

**КГУ «Управление архитектуры и
градостроительства города Алматы»**

УТВЕРЖДЕНО

**Руководитель Управления
архитектуры и градостроительства
города Алматы**



 Ахмеджанов А. Т.

М. П.

«14» сентября 2019 г.

**Правила идентификации, классификации и маркировки активов,
связанных со средствами обработки информации
Информационной системы «3D автоматизированная
геоинформационная система города Алматы»
3DGEO.СМИБ.ПР.03.r01.19**

**г. Алматы
2019 г.**

1. Область применения

Целью настоящего документа является описание правил идентификации, классификации и маркировки активов, связанных со средствами обработки информации ИС и определение порядка действий ответственных сотрудников Организации, а также определение ответственности при проведении этих мероприятий или нарушении требований настоящего Документа.

Настоящий документ обязателен для исполнения в рамках проекта обеспечения работы ИС.

Настоящий документ применим как к активам в физической, так и в электронной форме.

2. Нормативные ссылки

Настоящий документ содержит указания к практическому исполнению требований изложенных в нормативных документах согласно п. 3 Нормативные ссылки действующей Политики информационной безопасности.

3. Термины, определения и сокращения

В настоящем документе используются термины и сокращения, принятые в действующей Политике информационной безопасности.

4. Общие положения

Настоящий документ регламентирует:

- 1) порядок по проведению идентификации и классификации активов (информационные активы, физические активы и другие);
- 2) закрепление ответственных лиц за идентифицированные активы;
- 3) порядок составления и ведения реестра активов (с указанием класса актива, вида актива, значимость и владельца актива);
- 4) порядок маркировки активов в зависимости от их установленного класса, конфиденциальности, ценности и критичности;
- 5) выполнение требований на полноту сведений реестра активов.

Ответственный за обеспечение ИБ должен регулярно сопоставлять применяемые категории (классы, грифы) информации сторонних организаций с соответствующими классами, принятыми в Организации, которые могут иметь другие определения или содержание для тех же самых или подобных категорий, держать таблицу сопоставлений в актуальном состоянии и уведомлять заинтересованные стороны в случае их изменений.

В случае если сторонняя организация запрашивает сведения о классификации информации ответственный за обеспечение ИБ сотрудник может предоставить сведения только получив соответствующее разрешение руководства Организации.

5. Порядок составления и ведения реестра активов

Активы классифицируются исходя из требований законодательства РК, ее конфиденциальности, а также ценности и критичности для Организации.

Все информационные активы ИС подлежат обязательному учету, за каждым активом закрепляется ответственный сотрудник.

Ответственный за обеспечение ИБ должен составить и держать в актуальном состоянии перечень (реестр) активов и ответственных за них сотрудников (по форме Приложения 4), обеспечивающих поддержание соответствующих мероприятий по управлению информационной безопасностью в отношении вверенных им активов.

Реестр активов должен содержать полную и достоверную информацию об активе.

При классификации активов и связанных с ними мероприятий по управлению информационной безопасностью учитываются требования бизнеса в совместном использовании и ограничении доступа к информации, а также последствия, связанные с такими требованиями.

Процедура классификации и переклассификации активов выполняется в ходе инвентаризации, и как одно из корректирующих действий внутреннего аудита. Результаты классификации должны учитываться в процессе предоставления доступа, в соответствии с заданной политикой контроля доступа.

Ответственный за обеспечение ИБ должен составить и держать в актуальном состоянии перечень активов и ответственных за них сотрудников, обеспечивающих поддержание соответствующих мероприятий по управлению информационной безопасностью в отношении вверенных им активов.

6. Классификация активов

Настоящий документ регламентирует следующую классификацию активов Организации.

Классификация активов по возможностям мобильности:

- а) стационарные;
- б) переносные (или мобильные).

Классификация активов по месту расположения:

- а) в помещениях заказчика, клиентов, партнеров, пользователей, сторонних организаций;
- б) в здании Организации;
- с) на сторонних серверных площадках.

Классификация активов по типу:

- а) оборудование: активное оборудование (например, серверы, дисковые массивы, сетевое оборудование, СКУД, обеспечение климата,

автоматическое пожаротушение и т. д.), пассивное оборудование (например, кабели, порты, электрические розетки и т. д.);

- б) программное обеспечение: проприетарное ПО, свободное ПО;
- с) услуга, предоставляемая Организации;
- д) услуга, предоставляемая Организацией.

Классификация оборудования по месту использования:

- а) серверное оборудование;
- б) клиентское оборудование.

