих и хранящих персональные данные, является обязательным условием для обеспечения прозрачного процесса управления ИПХ. Для этого организациям рекомендуется внедрить циклически повторяющийся процесс принятия решений в сфере защиты ИПХ, действующий по принципу Дёминга-Шухарта, иначе называемый PDCA (англ. *«**P**lan-**D**o-**C**heck-**A**ct»* — планирование-действие-проверка-корректировка).

Методология PDCA представляет собой простейший повторяющийся алгоритм действий руководителя по управлению процессом и достижению его целей. Цикл управления начинается с планирования:

- Планирование — разработка документов, установление целей и процессов, требуемых законодательством, планирование работ по достижению требуемого уровня соответствия, а также планирование выделения и распределения необходимых ресурсов, формирование бюджета закупок.
- Выполнение — выполнение запланированных работ.
- Проверка — сбор информации и контроль результата, получившегося в ходе выполнения процедур внедрения защитных мер ИПХ, выявление и анализ отклонений, установление причин отклонений. Как правило, этот этап наступает примерно через год после старта первой фазы цикла.

- Воздействие (управление, корректировка) — принятие мер по устранению причин отклонений от запланированного результата, внесение изменений в ранее разработанные документы, изменение планов по распределению ресурсов. Перезапуск цикла.

### Цель защиты персональных данных

Закон №58 описывает не просто требования к защите систем и серверов, а условия обработки персональных данных граждан. Поэтому соблюдение Закона №58 начинается не с антивируса и файрвола, а с разработки документов и постановки соответствующих организационных и организационно-технических процессов управления. Уполномоченный государственный орган по персональным данным в первую очередь будет требовать не просто обеспечения защиты соответствующими техническими средствами, а соблюдения правовых оснований для обработки персональных данных, таких как:

- с какой целью организация собирает персональные данные граждан;
- соответствует ли заявленная цель реальным потребностям организации;
- не собирает ли организация персональных данных больше, чем это требуется для её цели;
- существует ли политика обработки информации персонального характера, насколько она исполняется и соответствует требованиям Закона и декларируемым целям обработки ИПХ;
- определены ли сроки хранения персональных данных, насколько они объективны;
- имеется ли согласие Субъектов ИПХ о сборе, обработке, хранении, на трансграничную передачу, на обработку третьими лицами;
- имеются ли исторические данные, свидетельства исполнения требований Закона №58;
- корректно ли ведётся учёт обращений граждан, материальных носителей и экземпляров ИПХ.

Ответы на эти и другие подобные вопросы, а также сами управляющие процессы, должны быть зафиксированы в соответствующих документах. И лишь после создания необходимых документов, назначения офицера по ИПХ и внедрения соответствующих процессов управления можно приступать к подбору конкретных мер защиты и выбору технических средств. Какие именно средства, инструменты и сотрудники понадобятся каждой организации зависит от применяемых информационных систем, условий их работы и наличия актуальных угроз.

Такими образом, соблюдение законодательства по защите персональных данных — это, в первую очередь, внедрение и соблюдение определённых процессов, и

лишь во вторую — использование специальных технических средств защиты информации.

### Необходимость соответствия при хранении данных в облаке, за рубежом или у сервис-провайдера, в дата-центре

Существующей нормативной базой допускается размещение персональных данных на территории других стран при соблюдении фактически только двух базовых условий:

- при заключении международного договора, условия защиты персональных данных в котором не хуже действующих национальных норм;
- при наличии согласия субъекта персональных данных на передачу данных за рубеж.

При размещении персональных данных за пределами защищаемого периметра Держателя массива персональных данных, в местном или зарубежном облаке, с использованием мощностей сервис-провайдера, дата-центра, даже если они декларируют полное соответствие требованиям Закона №58, Держатель массива персональных данных не освобождается от ответственности за обеспечение безопасности персональных данных. По сути, внешний сервис-провайдер может нести солидарную ответственность только за два аспекта Управления ИПХ: их хранение и уничтожение в случае расторжения договора на предоставления услуг размещения. Все остальные действия с ИПХ совершаются Держателем — сбор, запись, систематизация, накопление, обновление (уточнение), изменение, обеспечение доступа, использование, передача, обезличивание, блокирование, а также удаление.

Для соблюдения правовых основ обработки персональных данных сервис-провайдером — пусть даже в ограниченном объёме «хранение и уничтожение», — было бы разумно предусмотреть в договоре поручение о передаче конкретных прав, что может и не может делать сервис-провайдер с персональными данными Держателя массива персональных данных. Декларация этих действий должна быть предусмотрена в Политике по защите ИПХ и доведена до сведения Субъектов при получении согласия на обработку ИПХ.

Таким образом, будучи Держателем массива персональных данных необходимость соблюдения требований законодательства об информации персонального характера сохраняется в любом случае вне зависимости от места размещения информационных систем, ответственных за Управление ИПХ.

## Документация

В качестве отправной точки при начале процедур внедрения рекомендуется остановится на разработке и утверждении следующих видов документов, которые должны быть соответствующим образом имплементированы в организационно-техническую инфраструктуру организации, а также быть подкреплёнными соответствующими кадровыми и материально-техническими ресурсами.

