КГУ «Управление архитектуры и градостроительства города Алматы»

УТВЕРЖДЕНО

Руководитель Управления архитектуры и градостроительства города Алматы

_____ Ахмеджанов А. Т.

«14» января 2019г.

М. П.

Правила организации физической защиты средств обработки информации и безопасной среды функционирования информационных ресурсов Информационной системы «3D автоматизированная геоинформационная система города Алматы» 3DГЕО.СМИБ.ПР.13.r01.19

г. Алматы
2019 г.

1. Область применения

Целью настоящего документа является описание правил организации, физической защиты средств обработки информации и безопасной среды функционирования информационных ресурсов, 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 ИС.

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

Предотвращение несанкционированного физического доступа, повреждения и воздействия на помещения и информацию является обязательным аспектом обеспечения ИБ.

Средства обработки критичной или важной служебной информации необходимо размещать в зонах безопасности, обозначенных определенным периметром безопасности, обладающим соответствующими защитными барьерами и средствами контроля проникновения. Эти зоны должны быть физически защищены от неавторизованного доступа, повреждения и воздействия.

Контроль исполнения требований возлагается на ответственного за обеспечение ИБ.

В рамках проекта используются три защищаемых помещения:

1. рабочее помещение проекта, служащее основным местом исполнения служебных обязанностей сотрудниками проекта;
2. серверное помещение основного узла проекта;
3. серверное помещение резервного узла проекта.

Перечень защищаемых помещений проекта ИС утверждается руководством Организации (по форме Перечня активов и ответственных за них сотрудников).

5. Периметр физической безопасности

Для защиты рабочего помещения проекта применяются следующие меры:

a) периметр безопасности помещения четко ограничен, защите подлежат все активы внутри помещения;

b) периметр помещения, физически непрерывен, одну дверь и окна запираются; внешние стены помещения имеют достаточно прочную конструкцию;

c) вход в помещение только для авторизованных сотрудников проекта;

d) помещение отделено от других зон стенами от пола до потолка; ключ от двери помещения находится у ответственного за обеспечение ИБ, дубликат у руководства Организации в надежном сейфе;

e) противопожарные выходы отсутствуют;

f) помещение оснащено сигнализацией, которая проходит тестирование в соответствии с требованиями законодательства РК и договором об аренде;

g) помещение содержит только оборудование проекта.

Для защиты серверных помещений проекта применяются следующие меры:

a) периметр безопасности четко ограничен, защите подлежат все информационные активы в помещении;

b) периметр помещений, где расположены средства обработки информации, физически непрерывен, дверные и оконные проемы запираются на замки, находятся под видеонаблюдением, контролем СКУД и сигнализацией для защиты от неавторизованного доступа; внешние стены помещений имеют достаточно прочную конструкцию; все служебные входы закрыты и опечатаны;

c) на входе в охраняемый периметр предусмотрена зона регистрации посетителей. Доступ в помещения предоставляется только авторизованному персоналу;

d) охраняемые помещения, разделены физическими барьерами от пола до потолка;

e) все противопожарные выходы в периметре безопасности оборудованы аварийной сигнализацией и плотно закрываются, в соответствии с действующими нормативными документами и нормами противопожарной безопасности;

f) все охраняемые зоны оснащены сигнализацией, которая проходит тестирование в соответствии с требованиями законодательства РК и договором об аренде;

g) средства обработки информации проекта отделены от средств обработки информации, которыми управляют сторонние организации.

В случае необходимости ответственный за обеспечение ИБ может инициировать установку дополнительных средств защиты помещений проекта.

Обеспечение безопасности зданий, производственных помещений и оборудования

Для обеспечения безопасности помещений и оборудования проекта разработаны и реализованы физические меры защиты. В организации применяются следующие меры для обеспечения безопасности помещений проекта, помещений и оборудования:

a) рабочие места сотрудников и места расположения средств обработки информации соответствуют требованиям охраны здоровья и безопасности труда, действующим на территории РК;

b) серверное оборудование расположено в отдельных помещениях с ограничением доступа посторонних лиц;

c) здания с помещениями проекта не выделяются на общем фоне и обозначены лишь маркетинговыми материалами для продвижения бизнеса и не имеют очевидных вывесок вне или внутри здания, по которым можно сделать вывод о выполняемых функциях обработки информации;

d) любая информация, идентифицирующая местоположение средств обработки важной информации, не доступны посторонним лицам.