Классификация ПО по месту использования:

- а) серверное ПО;
- б) клиентское ПО.

Классификация охраняемых помещений по назначению:

- а) серверное помещение;
- б) рабочее помещение.

Все типы активов, за исключением информационных классифицируются следующим способом.

Непродолжительное отсутствие (неработоспособность, недоступность, выход из строя) актива (от нескольких минут до 24 часов):

- не нанесет никакого ущерба – 0 баллов;
- нанесет ущерб Организации – 1 балл;
- нанесет ущерб клиентам – 1 балл;
- нанесет ущерб партнерам – 1 балл.

Краткосрочное отсутствие (неработоспособность, недоступность, выход из строя) актива (от 24 часов до 3 суток):

- не нанесет никакого ущерба – 0 баллов;
- нанесет ущерб Организации – 1 балл;
- нанесет ущерб клиентам – 1 балл;
- нанесет ущерб партнерам – 1 балл.

Среднесрочное отсутствие (неработоспособность, недоступность, выход из строя) актива (от 3 суток до 5 недель):

- не нанесет никакого ущерба – 0 баллов;
- нанесет ущерб Организации – 1 балл;
- нанесет ущерб клиентам – 1 балл;
- нанесет ущерб партнерам – 1 балл.

Длительное отсутствие актива (неработоспособность, недоступность, выход из строя) (от 5 недель до 6 месяцев):

- не нанесет никакого ущерба – 0 баллов;

- нанесет ущерб Организации – 1 балл;
- нанесет ущерб клиентам – 1 балл;
- нанесет ущерб партнерам – 1 балл.

Постоянное отсутствие актива (неработоспособность, недоступность, выход из строя) (более 6 месяцев):

- не нанесет никакого ущерба – 0 баллов;
- нанесет ущерб Организации – 1 балл;
- нанесет ущерб клиентам – 1 балл;
- нанесет ущерб партнерам – 1 балл.

При классификации должен учитываться как прямой ущерб, так и косвенный.

Ответственный за обеспечение ИБ должен определить период обеспечения защиты для каждого актива, по окончании которого он становится менее защищен. Поскольку присвоение повышенной категории может вести к ненужным дополнительным расходам.

Результатом классификации относительной ценности актива является численная величина, получающаяся суммированием определенных классов актива.

Низкая ценность актива: 0-4 баллов.

Средняя ценность актива: 5-9 баллов.

Высокая ценность актива: 10-15 баллов.

7. Классификация информации

Целью классификации информации (информационных активов) Организации является обеспечение уверенности в том, что информационные активы защищены на надлежащем уровне в соответствии с их ценностью.

В общем, классификация информации позволяет определить ее ценность, как эта информация должна быть обработана и защищена.

В Организации используется следующая система классификации:

Классификация по типу возможного носителя:

- a) информация всегда на мобильном электронном носителе;
- b) информация всегда на стационарном электронном носителе;
- c) информация всегда на стационарном и мобильном электронном носителе;
- d) информация всегда только на бумажном носителе;
- e) информация может быть на электронном носителе и бумажном носителе.

Классификация по возможности передачи:

- a) информация без права электронной передачи;
- b) информация с правом электронной передачи;

- с) информация без права передачи на бумажном носителе;
- д) информация с правом передачи на бумажном носителе;
- е) информация с правом передачи на электронном и бумажном носителе.

Классификация по доступу:

- 0. информация для открытого доступа – 0;
- 1. информация для всех авторизованных пользователей – 1;
- 2. информация для ограниченной группы авторизованных пользователей – 2;
- 3. информация, закрытая для всех, кроме ее владельца – 3;
- 4. служебная информация – 4;
- 5. информация, конфиденциальность которой описывается отдельными соглашениями со сторонними организациями или частными лицами – 5;
- 6. информация, защищаемая согласно требованиям законодательства РК – 6.

Классификация по чувствительности к нарушению конфиденциальности:

- 0. нарушение доступности не наносит ущерба ни Организации, ни третьим лицам – 0 баллов;
- 1. нарушение доступности наносит ущерб только Организации – 1 балл;
- 2. нарушение доступности наносит ущерб только третьим лицам – 2 балла;
- 3. нарушение доступности наносит ущерб только владельцу информации – 3 балла;
- 4. нарушение доступности наносит ущерб Организации и третьим лицам – 4 балла.