**Положения и политики**

1) Политика обработки и защиты ИПХ
2) Положение об обработке персональных данных
3) Положение об обеспечении безопасности персональных данных

**Проектная документация**

1) Частная модель угроз безопасности ИПХ
2) Общее описание ИС ИПХ
3) Описание технологического процесса обработки персональных данных
4) Концепция обеспечения безопасности ИПХ
5) Аналитическое обоснование набора мер по защите ИПХ
6) Техническое задание на создание средств защиты ИПХ
7) Технический паспорт ИС ИПХ
8) Технический паспорт защищаемого помещения

**Планы (опционально)**

1) План работ по внедрению и обеспечению соответствия требованиям законодательства и нормативной базы в области персональных данных
2) План мероприятий по защите ИПХ
3) План работ по контролю эффективности СЗ ИПХ

**Инструкции и регламенты**

1) Инструкция администратора безопасности ИС ИПХ
2) Инструкция системного администратора ИС ИПХ
3) Инструкция пользователя ИС ИПХ
4) Инструкция по проведению контроля защищённости
5) Инструкция по осуществлению антивирусного контроля
6) Инструкция по обеспечению режима безопасности и эксплуатации оборудования в защищаемом помещении
7) Инструкция ответственного за защиту информации в защищаемом помещении
8) Инструкция об организации работы с СКЗИ
9) Инструкция о порядке обращения с носителями ИПХ
10) Регламент реагирования на запросы субъектов ИПХ

11) Регламент реагирования на инциденты ИБ

**Приказы**

1) Приказ об организации работ по защите персональных данных
2) Приказ о вводе в действие организационно-распорядительных документов по обработке и защите персональных данных
3) Приказ о вводе в эксплуатацию объектов информатизации
4) Приказ о вводе в эксплуатацию АРМ ИС ИПХ
5) Приказ о назначении системного администратора ИС ИПХ
6) Приказ о назначении администратора безопасности ИС ИПХ
7) Приказ о контролируемой зоне
8) Приказ о назначении комиссии по проведению аттестации ИС ИПХ

**Акты**

1) Акт классификации ИС ИПХ
2) Акт определения уровня защищённости ИПХ
3) Акт установки СЗИ от НСД
4) Акт приёмки ИС ИПХ в опытную эксплуатацию
5) Акт приёмки ИС ИПХ в промышленную эксплуатацию
6) Акт приёма-передачи носителей персональных данных
7) Акт комиссионного уничтожения экземпляра ИПХ

**Журналы**

1) Журнал учёта обращений по вопросам персональных данных
2) Памятка к журналу регистрации обращений по вопросам персональных данных
3) Журнал учёта носителей конфиденциальной информации
4) Журнал учёта персональных идентификаторов и паролей ИС ИПХ
5) Журнал по учёту работ по контролю эффективности СЗ ИПХ

**Перечни**

1) Перечень лиц, имеющих доступ в помещения ИС ИПХ
2) Перечень лиц, допущенных к обработке персональных данных
3) Перечень объектов информатизации, предназначенных для обработки конфиденциальной информации
4) Перечень материальных носителей, содержащих ИПХ
5) Данные по уровню подготовки кадров, обеспечивающих защиту информации

**Обязательства и уведомления**

1) Уведомление-регистрация в уполномоченный государственный орган по персональным данным об обработке персональных данных

2) Обязательство работника о неразглашении персональных данных
3) Обязательство работника о соблюдении режима конфиденциальности персональных данных

**Согласие субъекта**

1) Согласие субъекта на обработку его персональных данных
2) Согласие субъекта на получение его персональных данных у третьей стороны
3) Согласие субъекта (работника) на передачу его персональных данных третьей стороне
4) Согласие субъекта (работника) на передачу его персональных данных в коммерческих целях

## Разработка частной модели угроз

Для оценки уровня состояния систем защиты и наиболее эффективного детектирования и устранения угроз ИБ, применяется технология построения модели угроз. Она позволяет описать перечень известных угроз ИБ применительно к используемым информационным системам Держателю массива персональных данных, и на основе этого получить актуальное состояние принятых или планируемых к принятию мер. Процесс построения моделей угроз состоит из пяти основных этапов:

1. Определение источников угроз
2. Выявление критических объектов информационной системы
3. Определение перечня угроз для каждого критического объекта
4. Выявление способа реализации угроз
5. Оценка ущерба от реализации угроз

Моделирование угроз — это процесс, с помощью которого потенциальные угрозы, такие как структурные уязвимости, могут быть идентифицированы, перечислены и приоритизированы с гипотетической точки зрения потенциального злоумышленника. Цель моделирования угроз состоит в том, чтобы предоставить Держателю массива персональных данных систематический анализ вероятного профиля злоумышленника, наиболее вероятных векторов атаки и наиболее желаемых атакующим активов. Моделирование угроз даст ответы на такие вопросы, как «Где ценные активы?», «В каком месте мы наиболее уязвимы для атак?», «Каковы наиболее актуальные угрозы?» и «Существует ли вектор атаки, который может остаться незамеченным?».

Концептуально большинство людей включают ту или иную форму моделирования угроз в свою повседневную жизнь и даже не осознают этого. Приезжающие на работу сотрудники используют моделирование угроз, чтобы рассмотреть, что может случиться утром во время поездки на работу, и принять

превентивные меры во избежание возможных ситуаций, которые могут привести к опозданию.

В соответствии с Постановлением от 21 ноября 2017 года № 760 Об утверждении Требований к обеспечению безопасности и защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищённости персональных данных», Держатель (обладатель) массива персональных данных, исходя из ценности защищаемой информации и стоимости мер по её защите, должен разработать и утвердить собственный перечень угроз безопасности персональных данных по особой форме, утверждённой уполномоченным государственным органом по персональным данным.

К моменту разработки данной методической рекомендации базовый перечень угроз безопасности находится на этапе разработки и рассмотрения. В данном случае проблемой является отсутствие утверждённого базового перечня угроз, а в результате и отсутствие инструмента построения модели угроз, что вкупе не позволяет корректно оценить угрозы безопасности ИПХ и соответственно провести самооценку уровня защиты. Поэтому в настоящем разделе будут рассмотрены варианты построения частной модели угроз, составленные на базе применяемых в странах СНГ и мире методах. Держатели массивов ИПХ могут также воспользоваться одной из популярных на Западе методологий по составлению модели угроз: STRIDE, P.A.S.T.A, VAST или Trike.

### Цель

Так как в пределах стран СНГ перечень угроз информационной безопасности является приблизительно одинаковым, то основой для данного руководства послужили методические документы, разработанные в поддержку российского и казахстанского законодательства по защите персональных данных. Целью данной методологии является построение методическая помощь при построении частной модели угроз в условиях отсутствия утверждённой Правительством базовой модели.

