

**КГУ «Управление архитектуры, градостроительства и земельных  
отношений города Нур-Султан»**

**УТВЕРЖДЕНО**

**Директор ТОО  
«АстанаГорАрхитектура» города  
Нур-Султан**




\_\_\_\_\_ Кенжебеков Н. К.



« 19 » \_\_\_\_\_ 2020 г.

**УТВЕРЖДЕНО**

**Руководитель Управления  
архитектуры, градостроительства и  
земельных отношений города  
Нур-Султан**



\_\_\_\_\_ Уранхаев Н. Т.



« 19 » \_\_\_\_\_ 2020 г.

**Правила разграничения прав доступа к электронным ресурсам  
Информационной системы «Геоинформационный портал  
города Нур-Султан»**

**ГПГ.СМИБ.ПР.08.r02.20**

**г. Нур-Султан  
2020 г.**

## **1. Область применения**

Целью настоящего документа является описание правил разграничения прав доступа к электронным ресурсам объекта аттестации, 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**

Доступ к информации и бизнес-процессам должен быть контролируемым с учетом требований бизнеса и безопасности.

Настоящий документ и Матрица доступа ИС однозначно определяют права и обязанности каждого пользователя или группы пользователей.

Физический контроль доступа описан в Правилах организации, физической защиты средств обработки информации и безопасной среды функционирования информационных ресурсов ИС. Пользователи ИС и поставщики услуг должны быть оповещены о необходимости выполнения требований в отношении доступа к ИС.

## **5. Классификация доступа**

В рамках проекта принята следующая классификация доступа к активам ИС.

По типу доступа:

1. удаленный;
2. локальный;
3. физический.

По набору привилегий:

1. чтение;
2. запись (создание);
3. удаление;
4. изменение (редактирование).

По способу аутентификации:

1. логин/пароль;
2. криптографический ключ;
3. ЭЦП НУЦ РК.
4. По документальной идентификации личности (удостоверение личности, служебное удостоверение)

По применяемому алгоритму шифрования:

1. без шифрования;
2. RSA;
3. ГОСТ 28147-89;
4. AES.

Удаленный доступ осуществляется с использованием шифрования трафика.

Доступ предоставляется только после аутентификации и авторизации пользователя.

Аутентификация пользователя происходит с использованием пароля и/или, ключа и/или ЭЦП или их комбинацией.

## **6. Управление доступом пользователей**

Настоящий документ охватывает все стадии жизненного цикла пользовательского доступа от начальной регистрации новых пользователей до конечного снятия с регистрации пользователей, которым больше не требуется доступ к информационным системам и сервисам. Особое внимание уделено мероприятиям в отношении предоставления прав привилегированного доступа, с помощью которых пользователи могут обходить системные средства контроля.

### **Регистрация пользователей**

Функционал ИС и организационные меры информационной безопасности обеспечивают:

- а) использование уникальных ID (идентификаторов или имен) пользователей, таким образом, чтобы действия в системе можно было бы соотнести с пользователями и установить ответственных;
- б) проверку того, что пользователь имеет авторизацию от владельца системы на использование информационной системы или сервисов;
- в) проверку того, что уровень предоставленного доступа соответствует производственной необходимости, а также учитывает требования политики безопасности ИС;
- г) предоставление пользователям письменного документа, в котором указаны их права доступа;
- е) требование того, чтобы пользователи подписывали документ о том, что они понимают условия предоставления доступа;

f) обеспечивает не предоставление доступа, пока процедура авторизации не завершена;

g) ведение формализованного учета в отношении всех лиц, зарегистрированных для использования информации ИС;

h) немедленную отмену прав доступа пользователей, у которых изменились должностные обязанности или уволившись из организации;

i) периодическую проверку и удаление избыточных пользовательских ID и учетных записей;

j) обеспечение того, что избыточные пользовательские учетные записи не передаются другим пользователям.

Все пользователи ИС подлежат обязательному учету по средствам регистрации в ИС. Все зарегистрированные пользователи должны иметь уникальные, персональные учетные записи.