Классификация по чувствительности к нарушению целостности:

- 0. нарушение доступности не наносит ущерба ни Организации, ни третьим лицам – 0 баллов;
- 1. нарушение доступности наносит ущерб только Организации – 1 балл;
- 2. нарушение доступности наносит ущерб только третьим лицам – 2 балла;
- 3. нарушение доступности наносит ущерб только владельцу информации – 3 балла;
- 4. нарушение доступности наносит ущерб Организации и третьим лицам – 4 балла.

Классификация по чувствительности к нарушению доступности:

- 0. нарушение доступности не наносит ущерба ни Организации, ни третьим лицам – 0 баллов;

1. нарушение доступности наносит ущерб только Организации – 1 балл;
2. нарушение доступности наносит ущерб только третьим лицам – 2 балла;
3. нарушение доступности наносит ущерб только владельцу информации – 3 балла;
4. нарушение доступности наносит ущерб Организации и третьим лицам – 4 балла.

Классификация по критичности:

0. потеря информации не наносит ущерба ни Организации, ни третьим лицам – 0 баллов;
1. потеря информации наносит ущерб только Организации – 1 балл;
2. потеря информации наносит ущерб только третьим лицам – 2 балла;
3. потеря информации наносит ущерб только владельцу информации – 3 балла;
4. потеря информации наносит ущерб Организации и третьим лицам – 4 балла.

Коэффициенты определяют ценность информации для Организации, и определения способов и методов ее защиты.

В случае, если в рамках одной классификации информация принадлежит нескольким классам, баллы суммируются.

При классификации должен учитываться как прямой ущерб так и косвенный.

Результатом классификации относительной ценности актива является численная величина, получающаяся суммированием определенных классов актива.

Низкая ценность актива: 0-9 баллов.

Средняя ценность актива: 10-19 баллов.

Высокая ценность актива: 20-30 баллов.

Ответственный за обеспечение ИБ должен определить период обеспечения защиты для каждого информационного актива, по окончании которого информация становится менее защищаемой. Поскольку присвоение повышенной категории может вести к ненужным дополнительным расходам.

8. Маркировка и обработка активов

Серверное оборудование, рабочие станции и активное сетевое оборудование в рамках проекта ИС маркируются путем наклейки на них паспорта оборудования и инвентарного номера.

Маркировка кабелей передачи данных, и электропитания осуществляется путем сквозной нумерации и наклейки на жилу

соответствующего номера. Системный администратор обязан составить перечень всех кабелей передачи данных, и электропитания в рамках проекта ИС с указанием источника и приемника соединения и внести соответствующие записи в Журнал учета кабельных соединений (по форме Приложения 1).

Маркировка съемных носителей информации (flash-дисков, оптических дисков и др.) осуществляется путем нанесения соответствующего инвентарного номера, определенного в процессе инвентаризации.

При осуществлении вывода данных из ИС, содержащих информацию, которая должна сохранять свою конфиденциальность используется соответствующая метка на дополнительном титульном листе или на обороте титульного листа (для бумажных носителей; по форме Приложения 2) или на корпусе носителя информации (сохраненный объект, ответственный, класс по типу доступа информации). Если размеры носителя информации не позволяют нанести маркировку, то его хранение, перемещение и передача должна осуществляться в конверте, на котором должна отражаться информация по форме Приложения 3.

В маркировке следует отражать классификацию выводимой (хранимой) информации по типу доступа. Маркировке подлежат напечатанные отчеты, экранные формы, носители информации (ленты, диски), электронные сообщения и передаваемые файлы.

В соглашениях с другими организациями, которые включают обмен информацией, должны быть предусмотрены процедуры определения классификации информации и интерпретацию категорий (грифов) информации других организаций.

Маркировка и безопасная обработка важной информации является ключевым требованием в обеспечении ИБ. Физические метки являются, в общем случае, наиболее подходящей формой маркировки. Однако некоторые информационные активы, такие как документы в электронной форме, физически не могут быть промаркированы, поэтому ответственный за обеспечение ИБ разрабатывает, а руководство Организации утверждает каталог информационных активов с указанием класса информации, периода защиты и группы доступа.

9. Ответственность

СОИБ несет ответственность за:

- a) контроль исполнения требований настоящего документа,
- b) исполнение настоящей Инструкции.

Сотрудники проекта ИС:

- a) исполнение настоящей Инструкции.

Пользователи ИС:

- b) исполнение настоящей Инструкции.