Защита от внешних угроз и угроз со стороны окружающей среды

Средства физической защиты помещений проекта учитывают возможные последствия от пожара, наводнения, землетрясения, взрыва, уличных беспорядков и других форм природного или искусственного бедствия, а также угрозы безопасности от соседних помещений.

Защита от внешних угроз и угроз со стороны окружающей среды соответствует требованиям:

a) опасные или горючие материалы хранятся на достаточном расстоянии от зоны информационной безопасности. Большие запасы бумаги для печатающих устройств не хранятся в помещениях проекта или вблизи от них;

b) резервное оборудование и носители данных располагаются на безопасном расстоянии во избежание повреждения от последствий стихийного бедствия в помещении основном узла ИС;

c) здание с помещениями проекта оснащено противопожарным оборудованием, размещенным в доступном месте.

Серверные помещения проекта оборудованы системами:

1. контроля и управления доступом;
2. обеспечения микроклимата;
3. охранной сигнализации;
4. видеонаблюдения;
5. пожарной сигнализации;
6. пожаротушения;
7. гарантированного электропитания;
8. заземления;

Отказоустойчивость инфраструктуры серверных помещений проекта составляет не менее 99,7%.

Система контроля и управления доступом серверных помещений проекта обеспечивает санкционированный вход в серверное помещение и санкционированный выход из него. Преграждающие устройства и конструкция входной двери предотвращают возможность передачи идентификаторов доступа в обратном направлении через тамбур входной двери.

Устройство центрального управления системы контроля и управления доступом серверных помещений проекта устанавливается в защищенных от доступа посторонних лиц отдельных служебных помещениях, помещении поста охраны. Доступ к программным средствам системы контроля и управления доступом, влияющим на режимы работы системы со стороны персонала охраны, исключены.

Электроснабжение системы контроля и управления доступом осуществляется от свободной группы щита дежурного освещения. Система контроля и управления доступом обеспечена резервным электропитанием.

Система обеспечения микроклимата серверных помещений проекта включает систему кондиционирования, систему вентиляции и систему мониторинга микроклимата.

Температура в серверном помещении поддерживается в диапазоне от 20 С до 25 С при относительной влажности от 45% до 55 %.

Мощность системы кондиционирования воздуха серверных помещений проекта, превышает суммарное тепловыделение всего оборудования и систем. Система кондиционирования воздуха обеспечивается резервированием. Электропитание кондиционеров серверного помещения осуществляется от системы гарантированного электропитания или системы бесперебойного электропитания.

Система вентиляции обеспечивает приток свежего воздуха с фильтрацией и подогревом поступающего воздуха в зимний период. В серверном помещении давление создается избыточным для предотвращения поступления загрязненного воздуха из соседних помещений. На воздуховодах приточной и вытяжной вентиляций устанавливаются защитные клапаны, управляемые системой пожаротушения.

Системы кондиционирования и вентиляции отключаются автоматически по сигналу пожарной сигнализации.

Система охранной сигнализации серверных помещений проекта выполнена отдельно от систем безопасности здания. Сигналы оповещения выводятся в помещение круглосуточной охраны в виде отдельного пульта. Контролю и охране подлежат все входы и выходы серверного помещения, а также внутренний объем серверного помещения. Система охранной сигнализации имеет собственный источник резервированного питания.

Расположение камер системы видеонаблюдения серверных помещений проекта, выбрано с учетом обеспечения контроля всех входов

и выходов в серверное помещение, пространства и проходов возле оборудования. Угол обзора и разрешение камер обеспечивают распознавание лиц. Изображение с камер выводятся на отдельный пульт в помещение круглосуточной охраны

Система пожарной сигнализации серверных помещений проекта выполняется отдельно от пожарной сигнализации здания. В серверных помещениях проекта устанавливаются два типа датчиков: температурные и дымовые.

Датчиками контролируются общее пространство серверных помещений проекта и объемы, образованные фальшполом и (или) фальшпотолком. Сигналы оповещения системы пожарной сигнализации выводятся на пульт в помещение круглосуточной охраны.