Следует обратить особое внимание на то, что после окончания работ над моделью, необходимо повторно проанализировать результаты и убедиться, что модель не имеет неточностей или неправильных интерпретаций.

### A1 Описание информационной системы

Первым этапом при построении модели угроз необходимо описать все имеющиеся информационные системы, задействованные при обработке персональных данных. Описание информационных систем должно быть достаточным для того, чтобы сотрудник, который не принимал участия в составлении модели угроз, мог понять, какие именно функции выполняет и из чего состоит данная информационная система.

**Пример**[1]

*Информационная система «Мүйүздөр жана туяктар» представляет собой физический сервер, который стоит в дальнем углу общего коридора, не имеет установленного пароля доступа и не обеспечен системой резервного копирования данных. На сервере развёрнута операционная система «MS Windows Server 2008». Основным программным обеспечением является база данных «MS SQL», которая содержит в себе персональные данные клиентов. Сотрудники могут получить доступ к системе из локальной сети или из сети интернет без использования защищённых каналов связи.*

### A2 Классификация и перечень угроз

Далее необходимо определить применимые к исследуемой информационной системе классы уязвимостей и перечень угроз. Определение «применимости» класса уязвимостей, той или иной угрозы производится экспертным методом, на основании компетентных профессиональных оценок и исходя из имеющейся для анализа информации.

**Пример**[2]

1. *Просмотр информации на дисплее компьютера в составе системы работниками, не допущенными к персональным данным;*
2. *Просмотр информации на дисплее компьютера в составе системы посторонними лицами, находящимися в помещении, в котором ведётся обработка персональных данных;*
3. *Просмотр информации на дисплее пользователей системы посторонними лицами, ведущими наблюдение (регистрацию) из-за границ контролируемой зоны;*
4. *Просмотр информации на дисплеях пользователей системы с помощью специальных устройств регистрации, внедрённых в помещение, в котором ведётся обработка персональных данных;*
5. *Перехват управления загрузкой операционной системы компьютеров в составе системы (угрозы, направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывод, перехват управления загрузкой);*

[1] Стиль и формат описания может от отличаться в зависимости от сложившихся в организации требований к оформлению.

[2] Классы уязвимостей взяты из ГОСТ Р 56546-2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем» указаны исключительно для примера, более подробная информация о классах и их описаниях находятся в этом же стандарте

6. *Вызов штатных программ ОС компьютеров в составе системы или запуск специально разработанных программ, реализующих несанкционированный доступ к системе;*
7. *Внедрение в систему вредоносных программ;*
8. *Хищение элементов компьютера в составе системы, содержащих персональные данные;*
9. *Хищение отчуждаемых носителей информации, содержащих персональные данные;*
10. *Вывод из строя компьютера в составе системы;*
11. *Внедрение в систему аппаратных закладок;*
12. *Анализ сетевого трафика с перехватом информации внешних сетей;*
13. *Сканирование для выявления типа операционной системы компьютера, открытых портов и служб, открытых соединений и др.;*
14. *Подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа;*
15. *Выявление паролей;*
16. *Сетевые атаки типа «Отказ в обслуживании»;*
17. *Удалённый запуск приложений на компьютере;*
18. *Внедрение по сети вредоносных программ;*
19. *Ошибочные действия пользователей, приводящие к нарушению безопасности персональных данных;*
20. *Выход из строя техсредств системы в результате сбоев, аварий;*
21. *Уничтожение данных в системе или блокирование доступа к системе, вызванное стихийными бедствиями*

### А3 Определение глобального уровня исходной защищённости $Y_1$

Следующим этапом необходимо определить глобальный уровень исходной защищённости. Этот этап определяется единожды при построении или пересмотре модели угроз конкретной информационной системы и не меняется в зависимости от угрозы. Под уровнем исходной защищённости ИС ИПХ понимается обобщённый показатель, зависящий от технических и эксплуатационных характеристик ИС ИПХ ($Y_1$ = N).

| Технические и эксплуатационные характеристики | Уровень исходной защищённости $Y_1$ | | |
|---|---|---|---|
| | Высокий | Средний | Низкий |
| **По территориальному размещению:** | | | |
| распределённая ИС ИПХ, которая охватывает несколько областей, районов или государство в целом; | — | — | ● |
| городская ИС ИПХ, охватывающая не более одного населённого пункта (города, посёлка); | — | — | ● |
| корпоративная распределённая ИС ИПХ, охватывающая многие подразделения одной организации; | — | ● | — |
| локальная (кампусная) ИС ИПХ, развёрнутая в пределах нескольких близко расположенных зданий; | — | ● | — |
| локальная ИС ИПХ, развёрнутая в пределах одного здания | ● | — | — |
| **По наличию соединения с сетями общего пользования:** | | | |

| Технические и эксплуатационные характеристики | Уровень исходной защищённости $Y_1$ | | |
|---|---|---|---|
| | Высокий | Средний | Низкий |
| ИС ИПХ, имеющая многоточечный выход в сеть общего пользования; | — | — | ● |
| ИС ИПХ, имеющая одноточечный выход в сеть общего пользования; | — | ● | — |
| ИС ИПХ, физически отделённая от сети общего пользования | ● | — | — |
| **По встроенным (легальным) операциям с записями баз персональных данных:** | | | |
| чтение, поиск; | ● | — | — |
| запись, удаление, сортировка; | — | ● | — |
| модификация, передача | — | — | ● |
| **По разграничению доступа к персональным данным:** | | | |
| ИС ИПХ, к которой имеют доступ определённые перечнем сотрудники организации, являющейся владельцем ИС ИПХ, либо субъект ИПХ; | — | ● | — |
| ИС ИПХ, к которой имеют доступ все сотрудники организации, являющейся владельцем ИС ИПХ; | — | — | ● |
| ИС ИПХ с открытым доступом | — | — | ● |
| **По наличию соединений с другими базами ИПХ иных ИС ИПХ:** | | | |
| интегрированная ИС ИПХ (организация использует несколько баз ИПХ ИС ИПХ, при этом организация не является владельцем всех используемых баз ИПХ); | — | — | ● |
| ИС ИПХ, в которой используется одна база ИПХ, принадлежащая организации — владельцу данной ИС ИПХ | ● | — | — |
| **По уровню обобщения (обезличивания) ИПХ:** | | | |
| ИС ИПХ, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.); | ● | — | — |
| ИС ИПХ, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации; | — | ● | — |
| ИС ИПХ, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ИПХ) | — | — | ● |
| **По объёму ИПХ, которые предоставляются сторонним пользователям ИС ИПХ без предварительной обработки:** | | | |
| ИС ИПХ, предоставляющая всю базу данных с ИПХ; | — | — | ● |
| ИС ИПХ, предоставляющая часть ИПХ; | — | ● | — |
| ИС ИПХ, не предоставляющая никакой информации. | ● | — | — |

