КГУ «Управление архитектуры и градостроительства города Алматы»

УТВЕРЖДЕНО

Руководитель Управления архитектуры и градостроительства города Алматы

_____ Ахмеджанов А. Т.

«14» января 2019 г.

М. П.

Правила инвентаризации и паспортизации средств вычислительной техники, телекоммуникационного оборудования и программного обеспечения Информационной системы «3D автоматизированная геоинформационная система города Алматы» 3DГЕО.СМИБ.ПР.05.г01.19

г. Алматы
2019 г.

1. Область применения

Целью настоящего документа является описание правил инвентаризации и паспортизации средств вычислительной техники, телекоммуникационного оборудования и программного обеспечения 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 к средствам вычислительной техники, телекоммуникационного оборудования и программного обеспечения.

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

Все основные информационные активы Организации подлежат обязательному учету, за каждым активом закреплен ответственный сотрудник.

Ответственный за обеспечение ИБ должен составить и держать в актуальном состоянии перечень активов и ответственных за них сотрудников (по форме Приложения 4 к Правилам идентификации, классификации и маркировки активов, связанных со средствами обработки информации), обеспечивающих поддержание соответствующих мероприятий по управлению информационной безопасностью в отношении вверенных им активам.

Настоящий документ регламентирует:

1) требования к идентификации средств вычислительной техники (далее – СВТ) с учетам их ценности и важности;
2) порядок оформления паспортов СВТ;
3) требования к периодичности проведения инвентаризации и паспортизации СВТ;
4) требования к утилизации и (или) списанию СВТ, телекоммуникационного оборудования и программного обеспечения, в том числе по утилизации устройств хранения

данных и гарантированному уничтожению информации при повторном использования оборудования;

5) требования по назначению ответственных за инвентаризацию и паспортизацию СВТ;
6) требования к использованию, приобретению и учету лицензионного ПО.

Осуществление мероприятий по управлению информационной безопасностью может быть делегировано от ответственного за актив другому лицу, закрепленному приказом руководства Организации, но ответственность должна оставаться за назначенным ответственным за актив сотрудником.

5. Инвентаризация активов

Инвентаризация (учет) активов осуществляется в рамках финансово-бухгалтерского учета имущества Организации, в соответствии с утвержденными внутренними документами. В настоящем документе рассматривается только аспект инвентаризации тех активов, которые используются для обеспечения работы ИС.

Описываемый процесс инвентаризации активов может рассматриваться как расширение, либо дополнение к финансово-бухгалтерскому учету имущества Организации, проводится отдельно и никак не может его заменить.

Инвентаризация и паспортизация СВТ проводится один раз в год.

Перечень активов и ответственных за них сотрудников должен быть составлен с указанием относительной ценности и важности активов, а также данные о них должны быть документированы.

Основываясь на инвентаризации и классификации активов, Организация обеспечивает заданные уровни защиты, соответствующие ценности и важности активов.

Перечень следует составлять и поддерживать для важных активов проекта ИС. Каждый актив должен быть четко идентифицирован и классифицирован с точки зрения безопасности, ответственный за него должен быть определен и утвержден руководством Организации.

Кроме того, должно быть указано фактическое местоположение актива (это важно в случае восстановления активов при потере или повреждении), соответствующие ценности и важности актива.

Примерами активов, связанных с информационными системами, являются:

а) информационные активы: база данных и файлы данных, системная документация, руководства пользователя, учетные материалы, процедуры эксплуатации или поддержки (обслуживания), планы по обеспечению непрерывности функционирования информационного обеспечения, процедуры действий при сбоях, архивированная информация;

b) активы программного обеспечения: прикладное программное обеспечение, системное программное обеспечение, инструментальные средства разработки и утилиты;

c) физические активы: компьютерное оборудование, оборудование связи, магнитные носители и другое техническое оборудование, помещения;

d) услуги: вычислительные услуги и услуги связи, основные коммунальные услуги, например, отопление, освещение, электроэнергия, кондиционирование.

Описание активов дает уверенность в том, что обеспечивается эффективная защита активов, и оно может также потребоваться для целей обеспечения безопасности труда, охраны здоровья, страхования или решения финансовых вопросов (управление активами). Процесс составления описи активов - важный аспект управления риском (см. Методика оценки рисков информационной безопасности).

Ответственный за обеспечение ИБ обязан проводить инвентаризацию и осуществлять контроль за паспортизацией средств вычислительной техники, телекоммуникационного оборудования и программного обеспечения.

6. Порядок инвентаризации активов

Инвентаризация активов должна проводится в рамках внутреннего аудита информационной безопасности согласно утвержденного плана. Инвентаризация активов проекта ИС проводится ответственным за обеспечение ИБ.

