Приложение 5
к распоряжению Администрации
городского округа Химки
Московской области
от 30.09.2021 № 56-р

**ПРОЕКТ ИНСТРУКЦИИ
АДМИНИСТРАТОРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
СЕГМЕНТА**

УТВЕРЖДАЮ

Руководитель

_____ *И.О. Фамилия*
от «___» _____20___г. №____

ИНСТРУКЦИЯ АДМИНИСТРАТОРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕГМЕНТА «___» ЕИСОУ

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая инструкция определяет задачи, обязанности, права и ответственность должностного лица (далее – администратора ИБ), ответственного за обеспечение безопасности информации (в том числе персональных данных (далее – ПДн)), обрабатываемой в Сегменте «___» (далее – Сегмент) Единой информационной системе оказания государственных и муниципальных услуг Московской области (далее – Система) _____ (далее – Организация).

1.2. Администратор ИБ назначается приказом руководителя из числа штатных подготовленных работников подразделения информационной безопасности (далее – ИБ) Организации, по представлению

начальника подразделения ИБ и согласованию с начальником подразделения информатизации (далее – ИТ).

1.3. Администратор ИБ подчиняется руководителю подразделения ИБ, назначаемым ответственным за обеспечение безопасности информации в Организации.

1.4. Администратор ИБ руководствуется локальными документами Организации и настоящей инструкцией.

1.5. Администратор ИБ координирует и контролирует работу системных администраторов по вопросам информационной безопасности на основании инструкции системного администратора и настоящей инструкции.

1.6. Администратор ИБ отвечает за поддержание установленного уровня безопасности защищаемой информации, в том числе ПДн, при их обработке в Сегменте.

1.7. Администратор ИБ осуществляет методическое руководство деятельностью пользователей Сегмента в вопросах обеспечения безопасности информации.

1.8. Требования администратора ИБ, связанные с выполнением им своих обязанностей, обязательны для исполнения всеми пользователями Сегмента.

1.9. Администратор ИБ несет персональную ответственность за качество проводимых им работ в части осуществления контроля действий пользователей при работе в Сегменте, состояние и поддержание установленного уровня защиты информации, обрабатываемой в Сегменте.

2 ЗАДАЧИ АДМИНИСТРАТОРА ИБ

2.1. Основными задачами администратора ИБ являются:

- поддержание необходимого уровня защиты информации в Сегменте от несанкционированного доступа (далее – НСД) к информации;
- обеспечение конфиденциальности обрабатываемой, хранимой и передаваемой по каналам связи информации;
- установка средств защиты информации и контроль выполнения правил их эксплуатации;
- сопровождение средств защиты информации (далее – СЗИ) от НСД и основных технических средств и систем (ОТСС) Сегмента;
- периодическое обновление СЗИ и комплекса мероприятий по предотвращению инцидентов ИБ;
- оперативное реагирование на нарушения требований по ИБ в Сегменте и участие в их прекращении и предотвращении.

2.2. В рамках выполнения основных задач администратор ИБ осуществляет:

- текущий контроль работоспособности и эффективности функционирования эксплуатируемых программных и технических СЗИ;

– текущий контроль технологического процесса автоматизированной обработки ПДн;

– участие в проведении служебных расследований фактов нарушений или угрозы нарушений безопасности ПДн;

– контроль соблюдения нормативных требований по защите информации, обеспечения комплексного использования технических средств, методов и организационных мероприятий по безопасности информации в Организации.

3 ОБЯЗАННОСТИ

Администратор ИБ обязан:

3.1. Знать и выполнять требования документов по защите информации, регламентирующих порядок защиты информации, обрабатываемой в Сегменте.

3.2. Знать перечень установленных в Организации объектов вычислительной техники (далее – ОВТ) и перечень задач, решаемых с их использованием в Сегменте.

3.3. Осуществлять учет и периодический контроль надлежащего исполнения пользователями должностных обязанностей с использованием различных ОВТ Сегмента.