Соотнося технические, нормативные и географические показатели целевой ИС подсчитывается количество положительных соответствий и на основании нижеприведённой таблицы выводится обобщённый показатель исходного уровня защищённости информационной системы

| Уровень исходной защищённости | Процент положительных результатов соответствия | Коэффициент $Y_1$ |
|---|---|---|
| Низкий | Высокий < 70% и Средний < 70% и Низкий > 0% | 10 |
| Средний | Высокий < 70% и Средний > 70% | 5 |

| | | |
|---|---|---|
| Высокий | Высокий > 70% и Средний >= 30% | 0 |

1. ИС ИПХ имеет высокий уровень исходной защищённости, если не менее 70% характеристик ИС ИПХ соответствуют уровню «высокий» (суммируются положительные решения по первому столбцу, соответствующему высокому уровню защищённости), а остальные — среднему уровню защищённости (положительные решения по второму столбцу).
2. ИС ИПХ имеет средний уровень исходной защищённости, если не выполняются условия по пункту 1 и не менее 70% характеристик ИС ИПХ соответствуют уровню не ниже «средний» (берётся отношение суммы положительных решений по второму столбцу, соответствующему среднему уровню защищённости, к общему количеству решений), а остальные — низкому уровню защищённости.
3. ИС ИПХ имеет низкую степень исходной защищённости, если не выполняются условия, соответствующие пунктам 1 и 2.

**Пример расчёта уровня исходной защищённости**

| **Технические и эксплуатационные характеристики** | **Уровень исходной защищённости $Y_1$** | | |
|---|---|---|---|
| | Высокий | Средний | Низкий |
| **По территориальному размещению:** | | | |
| локальная ИС ИПХ, развёрнутая в пределах одного здания | • | — | — |
| **По наличию соединения с сетями общего пользования:** | | | |
| ИС ИПХ, имеющая одноточечный выход в сеть общего пользования; | — | • | — |
| **По встроенным (легальным) операциям с записями баз персональных данных:** | | | |
| запись, удаление, сортировка; | — | • | — |
| **По разграничению доступа к персональным данным:** | | | |
| ИС ИПХ, к которой имеют доступ определённые перечнем сотрудники организации, являющейся владельцем ИС ИПХ, либо субъект ИПХ; | — | • | — |
| **По наличию соединений с другими базами ИПХ иных ИС ИПХ:** | | | |
| ИС ИПХ, в которой используется одна база ИПХ, принадлежащая организации — владельцу данной ИС ИПХ | • | — | — |
| **По уровню обобщения (обезличивания) ИПХ:** | | | |
| ИС ИПХ, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.); | • | — | — |
| **По объёму ИПХ, которые предоставляются сторонним пользователям ИС ИПХ без предварительной обработки:** | | | |
| ИС ИПХ, предоставляющая часть ИПХ | — | • | — |
| **Итого** | **42,86%** | **57,14%** | **0,00** |

*Подсчитав все показатели по всем уровням защищённости согласно разделу А3 «Определение глобального уровня исходной защищённости», показатели распределились следующим образом:*

*Низкий — ни одного пункта*

*Средний — 4 пункта*

*Высокий — 3 пункта*

*Таким образом, применяя элементарную пропорцию, рассчитывается относительное количество занятых ячеек в таблице:*

*Низкий:* $0{,}00\%$

*Средний (4 пункта из 7 возможных):* $\frac{4\times100}{7} = \mathbf{57,14}\%$

*Высокий (3 пункта из 7 возможных):* $\frac{3\times100}{7} = \mathbf{42,86}\%$

| $Y_1$ | Уровень защищённости | | |
|---|---|---|---|
| | Высокий | Средний | Низкий |

| | | | |
|---|---|---|---|
| **Высокий = 0** | ∑ ≥ 70% | ∑ ≤ 30% | 0% |
| **Средний = 5** | ∑ < 70% | ∑ ≥ 70% | ∑ ≤ 30% |
| **Низкий = 10** | ∑ < 70% | ∑ < 70% | ∑ > 0% |

*Согласно таблице, исходная защищённость системы является средней ($Y_1$=5), так как удовлетворяет описанным выше условиям.*

### А4 Модель нарушителя

Следующим этапом предстоит определить модель нарушителя для конкретной информационной системы. Определение типов и видов потенциальных нарушителей необходимо для подтверждения, что применимые к ИС ИПХ угрозы могут стать реальными, если для их реализации будут привлечены соответствующие исполнители, обладающие известными или предполагаемыми мотивами. В связи с тем, что не существует описанной методологии по построению модели нарушителя, то при построении модели следует экспертным путём, придерживаясь принципов сообразности, логичности и адекватности, сделать выводы самостоятельно.