Права пользователей объединены в роли и описаны в Матрице доступа (по форме Приложения 1).

### **Процедура регистрации пользователей ИС**

После заключения договора с заказчиком о предоставлении доступа к ИС, системный администратор проводит соответствующие работы для установки и настройки нового экземпляра базы данных. Доступ к новому экземпляру ИС из сети Интернет не предоставляется.

Ответственный за обеспечение ИБ подготавливает рабочие экземпляры (электронные и бумажные) НТД по ИБ и журнала ознакомления с документацией для заказчика. Менеджер проекта подготавливает рабочие экземпляры (электронные и бумажные) программно-технической документации ИС.

После окончания подготовительных работ системный администратор устно уведомляет ответственного за обеспечение ИБ о готовности.

Менеджер проекта и ответственный за обеспечение ИБ направляются к заказчику для проведения подготовки пользователей и первичной инициализации ИС.

Менеджер проекта проводит:

a) обучение использованию ИС сотрудников заказчика;

b) ознакомление сотрудников заказчика с программно-технической документацией ИС с обязательной отметкой в журнале ознакомления с документацией.

Ответственный за обеспечение ИБ проводит:

a) инструктаж по обеспечению информационной безопасности ИС сотрудников заказчика;

b) ознакомление сотрудников заказчика с НТД по ИБ с обязательной отметкой в журнале ознакомления с документацией.

Журнал ознакомления с документацией остается у заказчика для дальнейшего заполнения.

Руководство организации заказчика назначает приказом администратора ИС и сотрудника отдела кадров из сотрудников заказчика.

После подготовки пользователей, ответственный за обеспечение ИБ устно уведомляет системного администратора о готовности провести первичную инициализацию ИС. Для этого СОИБ сообщает системному администратору внешний IP-адрес сети, из которой будет проведена инициализация ИС.

Системный администратор открывает доступ к ИС из сети Интернет только для указанного IP-адреса.

Администратор ИС в соответствии с Руководством администратора по сопровождению ИС устанавливает логин и пароль для своей учетной записи, проводит первичную инициализацию ИС и регистрации ответственного сотрудника отдела кадров, и установку ему временного пароля.

Ответственный сотрудник отдела кадров обязан сменить временный пароль при первом входе в ИС.

В дальнейшем ответственный сотрудник отдела кадров самостоятельно регистрирует сотрудников заказчика и назначает им привилегии (роли) в соответствии с их должностными обязанностями.

После проведения первичной инициализации ИС ответственный за обеспечение ИБ сообщает системному администратору о необходимости снятия установленных ограничений на подключения к ИС.

После проведения первичной инициализации ИС сотрудники проекта имеют доступ к ИС в соответствии с Матрицей доступа к активам ИС.

Регистрация системных администраторов, ответственного за обеспечение ИБ, менеджера проекта проводится на основании приказа руководства Организации о назначении на должность с привилегиями в соответствии с Матрицей доступа к активам ИС.

### **Управление привилегиями**

Привилегии пользователей и сотрудников проекта устанавливаются строго по Матрице доступа к активам ИС в соответствии с их должностными обязанностями.

При этом применяются следующие меры:

- а) идентифицированы привилегии доступа в отношении каждого актива ИС: ОС, сервер приложений, средства защиты, СУБД и т. д.;
- б) используемые привилегии ограничены только теми, которые необходимы пользователю для работы;
- в) привилегии не предоставляются до завершения процесса авторизации, учитываются и регистрируются в ИС;
- г) на усмотрение ответственного за обеспечение ИБ могут быть автоматизированы функции системного администратора при помощи мобильного кода, вместо предоставления дополнительных привилегий;

- е) на усмотрение ответственного за обеспечение ИБ могут быть автоматизированы функции системного администратора при помощи специальных утилит, вместо предоставления дополнительных привилегий;
- ф) используются различные идентификаторы (ID) пользователей при работе в обычном режиме и с использованием привилегий.

В случае возникновения необходимости выделить роль с привилегиями, не входящими в Матрицу доступа к активам ИС, ответственный за обеспечение ИБ обязан инициировать пересмотр матрицы доступа.