Система пожаротушения серверных помещений проекта оборудуется автоматической установкой газового пожаротушения, независимой от системы пожаротушения здания. В качестве огнетушителя в автоматической установке газового пожаротушения используется специальный нетоксичный газ. Порошковые и жидкостные огнетушители не используются. Установка газового пожаротушения размещается непосредственно в серверных помещениях проекта или вблизи него в специально оборудованном для этого шкафу. Запуск системы пожаротушения производится от датчиков раннего обнаружения пожара, реагирующих на появление дыма, а также от ручных датчиков, расположенных у выхода из помещения. Время задержки выпуска огнетушителя составляет не более 30 с. Оповещение о срабатывании системы пожаротушения выводится на табло, размещаемые внутри и снаружи помещения. Система пожаротушения выдает команды на закрытие защитных клапанов системы вентиляции и отключение питания оборудования. Серверное помещение, оборудованное системой пожаротушения, оснащается вытяжной вентиляцией для удаления огнегасящего газа.

Система гарантированного электропитания серверных помещений проекта предусматривает наличие двух вводов электропитания от разных источников внешнего электропитания на напряжение ~400/230В, частотой 50 Гц и автономного генератора. Все источники электроэнергии подаются на автомат ввода резерва, осуществляющий автоматическое переключение на резервный ввод электропитания при прекращении, перерыве подачи электропитания на основном вводе. Параметры линий электропитания и сечение жил определяются исходя из планируемой суммарной потребляемой мощности оборудования и подсистем серверного помещения. Линии электропитания выполняются по путепроводной схеме.

Система гарантированного электропитания предусматривает электроснабжение оборудования и систем серверного помещения через источники бесперебойного питания. Мощность и конфигурация источников бесперебойного питания рассчитываются с учетом всего запитываемого оборудования и запаса для перспективного развития. Время

автономной работы от источников бесперебойного питания рассчитывается с учетом потребностей, а также с учетом необходимого времени для перехода на резервные линии и времени запуска генератора в рабочий режим.

Система заземления серверных помещений проекта выполняется отдельно от защитного заземления здания. Все металлические части и конструкции серверного помещения заземляются с общей шиной заземления. Каждый шкаф (стойка) с оборудованием заземляется отдельным проводником, соединяемые с общей шиной заземления.

Выполнение работ в охраняемых зонах

Перечень сотрудников, допущенных в защищаемые помещения проекта утверждается приказом руководства Организации (по форме Приложение 3 Политики).

Выполнение работ в охраняемых помещениях проекта контролируется ответственным за обеспечение ИБ.

Работы в рабочих помещениях проекта проводятся каждый день. Работы в серверных помещениях проекта проводятся по необходимости. Системный администратор обязан уведомлять ответственного за обеспечение ИБ о предстоящих работах в серверных помещениях проекта

При выполнении работ в защищаемых помещениях проекта выполняются следующие требования:

a) о существовании зоны информационной безопасности и проводимых в ней работах должны быть осведомлены только лица, которым это необходимо в силу производственной необходимости;

b) из соображений безопасности и предотвращения возможности злонамеренных действий в защищаемых помещениях проекта необходимо избегать случаев работы без надлежащего контроля со стороны ответственного за обеспечение ИБ;

c) пустующие зоны безопасности должны быть физически закрыты;

d) использование фото, видео, аудио или другого записывающего оборудования, цифровых камер в мобильных устройствах запрещено.

Зоны общественного доступа, приема и отгрузки материальных ценностей

Зона общественного доступа, приемки и отгрузки материальных ценностей, защищаемых помещений проекта находиться под контролем и изолирована от средств обработки информации во избежание неавторизованного доступа.

Исполняются следующие требования при организации приема и отгрузки материальных ценностей:

a) доступ к зоне складирования разрешен только сотрудникам Организации;

b) зона складирования организована так, чтобы поступающие материальные ценности могли быть разгружены без предоставления персоналу поставщика доступа к другим частям здания;

c) обеспечена безопасность двери помещения для складирования;

d) поступающие материальные ценности осматриваются на предмет потенциальных опасностей прежде, чем они будут перемещены из помещения для складирования к местам сотрудников проекта;

e) поступающие материальные ценности регистрируются при входе в помещение, в соответствии с процедурами управления активами;

f) приемка и отгрузка материальных ценностей отдельны.

6. Безопасность оборудования

В защищаемых помещениях проекта обеспечивается безопасность оборудования, чтобы уменьшить риск неавторизованного доступа к данным, защитить их от потери или повреждения, или компрометации активов и нарушения непрерывности работы ИС.

При этом необходимо принимать во внимание особенности, связанные с расположением оборудования и возможным его перемещением.