3.4. Осуществлять периодический контроль внесения изменений в конфигурацию (модификации) аппаратно-программных средств защищенных ОВТ и серверов, устанавливать и осуществлять контроль настройки средств защиты ОВТ Сегмента.

3.5. Периодически проверять состояние используемых СЗИ Сегмента, осуществлять проверку правильности их настройки (выборочное тестирование).

3.6. Проводить периодическое тестирование функций средств защиты Сегмента при изменении программной среды и персонала, с помощью тест-программ, имитирующих попытки НСД.

3.7. Проводить работу по выявлению возможных каналов вмешательства в процесс функционирования Сегмента и осуществления НСД к информации и ОВТ.

3.8. Контролировать своевременное и точное отражение изменений в организационно–распорядительных и нормативных документах в сфере управления средствами защиты Сегмента.

3.9. Проводить занятия с системными администраторами по вопросам разработки, внедрения и соблюдения правил работы на ОВТ Сегмента, оснащенных СЗИ.

3.10. Разрабатывать инструкции и памятки для пользователей, обрабатывающих ПДн в Сегменте.

3.11. Разрабатывать регламенты проведения работ, осуществляемых в целях обеспечения безопасности ПДн, обрабатываемых в Сегменте.

3.12. Участвовать в работе Организации по пересмотру планов защиты.

3.13. Обеспечить проведение автоматической проверки объектов ВТ, подключенных к Сегменту, на наличие вирусов с периодичностью не реже одного раза в неделю.

3.14. Осуществлять учет и периодический контроль действий системных администраторов, касающихся обеспечения информационной безопасности.

3.15. Участвовать в установке, настройке и сопровождении программных средств защиты информации Сегмента.

3.16.Участвовать в приемке новых программных средств обработки информации Сегмента.

3.17. Обеспечивать доступ к защищаемой информации пользователям Сегмента согласно их правам доступа при получении оформленного соответствующим образом разрешения (заявки).

3.18. Уточнять в установленном порядке обязанности пользователей Сегмента при обработке ПДн.

3.19. Вести контроль осуществления резервного копирования информации Сегмента.

3.20. Контролировать правильность функционирования средств защиты информации Сегмента и неизменность их настроек.

3.21. Контролировать физическую сохранность технических средств обработки информации Сегмента.

3.22. Контролировать исполнение пользователями Сегмента введенного режима безопасности, а также правильность работы с элементами Сегмента и средствами защиты информации.

3.23. Контролировать исполнение пользователями правил парольной политики.

3.24. Периодически анализировать журнал учета событий, регистрируемых средствами защиты, с целью контроля действий пользователей и выявления возможных нарушений.

3.25. Не допускать установку, использование, хранение и размножение в Сегменте программных средств, не связанных с выполнением функциональных задач.

3.26. Осуществлять периодические контрольные проверки автоматизированных рабочих мест (АРМ) Сегмента.

3.27. Оказывать помощь пользователям Сегмента в части применения средств защиты и консультировать по вопросам введенного режима защиты.

3.28. Периодически представлять руководству отчет о состоянии защиты Сегмента и о нештатных ситуациях и допущенных пользователями нарушениях установленных требований по защите информации, об имевших место попытках несанкционированного доступа к информации и ОВТ Сегмента.

3.29. В случае отказа работоспособности технических средств и программного обеспечения Сегмента, в том числе средств защиты, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

3.30. В случае выявления нарушений режима безопасности информации (ПДн), а также возникновения внештатных и аварийных ситуаций принимать необходимые меры с целью ликвидации их последствий.

3.31. Принимать участие в проведении работ по оценке соответствия Сегмента требованиям безопасности информации, указанным в:

– Федеральном законе от 27.07.2006 № 152–ФЗ «О персональных данных»;

– Постановлении Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– правовых, нормативных и организационно-распорядительных документов ФСТЭК России и ФСБ России в сфере защиты информации ограниченного доступа и содержащей персональные данные при их обработке в информационных системах.