Установка привилегий сотрудников проекта, проводится ответственным за обеспечение ИБ.

Установка привилегий сотрудников заказчика проводится ответственным сотрудником отдела кадров.

### **Пересмотр прав доступа пользователей**

Ответственный за обеспечение ИБ обязан осуществлять пересмотр прав сотрудников проекта в процессе внутреннего аудита.

Для пересмотра прав доступа должны проводиться следующие мероприятия:

- а) права доступа пользователей должны пересматриваться регулярно (рекомендуемый период - 6 месяцев) и после любых изменений, таких как продвижение по службе, понижение или увольнение с работы;
- б) права доступа пользователей должны подлежать пересмотру и перераспределяться при изменении обязанностей пользователя;
- с) проверка прав привилегированных пользователей должна осуществляться в рамках внутреннего аудита;
- д) предоставление привилегий должны проверяться в рамках внутреннего аудита для обеспечения уверенности в том, что не были получены неавторизованные привилегии;
- е) изменения привилегий учетных записей должны регистрироваться в журнале авторизации пользователей ИС и ее компонентов (ОС, сервере приложений, СУБД и др.).

Ответственный сотрудник отдела кадров обязан осуществлять пересмотр прав пользователей ИС каждые шесть месяцев с начала подписания договора. Результаты пересмотра должны оформляться в виде отчета и предоставляться руководству организации заказчика.

### **Требования по блокировке учетной записи**

Учетная запись пользователя подлежит обязательной блокировке в следующих случаях:

- а) выявления факта компрометации учетных данных пользователя или сотрудника проекта;
- б) выявление факта несанкционированного доступа с использованием учетных данных пользователя или сотрудника проекта;

- с) перерыв в работе пользователя или сотрудника проекта на срок более 15 дней;
- d) смена должностных обязанностей;
- е) перевод или освобождение от занимаемой должности;
- f) более трех неудачных попыток ввода пароля.

## **7. Ответственность пользователей**

Пользователи и сотрудники проекта должны быть осведомлены о своих обязанностях по использованию эффективных мероприятий по управлению доступом, в частности, в отношении паролей и безопасности оборудования, с которым они работают. Для снижения рисков неавторизованного доступа или повреждения документов, носителей и средств обработки информации применяется политика чистого стола и чистого экрана.

Пользователям строго запрещено разглашать, передавать другим лицам свои персональные учетные записи, логины и другие сведения, выданные для работы в ИС.

Каждый пользователь несет персональную ответственность за разглашение сведений.

В случае компрометации (или подозрения на таковую) информации пользователь ИС обязан уведомить об этом СОИБ и своего непосредственного руководителя.

### **Оборудование, оставленное пользователем без присмотра**

Всем пользователям и сотрудникам проекта необходимо соблюдать требования безопасности и методы защиты оставленного без присмотра оборудования так же, как и свои обязанности по обеспечению такой защиты.

Пользователям рекомендуется:

- a) завершать активные сеансы по окончании работы, если отсутствует механизм блокировки, например, хранитель экрана, защищенный паролем;
- b) отключаться от ИС и серверов, когда сеанс закончен;
- с) защищать рабочие станции от неавторизованного использования посредством пароля, когда оборудование не используется.

Все оборудование и ПО, включая рабочие станции пользователей и сотрудников проекта, должны быть, защищены паролем от неавторизованного доступа, когда не используются.

### **Политика «чистого стола» и «чистого экрана»**

Политика «чистого стола» и «чистого экрана» сокращает риски неавторизованного доступа, потери или повреждения информации как во время рабочего дня, так и при внеурочной работе. Если носители информации заперты в несгораемых сейфах, шкафах или в других

безопасных местах хранения, то могут быть сохранены при бедствии, например, при пожаре, землетрясении, наводнении или взрыве.