В мировой практике принято делить нарушителей на внутренних и внешних, обладающих низким, средним или высоким потенциалом (потенциал — мера усилий, затрачиваемых нарушителем при реализации угроз безопасности информации в информационной системе). Категории нарушителей традиционно включают в себя следующие типы:

| Нарушители | Категория нарушителя | Потенциал нарушителя | Возможная мотивация |
|---|---|---|---|
| **Неустановленные внешние субъекты (физические лица)** | Внешний нарушитель | с низким потенциалом | Идеологические или политические мотивы.<br>Причинение имущественного ущерба путем мошенничества или иным преступным путем.<br>Любопытство или желание самореализации (подтверждение статуса).<br>Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды. |
| **Бывшие работники (пользователи)** | Внешний нарушитель | с низким потенциалом | Причинение имущественного ущерба путем мошенничества или иным преступным путем.<br>Месть за ранее совершенные действия. |
| **Лица, обеспечивающие функционирование информационных систем или обслуживающих инфраструктуру оператора (администрация, охрана, уборщики и т.д.)** | Внутренний нарушитель | с низким потенциалом | Причинение имущественного ущерба путем обмана или злоупотребления доверием.<br>Непреднамеренные, неосторожные или неквалифицированные действия. |
| **Лица, привлекаемые для установки, наладки, монтажа, пуско-наладочных и иных работ** | Внутренний нарушитель | с низким потенциалом | Причинение имущественного ущерба путем обмана или злоупотребления доверием.<br>Непреднамеренные, неосторожные или неквалифицированные действия |

| Нарушители | Категория нарушителя | Потенциал нарушителя | Возможная мотивация |
|---|---|---|---|
| **Пользователи информационной системы** | Внутренний нарушитель | с низким потенциалом | Причинение имущественного ущерба путем мошенничества или иным преступным путем.<br>Любопытство или желание самореализации (подтверждение статуса).<br>Месть за ранее совершенные действия.<br>Непреднамеренные, неосторожные или неквалифицированные действия. |
| **Администраторы информационной системы и администраторы безопасности** | Внутренний нарушитель | со средним потенциалом | Причинение имущественного ущерба путем мошенничества<br>или иным преступным путем.<br>Любопытство или желание самореализации (подтверждение статуса).<br>Месть за ранее совершенные действия.<br>Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды.<br>Непреднамеренные, неосторожные или неквалифицированные действия. |
| **Террористические, экстремистские группировки** | Внешний нарушитель | со средним потенциалом | Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики.<br>Совершение террористических актов.<br>Идеологические или политические мотивы.<br>Дестабилизация деятельности органов государственной власти, организаций. |
| **Преступные группы (криминальные структуры)** | Внешний нарушитель | со средним потенциалом | Причинение имущественного ущерба путем мошенничества или иным преступным путем.<br>Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды |
| **Конкурирующие организации** | Внешний нарушитель | со средним потенциалом | Получение конкурентных преимуществ.<br>Причинение имущественного ущерба путем обмана или злоупотребления доверием |
| **Разработчики, производители, поставщики программных, технических и программно-технических средств** | Внешний нарушитель | со средним потенциалом | Внедрение дополнительных функциональных возможностей в программное обеспечение или программно-технические средства на этапе разработки.<br>Причинение имущественного ущерба путем обмана или злоупотребления доверием.<br>Непреднамеренные, неосторожные или неквалифицированные действия. |
| **Специальные службы иностранных государств (блоков государств)** | Внутренний нарушитель | с высоким потенциалом | Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики.<br>Дискредитация или дестабилизация деятельности органов государственной власти, организаций. |

Из этой таблицы следует, что:

1. Высокий потенциал подразумевает наличие возможностей уровня предприятия/группы предприятий/государства по разработке и использованию специальных средств эксплуатации уязвимостей.

2. Средний потенциал подразумевает наличие возможностей уровня группы лиц/организации по разработке и использованию специальных средств эксплуатации уязвимостей.
3. Низкий потенциал подразумевает наличие возможностей уровня одного человека по приобретению (в свободном доступе на бесплатной или платной основе) и использованию специальных средств эксплуатации уязвимостей

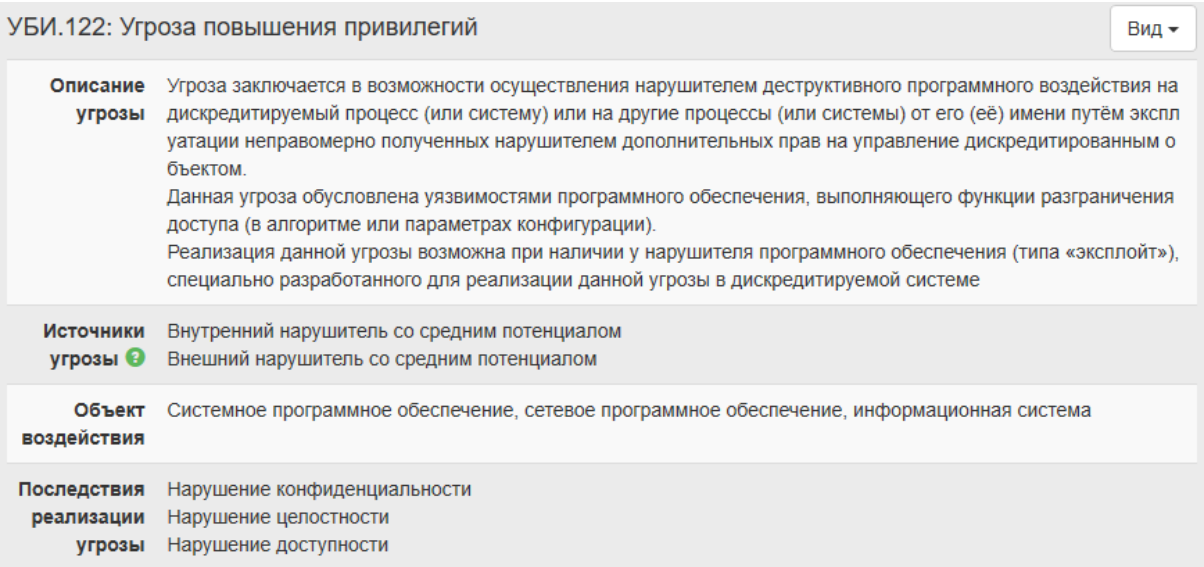
Порядок рассуждений при этом может выглядеть следующим образом, принимая во внимание ценность и важность защищаемой информации. Допустим, предполагаемая мотивация при реализации угрозы соответствует как минимум трём видам нарушителей с различным потенциалом: влиятельная иностранная разведывательная организация, специалист-пентестер и сотрудник, имеющий в распоряжении инсайдерскую информацию. Из чего можно сделать следующие выводы:

1. Влиятельная разведывательная организация имеет Высокий потенциал, так как ее технические и материальные ресурсы гипотетически ничем не ограничены.
2. Сотрудник с инсайдерской информацией имеет Средний потенциал, так как может проводить более точечные атаки, но не всегда преследует корыстные цели и часто имеет ограниченные ресурсы.
3. Независимый и незаинтересованный пентестер (хакер) имеет Низкий потенциал так как пользуется только общедоступной информацией и техническими средствами и вдобавок часто ограничен в ресурсах.

| Тип нарушителя | Категории нарушителей | Идентификатор | Потенциал |
|---|---|---|---|
| **Внешний нарушитель** | внешние субъекты (физические лица) | G1 | Низкий |
| | спецслужбы | G2 | Высокий |
| **Внутренний нарушитель** | Лица, имеющие санкционированный доступ в контролируемую зоны, но не имеющие доступа к ИС ИПХ (технический и обслуживающий персонал) | G3 | Средний |

### А6 Угрозы

Экспертные оценки, проведённые в рамках разделов А1—А5, создают минимально-необходимый исходный базис, который позволит перейти непосредственно к подбору актуальных угроз. В мире существует большое количество свободно-доступных баз данных угроз, поддерживаемых в актуальном состоянии. Для наглядности, в примере используется угроза из банка данных федеральной службы ТЭК РФ.




### А7 Оценка опасности угроз

Оценка опасности угрозы определяется экспертным методам на основе предполагаемого уровня негативности последствий нарушений основных свойств информации: доступности, конфиденциальности, целостности.

Существует четыре уровня опасности:

1. низкая опасность, если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;
2. средняя опасность, если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;
3. высокая опасность, если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

**Пример**

*Путём оценки уровня вреда субъекту персональных данных «Мүйүздөр жана туяктар», который может быть причинён в случае реализации угрозы, опираясь на таблицу, регламентирующую методологию оценки информации в Постановлении от 21 ноября 2017 года № 760, необходимо определить уровень опасности каждой угрозы, исходя из её ценности, возможной мотивации злоумышленника, предполагаемых прямых и косвенных потерь, включая санкции госорганов, штрафы, судебные иски и другие значимые факторы. Для примера используется часть угроз из главы А2.*

| Угроза | Опасность |
|---|---|
| Просмотр информации на дисплее компьютера в составе системы работниками, не допущенными к персональным данным; | Высокая |
| Просмотр информации на дисплее компьютера в составе системы посторонними лицами, находящимися в помещении, в котором ведётся обработка персональных данных; | Высокая |
| Просмотр информации на дисплее пользователей системы посторонними лицами, ведущими наблюдение (регистрацию) из-за границ контролируемой зоны; | Высокая |
| Просмотр информации на дисплеях пользователей системы с помощью специальных устройств регистрации, внедрённых в помещение, в котором ведётся обработка персональных данных; | Высокая |

| | |
|---|---|
| Перехват управления загрузкой операционной системы компьютеров в составе системы (угрозы, направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывод, перехват управления загрузкой); | Низкая |
| Вызов штатных программ ОС компьютеров в составе системы или запуск специально разработанных программ, реализующих несанкционированный доступ к системе; | Высокая |
| Внедрение в систему вредоносных программ; | Высокая |
| Хищение элементов компьютера в составе системы, содержащих персональные данные; | Высокая |

### A8 Вероятность реализации $Y_2$

Под частотой (вероятностью) реализации угрозы понимается определяемый экспертным способом показатель, который призван выявить, насколько вероятным является реализация конкретной угрозы безопасности ИПХ для данной ИС ИПХ в конкретной ситуации. Для определения вероятности применяется монополярная вербальная шкала в качестве формы фиксации данных, опирающаяся на набор суждений о наличии или степени выраженности изучаемого признака:

| Значение | Описание | Балл $Y_2$ |
|---|---|---|
| **маловероятно** | отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими легального доступа в помещение, где последние хранятся) | 0 |
| **низкая вероятность** | объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты информации) | 2 |
| **средняя вероятность** | объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ИПХ недостаточны | 5 |
| **высокая вероятность** | объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ИПХ не приняты | 10 |

Результатом экспертной оценки по вербальной шкале должен стать перечень предпосылок для вероятной эксплуатации угрозы и реализованные меры защиты, а также оценка вероятности угроз, например:

*Предпосылки:*

- *отсутствие защищённых каналов взаимодействия*
- *отсутствие жёсткого распределения полномочий сотрудников*
- *наличие неконтролируемого удалённого доступа из-за пределов защищаемого периметра (сети Интернет)*
- *ценная обрабатываемая персональная информация*
- *свободный физический доступ к оборудованию для сотрудников*
- *использование устаревших и небезопасных версий ПО*

*Меры защиты:*

- *помещение, в которой расположена информационная система, является местом ограниченного доступа за счёт пропускного режима в здании*

Таким образом:

**Пример**[3]

*Информация, хранящаяся на сервере «Мүйүздөр жана туяктар», может стать объектом промышленного шпионажа, так как она представляет ценность для конкурентов и спецслужб. Для её получения могут применяться различные средства, включая подкуп наших сотрудников или применение специализированных средств, доступных спецслужбам или внешним пентестерам. Соединение с сервером производится по небезопасному каналу, сетевой экран отсутствует или не настроен, версии применяемых операционных и прикладных систем являются устаревшими. Получить доступ к серверу для внутреннего сотрудника не составляет никакого труда. Следовательно, для некоторых угроз вероятность атаки будет являться «Высокой» или $Y_2 = 10$.*

| Угроза | Вероятность $Y_2$ |
|---|---|
| Просмотр информации на дисплее компьютера в составе системы работниками, не допущенными к персональным данным; | 10 |
| Просмотр информации на дисплее компьютера в составе системы посторонними лицами, находящимися в помещении, в котором ведётся обработка персональных данных; | 10 |
| Просмотр информации на дисплее пользователей системы посторонними лицами, ведущими наблюдение (регистрацию) из-за границ контролируемой зоны; | 0 |
| Просмотр информации на дисплеях пользователей системы с помощью специальных устройств регистрации, внедрённых в помещение, в котором ведётся обработка персональных данных; | 0 |
| Перехват управления загрузкой операционной системы компьютеров в составе системы (угрозы, направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывод, перехват управления загрузкой); | 0 |
| Вызов штатных программ ОС компьютеров в составе системы или запуск специально разработанных программ, реализующих несанкционированный доступ к системе; | 0 |
| Внедрение в систему вредоносных программ; | 10 |
| Хищение элементов компьютера в составе системы, содержащих персональные данные; | 10 |

В зарубежной литературе используется элементарное соотношение для определения коэффициента реализуемости каждой угрозы:

$$Y = \frac{(Y_1 + Y_2)}{20},$$

Где $Y$ — коэффициент реализации угроза, $Y_1$ — глобальный уровень защищённости (раздел А3), а $Y_2$ — вероятность реализации угрозы (раздел А8), при этом «*20*» — максимально возможное значение суммы $Y_1$ и $Y_2$. Таким образом, ряд угроз со значениями *$Y_2 = 0$ или $Y_2 = 10$ будут рассчитываться следующим образом*

$$Y = \frac{(Y_1 + Y_2)}{20} = \frac{(5 + 0)}{20} = 0{,}25$$

[3] Экспертная оценка определения возможности реализации угрозы должна по возможности учитывать все возможные факторы, которые так или иначе влияют на ослабление мер защиты или проведение атаки на ИС ИПХ.

$$Y = \frac{(Y_1 + Y_2)}{20} = \frac{(5 + 10)}{20} = 0{,}75$$

Интерпретация получившегося значения Y осуществляется согласно прилагаемой Таблице:

| Возможность реализуемости угрозы | Коэффициент Y |
|---|---|
| **Очень высокая** | $Y > 0{,}8$ |
| **Высокая** | $0{,}6 < Y \leq 0{,}8$ |
| **Средняя** | $0{,}3 < Y \leq 0{,}6$ |
| **Низкая** | $0 \leq Y \leq 0{,}3$ |

Таким образом, возможность реализации некоторых угроз в отношении рассматриваемой системы является **Высокой** (для Y=0,75), в то время как возможность реализации остальных угроз должны рассматриваться в качестве **Низкой** (для Y=0,25).

### A9 Актуальность угрозы

Несмотря на наличие явных предпосылок к реализации атак, высокие показатели незащищённости системы и применимых угроз, актуальность угрозы может быть поставлена под сомнение, если ущерб в результате реальной атаки будет являться несущественным. Если в результате экспертной оценки будет признано, что вероятный ущерб в стоимостном выражении будет существенно выше затрат на защиту информационной системы «Мүйүздөр жана туяктар», тогда актуальность угрозы должна быть признана положительной.

Это можно сделать, используя имеющиеся требования, отражённые в Постановлении ПКР:

| Характеристика | Показатель опасности угрозы |
|---|---|
| Незначительный вред, легко компенсируемый держателем ИПХ | **Низкий** |
| Незначительные затраты — менее 1000 расчётных показателей на ликвидацию/компенсацию последствий за причинённые убытки и моральный вред | **Средний** |
| Значительный вред, который может быть компенсирован держателем ИПХ, и Значительные затраты — более 1000 расчётных показателей, на ликвидацию/компенсацию последствий за причинённые убытки и моральный вред либо Критический вред — причинение убытков и морального вреда, которые не могут быть компенсированы | **Высокий** |

Для осуществления окончательного выбора из предварительного перечня угроз безопасности только тех угроз, которые относятся к актуальным для рассматриваемой ИС ИПХ, необходимо воспользоваться правилом, приведённым в таблице:

| Возможность реализации угрозы (A8) | Показатель опасности угрозы (A9) | | |
|---|---|---|---|
| | **Низкая** | **Средняя** | **Высокая** |
| **Низкая** | неактуальная | неактуальная | актуальная |
| **Средняя** | неактуальная | актуальная | актуальная |
| **Высокая** | актуальная | актуальная | актуальная |
| **Очень высокая** | актуальная | актуальная | актуальная |

| Угроза | Возможность реализации | Опасность | Актуаль-ность |
|---|---|---|---|
| Просмотр информации на дисплее компьютера в составе системы работниками, не допущенными к персональным данным; | Высокая | Высокая | **Да** |
| Просмотр информации на дисплее компьютера в составе системы посторонними лицами, находящимися в помещении, в котором ведётся обработка персональных данных; | Высокая | Высокая | **Да** |
| Просмотр информации на дисплее пользователей системы посторонними лицами, ведущими наблюдение (регистрацию) из-за границ контролируемой зоны; | Низкая | Высокая | **Да** |
| Просмотр информации на дисплеях пользователей системы с помощью специальных устройств регистрации, внедрённых в помещение, в котором ведётся обработка персональных данных; | Низкая | Высокая | **Да** |
| Перехват управления загрузкой операционной системы компьютеров в составе системы (угрозы, направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывод, перехват управления загрузкой); | Низкая | Низкая | **Нет** |
| Вызов штатных программ ОС компьютеров в составе системы или запуск специально разработанных программ, реализующих несанкционированный доступ к системе; | Низкая | Высокая | **Да** |
| Внедрение в систему вредоносных программ; | Высокая | Высокая | **Да** |
| Хищение элементов компьютера в составе системы, содержащих персональные данные; | Высокая | Высокая | **Да** |

Тем самым мы приходим к выводу, что лишь одна угроза из числа рассматриваемых является неактуальной для «Мүйүздөр жана туяктар», получившая одновременно низкие оценки вероятности и опасности.