В процессе инвентаризации выполняются следующие действия:

a) сверка наличия и соответствие заявленным характеристикам ранее учтенных активов;

b) выявление неучтенных активов;

c) выявление несанкционированных изменений активов;

d) классификация, переклассификация активов;

e) выявление активов, незакрепленных за сотрудником Организации;

f) выявление активов с незаполненными паспортами;

g) присваивание инвентарного номера;

h) маркировка активов;

i) выявление фактов несоблюдения требований утвержденных документов по информационной безопасности в отношении активов.

7. Порядок паспортизации средств вычислительной техники, телекоммуникационного оборудования, ПО и учета съемных носителей

На ответственного за обеспечение ИБ возлагается контроль за правильным и своевременным заполнением паспортов.

Сотрудники проекта ИС несут полную материальную ответственность за вверенные им СВТ, ПО (включая лицензионные ключи и оптические носители с оригинальным ПО) и съемные носители в соответствии с договором о полной материальной ответственности.

Материально-ответственные сотрудники с момента получения СВТ заполняют паспорт по форме согласно приложениям, к настоящему документу, прикрепляют копию к соответствующему оборудованию, и передают оригинал ответственному за обеспечение ИБ. В случае выполнения ремонта, модернизации, профилактики, гарантийного обслуживания материально-ответственный сотрудник должен внести соответствующую запись в паспорт СВТ.

Номер паспорта остается неизменным для СВТ.

Ответственный за обеспечение ИБ обязан составить и поддерживать в актуальном состоянии перечень выданных сотрудникам и используемых в проекте ИС съемных носителей с указанием ответственных за них лиц.

Все новые информационные ресурсы (активы) добавляются в соответствующий раздел реестра, как только они стали собственностью Организации или были переданы сторонней организацией в доверительное управление, а также удаляются из реестра, когда они выходят из использования Организации и ликвидируются.

Руководитель Организации инициирует процедуру актуализации реестра информационных активов после получения на баланс или списания с баланса Организации актива совместно с рабочей группой проводит идентификацию, классификацию и маркировку активов.

Актуализированный реестр утверждается Директором

8. Порядок передачи СВТ при увольнении сотрудника, переводе в другое структурное подразделение или уходе в длительный отпуск

Сотрудник при увольнении, переводе в другое структурное подразделение или уходе в длительный отпуск более чем на 60 дней (декретный отпуск, длительное обучение и т.д.) обязан: - передать руководителю своего подразделения необходимую служебную информацию, хранящуюся на персональном компьютере; - сдать персональный компьютер ответственному за обеспечение ИБ, в паспорте СВТ поставить отметку о сдаче персонального компьютера.

Материально-ответственное лицо проверяет высвободившийся персональный компьютер на комплектность (согласно паспорту СВТ) и передает его ответственному за обеспечение ИБ.

9. Безопасная утилизация (списание) или повторное использование оборудования и программного обеспечения

Настоящий раздел содержит требования к утилизации и (или) списанию СВТ, телекоммуникационного оборудования и программного обеспечения, в том числе по утилизации устройств хранения данных и

гарантированному уничтожению информации при повторном использования оборудования.

Все компоненты оборудования ИС (СВТ, телекоммуникационное оборудование), содержащие данных необходимо проверять на предмет удаления всех важных сведений и лицензионного программного обеспечения в случае передачи оборудования для использования третьей стороне, списания, утилизации или передачи для использования в других задачах или другим сотрудникам внутри Организации.

Все сведения должны быть удалены с носителей информации перед их утилизацией или повторном использовании.

Метод удаления должен гарантировать невозможность восстановления информации. Служебная информация может быть скомпрометирована вследствие небрежной утилизации или повторного использования оборудования.

Утилизация программного обеспечения с носителей информации (встроенных или съемных) должна проводиться методом, гарантирующим невозможность ее восстановления.

Обязанность по осуществлению контроля исполнения настоящих требований возлагается на ответственного за обеспечение ИБ.

Утилизация носителей информации

Носители информации по окончании использования следует надежно и безопасно утилизировать. Важная информация может попасть в руки посторонних лиц из-за небрежной утилизации носителей данных.

При утилизации или смены места использования носителей информации необходимо учитывать следующее:

a) носители, содержащие важную информацию, следует хранить и утилизировать надежно и безопасно (например, посредством сжигания/измельчения). Если носители информации планируется использовать в пределах организации для других задач, то информация на них должна быть уничтожена;

b) при смене места использования носителя информации, должна быть произведена смена маркировки носителя;

c) при смене места использования носителя информации должен быть указан ответственный сотрудник;

d) в случае необходимости следует прибегнуть к сторонним поставщикам услуг уничтожения носителей информации, однако процесс уничтожения должен контролироваться ответственным за обеспечение ИБ;

e) необходимо регистрировать утилизацию важных объектов с целью последующего аудита.

