

Приложение 7
к распоряжению Администрации
городского округа Химки
Московской области
от 30.09.2021 № 56-р

**ПРОЕКТ ОПИСАНИЯ
ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА ОБРАБОТКИ ИНФОРМАЦИИ В
СЕКМЕНТЕ ЕИСОУ**

«УТВЕРЖДАЮ»

(наименование должности, фамилия, инициалы)

печатъ

«__» _____ 20__ года

**ЕДИНАЯ ИНФОРМАЦИОННАЯ СИСТЕМА ОКАЗАНИЯ
ГОСУДАРСТВЕННЫХ И МУНИЦИПАЛЬНЫХ УСЛУГ
МОСКОВСКОЙ ОБЛАСТИ
(ЕИСОУ)**

**ОПИСАНИЕ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА
ОБРАБОТКИ ИНФОРМАЦИИ
В СЕКМЕНТЕ ЕИСОУ «_____»**

ОГЛАВЛЕНИЕ

1. Общие положения.....	3
2. Описание процесса.....	4
3. Подготовка АРМ к работе.....	7
4. Описание реализованных правил разграничения доступа.....	8

Общие положения

В настоящем документе описан технологический процесс обработки персональных данных на объекте вычислительной техники – Сегменте «____» ЕИСОУ (далее – Сегмент).

Описание процесса

В процессе обработки информации на объекте вычислительной техники – Сегменте «___» ЕИСОУ участвуют следующие группы пользователей:

Администратор информационной безопасности – обладает всей полнотой доступа к ресурсам объекта вычислительной техники (ОВТ), организует и контролирует работу ОВТ объектов информатизации, других пользователей.

Пользователи – имеющие доступ к АРМ объектов информатизации на основании приказа о допуске к АРМ.

Перечень объектов доступа:

жесткие магнитные диски (ЖМД);

гибкие магнитные диски (ГМД);

оптические диски (CD-ROM);

штатное программное обеспечение (ПО).

Перечень субъектов доступа: администратор информационной безопасности, пользователи. К работе в автоматизированной системе объектов вычислительной техники (далее – ОВТ) допускаются только сотрудники в соответствии с утвержденной «Разрешительной системой доступа к информационным (программным) ресурсам объекта вычислительной техники» – Сегменте «___» ЕИСОУ, допущенные к обработке персональных данных (далее - информации) и зарегистрированные в установленной системе защиты информации от несанкционированного доступа (далее – СЗИ НСД) «Secret Net 7.0» и после изучения организационно-распорядительной документации Сегмента. Схема информационных потоков на рисунках ниже.

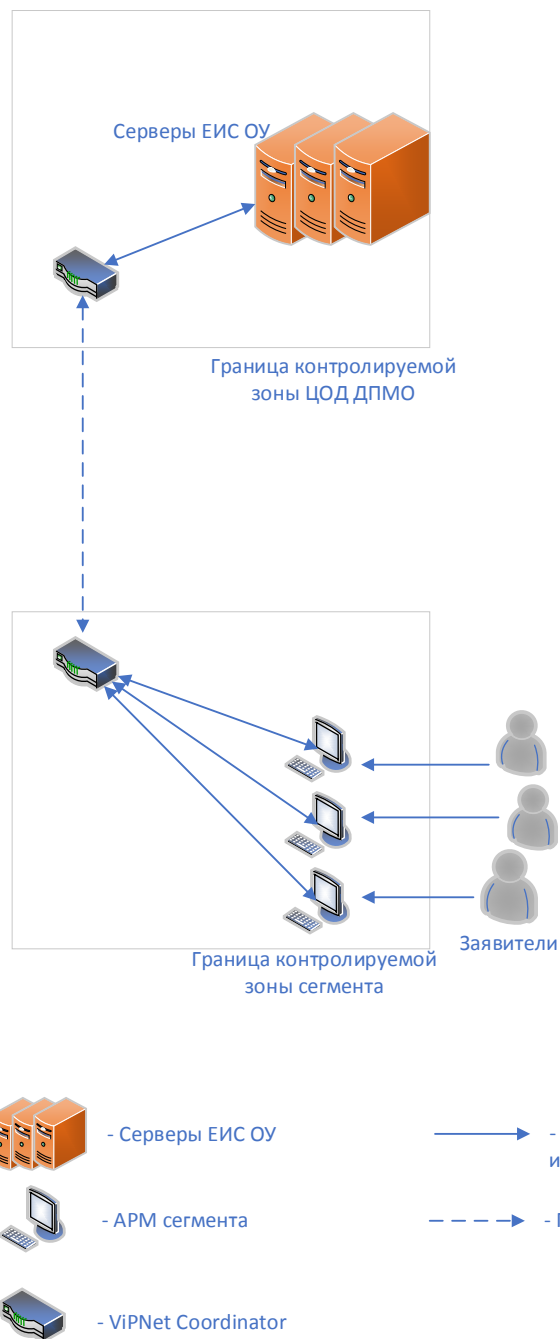


Рисунок 1. Схема информационных потоков при оказании Услуг с использованием ViPNet Coordinator.