### A10 Управление угрозами информационной безопасности

После успешного построения модели угроз, в зависимости от их актуальности, следует экспертными методами определить вероятную длительность воздействия каждой угрозы на конкретную информационную систему.

Для этого необходимо для каждой отдельной угрозы, изучив предпосылки и имеющиеся и предполагаемые меры защиты, определить вероятные события, в случае наступления которых наша угроза становится не актуальной, либо меняется уровень её опасности или вероятности реализации. Если ни один из имеющихся способов не в состоянии повлиять на изменение характеристик угрозы, ведущих к её деактуализации, следует рассматривать эту угрозу в качестве долгосрочной. В противном случае, когда прогноз наступления события, приводящего к деактуализации угрозы, является меньше 2-х недель, то угроза может быть сразу признана неактуальной.

**Пример**

На изменение общей актуальности угроз информационной системы может повлиять наступление одного или нескольких из следующих событий:

- увеличение уровня защиты за счёт установки дополнительных мер защиты, таких как: установка и настройка межсетевого экрана, установка шифрованного канала взаимодействия, внедрение процесса управления обновлениями и установка последних версий используемого ПО и т. д.;
- деактуализация угрозы за счёт уничтожения персональных данных, если наступило окончание срока их обработки;
- деперсонификация хранимых данных, в результате чего будет снижен уровень критичности информации, что в свою очередь снизит показатель опасности угрозы и может в итоге привести к деактуализации угрозы.

| Угроза | Вероятность Y1 | $Y = \frac{(Y_1 + Y_2)}{20}$ | Возможность Y | Опасность | Актуальность | Нарушитель |
|---|---|---|---|---|---|---|
| **Просмотр информации на дисплее компьютера в составе системы посторонними лицами, находящимися в помещении, в котором ведётся обработка персональных данных** | 0 | 0,25 | Низкая | Высокая | Да | ВН1 |
| Организационно-технические меры защиты от угрозы | 1. Реализация разрешительной системы допуска пользователей и обслуживающего персонала в помещения, в которых установлены устройства отображения информации ИС ИПХ<br>2. Автоматическая блокировка экрана при отсутствии пользователя на рабочем месте<br>3. Использование плотных штор или жалюзи на окнах в помещениях, в которых установлены устройства отображения | | | | | |
| **Внедрение в систему вредоносных программ** | 10 | 0,75 | Высокая | Высокая | Да | ВН1, ВН2 |
| Организационно-технические меры защиты от угрозы | 1. Использование средств антивирусной защиты;<br>2. Регулярное обновление ПО, используемого в серверных и клиентских компонентах ИС ИПХ;<br>3. Использование систем доверенной загрузки. | | | | | |

### А11 Результат

К завершению работ по составлению частной модели угроз держатель массива ИПХ должен получить следующую структуру документа:

1. Введение
2. Перечень сокращений
3. Перечень нормативных документов
4. Условия пересмотра модели угроз
5. Описание ИС ИПХ 1
6. Модель угроз ИС ИПХ 1
   - Угроза 1
   - Угроза 2
   - Угроза N
7. Описание ИС ИПХ N
8. Модель угроз ИС ИПХ N
   - Угроза 1
   - Угроза 2
   - Угроза N
9. Методология
10. Заключение

<table>
<tr><td>Актив</td><td colspan="5">Информационная система «Мүйүздөр жана туяктар» представляет собой физический сервер, который стоит в дальнем углу общего коридора, не имеет установленного пароля доступа и не обеспечен системой резервного копирования данных. На сервере развёрнута операционная система «MS Windows Server 2008». Основным программным обеспечением является база данных «MS SQL», которая содержит в себе персональные данные клиентов. Сотрудники могут получить доступ к системе из локальной сети или из сети интернет без использования защищённых каналов связи.</td></tr>
<tr><td rowspan="4">Угроза<br>Угроза повышения привилегий<br>Угроза заключается в возможности осуществления нарушителем деструктивного программного воздействия на дискредитируемый процесс (или систему) или на другие процессы (или системы) от его (её) имени путём эксплуатации неправомерно полученных нарушителем дополнительных прав на управление дискредитированным объектом.<br>Данная угроза обусловлена уязвимостями программного обеспечения, выполняющего функции разграничения доступа (в алгоритме или параметрах конфигурации).<br>Реализация данной угрозы возможна при наличии у нарушителя программного обеспечения (типа «эксплойт»), специально разработанного для реализации данной угрозы в дискредитируемой системе</td><td>Исходная степень защищённости</td><td>Вероятность реализации угрозы</td><td>Опасность угрозы</td><td>Возможность реализации</td><td>Актуальность</td></tr>
<tr><td>$Y_1 = 10$</td><td>$Y_2 = 10$</td><td>Высокая</td><td>Очень высокая</td><td>Актуальная</td></tr>
<tr><td colspan="2">Предпосылки</td><td colspan="2">Защитные меры</td><td>Эффективность защитных мер</td></tr>
<tr><td colspan="2">- отсутствие защищённых каналов взаимодействия<br>- наличие неконтролируемого удалённого доступа из-за пределов защищаемого периметра (сети Интернет)<br>- свободный физический доступ к оборудованию для сотрудников<br>- устаревшие версии ПО</td><td colspan="2">помещение, в которой расположена информационная система, является местом ограниченного доступа за счёт пропускного режима в здании</td><td>минимальная</td></tr>
<tr><td>Источник угрозы (нарушитель)</td><td colspan="5">Внутренний нарушитель со средним потенциалом<br>Внешний нарушитель со средним потенциалом</td></tr>
<tr><td rowspan="2">Последствия реализации угрозы</td><td colspan="2">Нарушение целостности</td><td colspan="2">Нарушение доступности</td><td>Нарушение конфиденциальности</td></tr>
<tr><td colspan="2">Да</td><td colspan="2">Да</td><td>Да</td></tr>
<tr><td>Длительность воздействия угрозы</td><td colspan="5">Долгосрочно</td></tr>
</table>