При накоплении носителей информации, подлежащих утилизации, применяются соответствующие меры по их защите.

Все сведения должны быть удалены с носителей информации перед их утилизацией или повторном использовании.

Метод удаления должен гарантировать невозможность восстановления информации.

Ответственный за обеспечение ИБ не должен допускать компрометации информации в результате небрежной утилизации носителей информации.

10. Описание требований к использованию, приобретению и учету лицензионного ПО

В рамках проекта ИС разрешается использовать только лицензионное программное обеспечение.

Приобретение программного обеспечения осуществляется в соответствии с законодательством РК и учредительными документами организации.

Для обеспечения информационной безопасности сотрудники проекта ИС с момента установки ПО на подотчетный компьютер или серверное оборудование предусматривают применение следующих мероприятий:

a) строгое следование требованиям авторского права на программное обеспечение, которое определяет законное использование программных и информационных продуктов;

b) соблюдение условий получения из общедоступных сетей программного обеспечения и информации;

c) устанавливать только разрешенное к установке ПО (в соответствии с перечнем разрешенного программного обеспечения).

Ответственный за обеспечение ИБ обязан осуществлять следующую деятельность:

a) консультировать сотрудников проекта ИС в вопросах лицензирования;

b) обеспечение осведомленности сотрудников по вопросам авторского права на программное обеспечение принятых правил в отношении закупок, а также уведомление о применении дисциплинарных санкций к нарушителям;

c) учитывать лицензионное ПО как актив проекта ИС в (по форме Приложения 4 к Правилам идентификации, классификации и маркировки активов, связанных со средствами обработки информации);

d) проверять (в рамках внутреннего аудита) установленное ПО на серверном оборудовании и рабочих станциях сотрудников проекта на предмет соблюдения лицензионных соглашений.

11. Ответственность

СОИБ несет ответственность за:

a) контроль исполнения требований настоящего документа,

b) исполнение настоящей Инструкции.

Сотрудники проекта ИС:

а) исполнение настоящей Инструкции.

Приложение 1

ПАСПОРТ №_____

сервера/рабочей станции

ЗДГЕО.СМИБ.ПР.05-01.г01.19

№ п/п	Производитель, модель	Серийный/ инвентарный номер	Физическое месторасположение	Тип (согласно технической документации)	Основное функциональное назначение
1	2	3	4	5	5

№ п/п	Характеристика	Значение	Примечание
1	2	3	4
1	CPU:		
2	RAM:		
3	HDD:		

Имя хоста: _____

№ п/п	Подключенные порты	Адрес	Примечание
1	2	3	4

Используемые методы защиты информации:

_____

_____

Подключенные периферийные устройства:

№ п/п	Производитель, модель	Серийный/ инвентарный номер	Тип (согласно технической документации)	Характеристики
1	2	3	4	5

МАТЕРИАЛЬНО-ОТВЕСТВЕННЫЙ

_____

_____

«____» _____ 20__ г.

ОТВЕТСТВЕННЫЙ ЗА ОБЕСПЕЧЕНИЕ ИБ

_____

_____

«____» _____ 20__ г.

Специальные замечания (ремонт, модернизация, профилактика, гарантийное обслуживание):

№ п/п	Описание	Дата	Ф.И.О, подпись ответственного
1	2	3	4

Приложение 2

ПАСПОРТ №_____

активного сетевого оборудования

ЗDГЕО.СМИБ.ПР.05-02.r01.19

№ п/п	Производитель, модель	Серийный/ инвентарный номер	Физическое месторасположение	Тип (согласно технической документации)	Основное функциональное назначение
1	2	3	4	5	6

Используемые сетевые стандарты и протоколы:

№ п/п	Характеристика	Значение
1	2	3
1	CPU:	
2	RAM:	
3	HDD:	

Имя хоста: _____

№ п/п	Подключенные порты	Адрес	Примечание
1	2	3	4

Используемые методы защиты информации:

_____

_____

МАТЕРИАЛЬНО-ОТВЕСТВЕННЫЙ

_____

_____

«____» _____ 20__ г.

ОТВЕТСТВЕННЫЙ ЗА ОБЕСПЕЧЕНИЕ ИБ

_____

_____

«____» _____ 20__ г.

Специальные замечания (ремонт, модернизация, профилактика, гарантийное обслуживание):

№ п/п	Описание	Дата	Ф.И.О, подпись ответственного
1	2	3	4