Пользователи и сотрудники проекта должны соблюдать политику «чистого стола» и «чистого экрана», а именно учитывать следующие мероприятия:

- а) носители с важной или критичной служебной информацией, когда они не требуются, следует убирать в защищенное место, особенно когда помещение пусто;
- б) персональные компьютеры, компьютерные терминалы и принтеры должны быть выключены по окончании работы;
- в) доступ в помещение проекта должен удовлетворять требованиям Правил организации, физической защиты средств обработки информации и безопасной среды функционирования информационных ресурсов ИС;
- г) рабочие помещения пользователей должны охраняться;
- д) напечатанные документы с важной или конфиденциальной информацией необходимо изымать из принтеров немедленно.

## **8. Контроль сетевого доступа**

Доступ к серверам ИС, доступ сотрудников проекта к сети проекта и сети Интернет контролируется и защищен межсетевым экраном.

### **Политика в отношении использования сетевых услуг**

Сотрудники проекта имеют доступ к сети проекта и сети Интернет. Сеть проекта отделена от сети Организации для предотвращения несанкционированного доступа.

Доступ к серверам по сети для осуществления обслуживания осуществляется строго по зашифрованному каналу виртуальной частной сети с использованием криптографических ключей персональной аутентификации сотрудников проекта.

### **Аутентификация пользователей для внешних соединений**

Аутентификация удаленного доступа к серверам для их обслуживания достигается путем использования средств криптографии с использованием виртуальной частной сети (VPN).

Аутентификация серверов ИС происходит по их уникальному IP-адресу.

Сотрудникам проекта запрещено использовать беспроводные сети и мобильные технологии для доступа к сети проекта, сети Интернет и серверам ИС или другим сетям.

Сотрудникам проекта запрещено автоматизировать ввод паролей, ключей и других идентификаторов при подключении к серверам ИС.



### **Идентификация оборудования в сетях**

Аутентификация серверов ИС происходит по их уникальному IP-адресу. Для обеспечения повышенной защищенности серверов в процессе работы и предотвращение несанкционированного подключения в свободные порты сервера используются статическая таблица MAC-адресов протокола ARP, что позволяет не допустить несанкционированные подключения.

Системному администратору ИС запрещено разглашать MAC-адреса серверного оборудования ИС.

### **Защита диагностических и конфигурационных портов при удаленном доступе**

Для обеспечения повышенной защищенности серверов в процессе работы и предотвращение несанкционированного подключения в свободные порты сервера используются статическая таблица MAC-адресов протокола ARP, что позволяет не допустить несанкционированные подключения.

Системному администратору ИС запрещено разглашать MAC-адреса серверного оборудования ИС.

### **Принцип разделения в сетях**

Сотрудники проекта имеют доступ к сети проекта и сети Интернет. Сеть проекта отделена от сети Организации для предотвращения несанкционированного доступа.

Сотрудникам проекта запрещено использовать беспроводные сети и мобильные технологии для доступа к сети проекта, сети Интернет и серверам ИС или другим сетям.

### **Контроль сетевых соединений**

Сотрудникам проекта запрещено использовать беспроводные сети и мобильные технологии для доступа к сети проекта, сети Интернет и серверам ИС или другим сетям.

Доступ к серверам ИС, доступ сотрудников проекта к сети проекта и сети Интернет контролируется и защищен межсетевым экраном.

Межсетевой экран выполняет функции:

- 1) фаервола;
- 2) фильтрации пакетов;
- 3) обнаружения и предотвращения вторжений;
- 4) фильтрацию доступа к запрещенным Интернет-ресурсам;
- 5) потокового антивируса.

Сеть проекта отделена от сети Организации для предотвращения несанкционированного доступа.

### **Управление маршрутизацией сети**

Обеспечение информационной безопасности при осуществлении маршрутизации основывается на надежном механизме контроля адресов источника и назначения сообщения.

Межсетевые экраны безопасности используются для проверки адреса источника и назначения на внутренние и внешние сети опорных точек, использующих прокси-сервер и/или сетевые технологии трансляции адресов.

Доступ к серверам ИС, доступ сотрудников проекта к сети проекта и сети Интернет контролируется и защищен межсетевым экраном с поддержкой маршрутизации.