3.32. Соблюдать требования режима конфиденциальности информации, содержащей персональные данные работников, а также третьих лиц, ставшей известной должностным лицам и сотрудникам Организации в связи с исполнением ими должностных обязанностей, в том числе в части запрета использования такой информации в интересах, не связанных с исполнением должностных обязанностей.

4 ПРАВА

Администратор ИБ имеет право:

4.1. Требовать от системных администраторов выполнения инструкций по обеспечению безопасности и защите информации.

4.2. Запрашивать и получать от работников Организации информацию и документы, необходимые для выполнения своих должностных обязанностей.

4.3. Доступа к программным и аппаратным ресурсам и информации на рабочих местах пользователей (за исключением информации, ограниченного доступа) и средствам их защиты.

4.4. Инициировать проведение служебных расследований и участвовать в проведении служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности,

несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов Сегмента.

4.5. Непосредственно обращаться к руководителям подразделений Организации с требованием прекращения работы в Сегменте при несоблюдении установленной технологии обработки информации и невыполнении требований по безопасности.

4.6. Отключать от ресурсов Системы АРМ работников, осуществивших НСД к защищаемым ресурсам или нарушивших другие требования по ИБ.

4.7. Вносить свои предложения по совершенствованию мер защиты информации в Сегменте.

4.8. Давать работникам обязательные для исполнения указания и рекомендации по вопросам ИБ.

4.9. Осуществлять контроль информационных потоков, генерируемых при работе пользователями Сегмента.

4.10. Запрещать устанавливать на серверах и автоматизированных рабочих местах Сегмента нештатное программное и аппаратное обеспечение.

5 ОТВЕТСТВЕННОСТЬ

5.1. Администратор ИБ несет ответственность за реализацию в Сегменте принятой в Организации политики безопасности.

5.2. На администратора ИБ возлагается персональная ответственность за работу программно-технических и криптографических средств защиты информации и за качество проводимых работ по обеспечению защиты информации на ОВТ в соответствии с функциональными обязанностями.

5.2.1. Администратор ИБ несет административную и уголовную ответственность за свои действия в порядке, установленном законодательством Российской Федерации.

6 ДЕЙСТВИЯ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ ПРИ ОБНАРУЖЕНИИ ПОПЫТОК НСД

7

6.1. К попыткам НСД относятся:

– сеансы работы с телекоммуникационными ресурсами Сегмента и/или Системы незарегистрированных пользователей, пользователей, нарушивших установленную периодичность доступа, либо срок действия полномочий которых истек, либо в состав полномочий которых не входят операции доступа к определенным данным или манипулирования ими.

– действия третьего лица, пытающегося получить доступ (или получившего доступ) к информационным ресурсам Сегмента и/или Системы с использованием учетной записи администратора или другого пользователя Сегмента, в целях получения коммерческой или другой личной выгоды, методом подбора пароля или другого метода (случайного разглашения пароля и т.п.) без ведома владельца учетной записи.

6.2. При выявлении факта/попытки НСД администратор ИБ обязан:

– прекратить доступ к информационным ресурсам со стороны выявленного участка НСД:

– доложить руководству подразделения ИБ о факте НСД, его результате (успешный, неуспешный) и предпринятых действиях;

– известить руководителя Организации, в которй работает пользователь, от имени учетной записи которого была осуществлена попытка НСД, о факте НСД;

– проанализировать характер НСД;

– по решению руководства подразделения ИБ осуществить действия по выяснению причин, приведших к НСД;

– предпринять меры по предотвращению подобных инцидентов в дальнейшем.

Начальник подразделения ИБ _____ _____
(подпись) (И.О. Фамилия)

СОГЛАСОВАНО:

Управление кадров

_____ _____
(подпись) (И.О. Фамилия)

Юридический отдел _____ _____
(подпись) (И.О. Фамилия)

С инструкцией ознакомлен:

_____ _____ _____
(подпись) (И.О. Фамилия)

«____» _____20___г.