Журнал учета кабельных соединений
ЗДГЕО.СМИБ.ПР.03-01.r01.19

Адрес:

Стойка (секция):

№	Конец А		Конец В	
	Оборудование	Порт	Оборудование	Порт
1	2	3	4	5

(для бумажных носителей информации)

Класс информации по типу доступа: _____

Допущенные: _____

Место хранения: _____

Период хранения: от «___» _____ 20__ г. до «___» _____ 20__ г.

**ОТВЕТСТВЕННЫЙ ЗА
СОХРАННОСТЬ**

«___» _____ 20__ г.

**ОТВЕТСТВЕННЫЙ ЗА
ОБЕСПЕЧЕНИЕ ИБ**

«___» _____ 20__ г.

(для цифровых носителей информации)

Класс информации по типу доступа: _____

Допущенные: _____

Серийный номер: _____

Инвентарный номер: _____

Место хранения: _____

Период хранения: от «___» _____ 20__ г. до «___» _____ 20__ г.

**ОТВЕТСТВЕННЫЙ ЗА
СОХРАННОСТЬ**

**ОТВЕТСТВЕННЫЙ ЗА
ОБЕСПЕЧЕНИЕ ИБ**

«___» _____ 20__ г.

«___» _____ 20__ г.

**Перечень активов и ответственных за них сотрудников
Информационной системы «3D автоматизированная геоинформационная система города Алматы»
3DGEO.СМИБ.ПР.03-04-01.r01.19**

Перечень защищаемых помещений:

[illegible]

Перечень технических активов:

№ п/п	Производитель, модель	Серийный/ инвентарный номер	Номер сертификата по информационной безопасности (при наличии)	Физическое месторасположения	Тип (согласно технической документации)	Основное функциональное назначение (согласно программной документации к объекту аттестации)	Используемые методы защиты информации	Разработчик, название, версия (встроенного программного обеспечения)	IP адреса	Ценность актива	Ответственный
1	2	3	4	5	6	7	8	9	10	11	12

Перечень дистрибутивов программных средств:

№ п/п	Разработчик	Название	Версия	Место установки (из перечня технических активов)	Тип (согласно программной документации)	Основное функциональное назначение (согласно программной документации)	Используемые методы защиты информации	Ценность актива	Ответственный
1	2	3	4	5	6	7	8	9	10

Перечень системных утилит и средств администрирования:

№ п/п	Разработчик	Название	Версия	Место установки (из перечня технических активов)	Тип (согласно программной документации)	Основное функциональное назначение (согласно программной документации)	Используемые методы защиты информации	Ценность актива	Ответственный
1	2	3	4	5	6	7	8	9	10

Перечень разрешенного программного обеспечения:

№ п/п	Разработчик	Название	Версия	Место установки (из перечня технических активов)	Тип (согласно программной документации)	Основное функциональное назначение (согласно программной документации)	Используемые методы защиты информации	Ценность актива	Ответственный
1	2	3	4	5	6	7	8	9	10

Перечень средств разработки, тестирования:

№ п/п	Разработчик	Название	Версия	Место установки (из перечня технических активов)	Тип (согласно программной документации)	Основное функциональное назначение (согласно программной документации)	Используемые методы защиты информации	Ценность актива	Ответственный
1	2	3	4	5	6	7	8	9	10

№ п/п	Разработчик	Название	Версия	Место установки (из перечня технических активов)	Тип (согласно программной документации)	Основное функциональное назначение (согласно программной документации)	Используемые методы защиты информации	Ценность актива	Ответственный
1	2	3	4	5	6	7	8	9	10

Перечень информационных активов:

№ п/п	Наименование актива	Место расположения (из перечня технических активов)	Чувствительность к нарушению конфиденциальности	Чувствительность к нарушению целостности	Чувствительность к нарушению доступности	Класс по типу возможного носителя	Класс по доступу	Класс по возможности передачи	Ответственный
1	2	3	4	5	6	7	8	9	10

Перечень приобретаемых и оказываемых услуг:

№ п/п	Наименование услуги	Место оказания услуги	Поставщик, заказчик, контактная информация	Номер и дата договора	Описание услуги	Дата начала и окончания оказания услуги	Ценность услуги (как актива)	Ответственный
1	2	3	4	5	6	7	8	9

**ПЕРЕЧЕНЬ
(мастер-лист)
документов**

**Информационной системы «3D автоматизированная геоинформационная система города Алматы»
3DGEO.СМИБ.ПР.03-04-02.r01.19**

№ п\п	Наименование актива	Место ранения	Ответственный
1	2	3	10
1.			
2.			
3.			
4.			
5.			
6.			