### **9. Контроль доступа к операционной системе**

На уровне операционной системы используются встроенные средства информационной безопасности для ограничения доступа к компьютерным ресурсам. Эти средства обеспечивают:

- а) аутентификацию авторизованным пользователям, в соответствии с требованиями настоящего документа;
- б) запись успешных и неудавшихся доступов в системе;
- с) регистрацию использования специальных привилегий системы;
- д) оповещение ответственного за обеспечение ИБ в случае нарушения политики безопасности системы;
- е) обеспечение надежных средств для аутентификации;
- ф) ограничение времени подключения пользователей.

### **Безопасные процедуры регистрации с терминала**

Контроль доступа к операционным системам должен, обеспечен безопасной процедурой регистрации.

Процедура регистрации в ОС происходит внутри зашифрованного канала с использованием протокола шифрования SSH. Процедура регистрации должна:

- а) не отображать наименований системы или приложений, пока процесс регистрации не будет успешно завершен;
- б) отображать общие уведомления, предупреждающее, что доступ к компьютеру могут получить только авторизованные пользователи;
- с) не предоставлять сообщений-подсказок в течение процедуры регистрации, которые могли бы помочь неавторизованному пользователю;
- д) подтверждать информацию регистрации только по завершении ввода всех входных данных. В случае ошибочного ввода система не показывает, какая часть данных является правильной или неправильной;
- е) ограничивать число разрешенных неудачных попыток регистрации до трех и предусматривать:
  - 1) запись неудачных и удачных попыток;

- 2) включение временной задержки прежде, чем будут разрешены дальнейшие попытки регистрации, или отклонение любых дальнейших попыток регистрации без специальной авторизации;
- 3) разъединение сеанса связи при передаче данных;
- 4) отправление тревожных сообщений на консоль (терминал), если достигнуто максимальное число попыток регистрации;
- 5) исполнять требования настоящего документа к надежности паролей;
- г) ограничивать максимальное и минимальное время, разрешённое для процедуры регистрации. Если оно превышено, система должна прекратить регистрацию;
- г) фиксировать информацию в отношении успешной завершённой регистрации:
  - 1) дату и время предыдущей успешной регистрации;
  - 2) детали любых неудачных попыток регистрации, начиная с последней успешной регистрации;
  - h) не показывать введенный пароль или скрыть пароль символами;
  - и) не передавать пароли по сети открытым текстом.

### **Использование системных утилит**

Системный администратор ИС должен составить, согласовать с ответственным за обеспечение ИБ, утвердить руководством Организации и поддерживать в актуальном состоянии перечень системных утилит (по форме приложения 1), предназначенных для поддержания серверного, сетевого оборудования ИС и рабочих станций проекта.

Для обеспечения безопасного использования системных утилит необходимо выполнение следующих мероприятий:

- а) использование процедур идентификации, аутентификации и авторизации пользователей системных утилит, а также идентификация самих системных утилит перед использованием;
- б) отделение системных утилит от прикладных программ;
- с) ограничение использования системных утилит путем выбора минимального числа доверенных авторизованных пользователей;
- д) авторизация эпизодического использования системных утилит;
- е) ограничение доступности системных утилит, например, на время внесения авторизованных изменений;
- г) регистрация использования всех системных утилит;
- г) определение и документирование уровней авторизации в отношении системных утилит в Матрице доступа к активам ИС;
- h) удаление или отключение всех ненужных утилит из системного программного обеспечения;
- и) ограничение доступности использования системных утилит пользователями, имеющим доступ к прикладным системам, где требуется разделение режимов работы.

### **Периоды бездействия в сеансах связи**

Все сеансы связи отключаются после десятиминутного периода бездействия.

Механизм блокировки по времени обеспечивает очистку экрана, а также закрытие работы сеансов приложения и сетевого сеанса оборудования. Время срабатывания блокировки устанавливается с учетом рисков безопасности, классификации обрабатываемой информации и используемых приложений, связанных с местом установки оборудования.