Контроль исполнения требований безопасности в отношении оборудования возлагается на ответственного за обеспечение ИБ.

7. Размещение и защита оборудования

Средства обработки информации расположены и защищены так, чтобы уменьшить риск от воздействий окружающей среды и возможности неавторизованного доступа.

Ответственный за обеспечение ИБ осуществляет контроль мест расположения средств обработки информации, на соответствие следующим требованиям:

a) оборудование необходимо размещать таким образом, чтобы свести до минимума излишний доступ в места его расположения;

b) средства обработки и хранения важной информации следует размещать так, чтобы, уменьшить риск несанкционированного наблюдения за их функционированием;

c) отдельные элементы оборудования, требующие специальной защиты, необходимо изолировать, чтобы повысить общий уровень необходимой защиты;

d) меры по управлению информационной безопасностью, должны свести к минимуму риск потенциальных угроз, например, воровство, пожар, взрыв, задымление, затопление (или перебои в подаче воды), пыль, вибрация, химические воздействия, помехи в электроснабжении, помехи связи, электромагнитное облучение, вандализм;

e) прием пищи, напитков и курения вблизи средств обработки информации строго запрещен;

f) следует проводить мониторинг состояния окружающей среды в целях выявления условий (температура, влажность), которые могли бы неблагоприятно повлиять на функционирование средств обработки информации;

g) все здания должны быть оснащены громоотводами, а все внешние линии связи оборудованы специальными грозозащитными фильтрами;

h) следует использовать специальные средства защиты, оборудования, расположенного в производственных цехах, например, защитные пленки для клавиатуры.

8. Вспомогательные услуги

При планировании использования вспомогательных услуг ответственный за обеспечение ИБ обязан предусмотреть механизмы безотказного их оказания.

Ответственный за обеспечение ИБ должен составить и поддерживать в актуальном состоянии перечень услуг, используемых для нормальной работы активов ИС.

В перечень вспомогательных услуг входят (но не ограничиваются) следующие услуги:

- электроснабжение;
- системы поддержания климатических условий;
- водоснабжение;
- пожаротушение;
- системы контроля и управления доступом;
- услуги связи;
- ограниченные во времени договорные (например, лицензионные) соглашения;
- услуги технической, консультационной поддержки;
- услуги охраны помещений.

Все используемые вспомогательные услуги должны соответствовать требованиям активов, для которых они предназначены. Требования к вспомогательным услугам должны быть изложены в договорных соглашениях с поставщиками этих услуг или в положениях подразделений Организации, которые оказывают эти услуги.

Ответственный за обеспечение ИБ должен осуществлять контроль вспомогательных услуг на соответствие требованиям.

Чтобы обеспечить безопасное выключение и/или непрерывное функционирование устройств, поддерживающих критические бизнес-процессы, необходимо подключать оборудование через UPS.

Кроме того, для серверного оборудования необходимо использовать нескольких источников энергии от отдельно стоящих подстанций.

В серверных помещениях аварийные выключатели электропитания необходимо располагать около запасных выходов помещений, где

расположено оборудование, чтобы ускорить отключение электропитания в случае критических ситуаций. Следует обеспечить работу аварийного освещения на случай отказа электропитания, потребляемого от сети.

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

9. Безопасность кабельной сети

Силовые и телекоммуникационные кабельные сети, к которым передаются данные или осуществляются другие информационные услуги, необходимо защищать от перехвата информации или повреждения.

Прокладка силовых и телекоммуникационных каналов должна выполняться с соблюдением следующих требований:

a) силовые и телекоммуникационные линии, связывающие средства обработки информации, должны быть, защищены от неавторизованного доступа и проходить по недоступным для посторонних лиц маршрутам;

b) сетевой кабель должен быть защищен от неавторизованных подключений или повреждения, например, посредством использования специального кожуха или выбора маршрутов прокладки кабеля в обход общедоступных участков;

c) силовые кабели должны и коммуникационные должны быть покрыты изоляционным материалом для предотвращения образования помех;

d) для маркировки силовых и телекоммуникационных кабелей должна использоваться сквозная нумерация подключений в границах одного здания;

e) результаты маркировки должны документироваться и поддерживаться в актуальном состоянии системными администраторами;

f) ответственный за обеспечение ИБ должен определить необходимость использования дополнительных мер защиты каналов (выбор мер должен быть документально обоснован и утвержден руководством Организации):

1) использование бронированных кожухов, а также закрытых помещений/ящиков в промежуточных пунктах контроля и конечных точках;

2) использование дублирующих маршрутов прокладки кабеля или альтернативных способов передачи;

3) использование оптико-волоконных линий связи;

4) использование электромагнитного экранирования для защиты кабелей;

5) инициирование технических зачисток и физических осмотров для несанкционированных устройств, присоединенных к кабелям;

6) ограничение доступа к соединительным панелям и кабельным линиям.