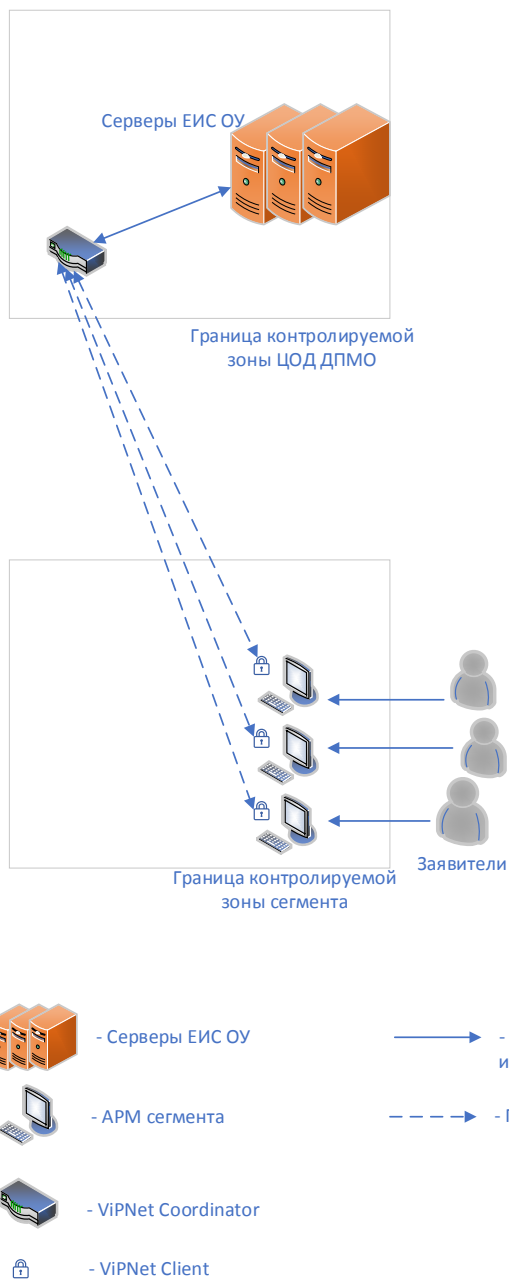


Рисунок 2. Схема информационных потоков при оказании Услуг с использованием ViPNet Client.

Подготовка АРМ к работе

Включить АРМ, для чего: подключить сетевые шнуры электропитания к сети 220 В. Включить источник бесперебойного питания, включить системный блок и монитор. После запроса системы необходимо предъявить персональный идентификатор и набрать персональный пароль на клавиатуре.

При отсутствии НСД произойдет загрузка операционной системы Windows. При нарушении или сбое системы защиты от НСД и при отказе загрузки операционной системы - прекратить работу и пригласить администратора информационной безопасности.

Запустить программу антивирусного контроля и проверить жесткий диск и используемые съемные носители на наличие вирусов.

Перечень штатных средств доступа к информации на ОВТ:
Microsoft Windows XP Лиц. № _____ SN _____;
Adobe Acrobat Reader _____; Антивирус Касперского № _____;
Microsoft Windows Office _____ Лиц. № _____ SN- _____;
Архиватор WinRAR _____ № _____; Файловый менеджер Far _____ -
; Программа записи оптических дисков Nero _____ Ultra Edition; СЗИ
НСД «Secret Net _____ –С» № _____.

На ОВТ разрешается обработка персональных данных и общедоступной информации.

Если во время работы на АРМ появилась необходимость временно покинуть рабочее место, исполнитель обязан заблокировать АРМ, для чего нужно нажать комбинацию клавиш <Ctrl-Alt-Del> и выбрать в диалоговом окне кнопку «Блокировать». Разблокирование АРМ производится набором пароля разблокировки, который был создан при настройке системы блокировки.

Описание реализованных правил разграничения доступа

Обработка информации осуществляется только на предварительно учтенных носителях информации (защищаемых ресурсах – ЖМД, гибкие магнитные диски (ГМД), прошедших антивирусный контроль, причем каждый исполнитель для обработки информации использует только свой профиль пользователя, в котором администратором закреплены правила разграничения доступа: возможность доступа к дискам, папкам и файлам, возможность записи и чтения информации и т.д.

Администратор организует и контролирует доступ пользователей к доступным ресурсам АРМ и состояние информации на носителях.

По окончании рабочего дня все съемные учтенные носители информации, документы и материалы запираются в сейфе, либо сдаются на хранение ответственному за защиту информации.

Пользователи обязаны предъявлять, по требованию ответственного за защиту информации, для проверки все числящиеся за ними носители информации.

Пользователю ЗАПРЕЩАЕТСЯ:

обрабатывать информацию при наличии оснований полагать, что информация может быть просмотрена посторонними лицами;

записывать информацию на неучтенных носителях информации, листах бумаги и т. д.;

использовать в работе пароли, если есть подозрение об их компрометации;

разглашать сведения о применяемой системе защиты и содержании информации;

изменять и тиражировать программное обеспечение;

вводить персональные данные под диктовку;

производить передачу персональных данных по каналам связи, имеющим выход за пределы контролируемой зоны Сегмента, без использования средств криптографической защиты;

производить печать персональных данных при помощи не предназначенного для этого принтера.

Ответственный за
защиту информации

_____ (подпись)

_____ (И.О. Фамилия)