Некоторые персональные компьютеры обеспечивают ограниченную возможность блокировки оборудования по времени путем очистки экрана и предотвращения несанкционированного доступа, не осуществляя при этом закрытия сеанса приложений и сетевого сеанса.

### **Ограничение времени соединения**

Функционал ИС и ее компонент позволяет использовать следующие меры для ограничения времени соединения:

- а) использование заранее определенных отрезков времени, например, для пакетной передачи файлов или регулярных интерактивных сеансов небольшой продолжительности;
- б) ограничение времени подключений часами работы организации, если нет необходимости сверхурочной или более продолжительной работы;
- с) повторная аутентификация в равные промежутки времени.

Функционал включается системным администратором по письменному запросу пользователя.

### **10. Контроль доступа к прикладным системам и информации**

Для обеспечения информационной безопасности применяют меры ограничения доступа к прикладным системам и информации. Логический доступ к программному обеспечению информации ограничен только авторизованными пользователями.

Для этого обеспечивается:

- а) контроль доступа пользователей к информации и функциям бизнес-приложений, в соответствии с определенной бизнес политикой контроля доступа;
- б) защиту от несанкционированного доступа любой утилиты и системного программного обеспечения, вредоносного программного обеспечения, которые позволяют обходить средства операционной системы или приложений;
- с) исключение компрометации безопасности других систем, совместно с которыми используются информационные ресурсы.

## **Ограничение доступа к информации**

Пользователям ИС, включая персонал поддержки и эксплуатации, обеспечивается доступ к информации и функциям ИС в соответствии с их должностными обязанностями.

Ограничения доступа основаны на требованиях к безопасности ИС и ее компонентов.

Применяются следующие мероприятия по управлению информационной безопасностью для обеспечения требований по ограничению доступа:

- а) контроль доступа к прикладным функциям системы;
- б) классификация и контроль прав доступа пользователей по ролям;
- в) контроль права доступа других прикладных программ и системных утилит;
- г) обеспечение уверенности в том, что выводимые данные из ИС, обрабатывающие важную информацию, содержат только требуемую информацию и пересылались в соответствии с установленным уровнем безопасности. Анализ процесса вывода информации, процесса проверки удаления избыточной информации проводится в рамках внутреннего аудита.

## **Изоляция систем, обрабатывающих важную информацию**

ИС и сотрудники проекта обеспечены выделенной (изолированной) вычислительной средой.

Для изоляции используется следующее:

- а) определена ценность каждого актива ИС и необходимость отделения ИС, и сотрудники проекта в изолированные сети;
- б) вычислительная среда и ресурсы ИС и сотрудников проекта отделены от оставшейся Организации и других сетей.

## **11. Ответственность**

СОИБ несет ответственность за:

- а) контроль исполнения требований настоящего документа,
- б) исполнение настоящей Инструкции.

Сотрудники проекта ИС:

- а) исполнение настоящей Инструкции.

Пользователи ИС:

- а) исполнение настоящей Инструкции.

**Матрица доступа к активам**  
**Информационной системы «Геоинформационный портал**  
**города Нур-Султан»**  
**ГП.СМИБ.ПР.08-01.г02.20**

Набор привилегий: С – создание; Ч – чтение; У – удаление; Р – редактирование; ТО – техническое обслуживание, КБ – контроль безопасности, ПСО – прочие служебные обязанности.													
Тип доступа: 1 - удаленный; 2 – локальный; 3 – физический, 0 – нет доступа.													
Способ аутентификации: УЛ – доступ при предъявлении уд. личности, ЛП – логин, пароль, К – RSA ключи, ЭЦП.													
X – неприменимо.													
№ п/п	Наименование актива	Роль 1				Роль 2				Роль 3			
		Тип доступа	Набор привилегий	Способ аутентификации	Алгоритм шифрования	Тип доступа	Набор привилегий	Способ аутентификации	Алгоритм шифрования	Тип доступа	Набор привилегий	Способ аутентификации	Алгоритм шифрования
1	2	3	4	5	6	7	8	9	10	11	12	13	14