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

10. Техническое обслуживание оборудования

Системные администраторы должны проводить надлежащее техническое обслуживание оборудования для обеспечения его непрерывной работоспособности и целостности.

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

Ответственные администраторы должны исполнять следующие требования при обслуживании оборудования:

a) оборудование необходимо обслуживать в соответствии с инструкциями и периодичностью, рекомендуемыми поставщиком;

b) необходимо, чтобы техническое обслуживание и ремонт оборудования проводились только авторизованным персоналом;

c) все работы, связанные с профилактическим и/или восстановительным техническим обслуживанием, сведения обо всех предполагаемых или фактических неисправностях необходимо документировать в журнале системно-технического обслуживания (по форме Приложения 5 Политики) и заверять подписью исполнителя и ответственного за обеспечение ИБ;

d) при отправке оборудования для технического обслуживания за пределы Организации необходимо уничтожать всю информацию надежным способом;

e) необходимо соблюдать все требования, связанные с соблюдением требований гарантийного, пост-гарантийного и лицензионного обслуживания.

f) все действия по техническому обслуживанию и администрированию серверов ИС и рабочих станций проекта необходимо регистрировать в паспортах оборудования и в журнале системно-технического обслуживания (по форме Приложения 5 Политики).

11. Обеспечение безопасности оборудования, используемого вне помещений организации

Оборудования по обработке и хранению информации включает все типы персональных компьютеров, электронных записных книжек, мобильных телефонов, смарт-карты, флэш-диски, а также бумагу или иные материальные ценности, которые используются для работы на дому или транспортируются за пределы рабочих помещений.

Работа с оборудованием вне защищаемых помещений проекта и/или удаленный доступ к ресурсам ИС строго запрещен.

12. Вынос имущества

Оборудование, информацию, программное обеспечение или другие активы можно выносить из защищаемых помещений проекта только на основании соответствующего приказа руководства Организации.

При выносе имущества должны соблюдаться следующие требования:

a) оборудование, информация, программное обеспечение или другие активы не должны вывозиться за пределы защищаемых помещений проекта без соответствующего разрешения.

b) приказом руководства Организации должны быть определены права лица с правом на вывоз активов за пределы защищаемых помещений проекта;

c) приказом необходимо установить лимит времени для вывоза оборудования и соблюдения условий возврата;

d) оборудование следует регистрировать при выносе и при вносе, а также делать отметку, когда оно возвращено в журнале системно-технического обслуживания (по форме Приложения 5 Политики).

Обязанность по осуществлению контроля исполнения настоящих требований возлагается на ответственного за обеспечение ИБ. Менеджер проекта должен выступать инициатором манипуляций с вверенными ему активами.

Руководство Организации или ответственный за обеспечение ИБ могут инициировать выборочные проверки используемого оборудования с целью выявления несанкционированного вноса. Сотрудники проекта должны быть осведомлены о выборочной проверке, и эти проверки должны осуществляться только в соответствии с правовыми и нормативными требованиями, принятыми на территории Республики Казахстан.

Требования к безопасной утилизации или повторному использованию оборудования в соответствии

Оборудование 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 оборудования 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, должна быть произведена смена маркировки носителя;

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

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

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

При накоплении оборудования, подлежащих утилизации, следует применять соответствующие меры по их защите.

В случае повторно использования оборудования все идентификационные и служебные данных (за исключением данных установленных производителем) должны быть надежно удалены.

Ответственный за обеспечение ИБ не должен допускать компрометации информации в результате небрежной утилизации и/или повторного использования оборудования (см. пп. 9.2.6, информация об утилизации использованного оборудования Политики ИБ).

13. Ответственность

СОИБ несет ответственность за:

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

Сотрудники проекта ИС:

a) исполнение настоящей Инструкции.

Пользователи ИС:

a) исполнение настоящей Инструкции.