|  |  |
| --- | --- |
|  | УТВЕРЖДЕНА  приказом ГКУ НСО ЦСПН  Усть-Таркского района  от «03» июня 2019 г.  № 61 |

**Инструкция администратора безопасности информационных систем**

1. Общие положения

1.1. Настоящая инструкция определяет функции, права и ответственность лица, ответственного за обеспечение безопасности информационных систем (далее – ИС) ГКУ НСО ЦСПН Усть-Таркского района, определенного администратором безопасности ИС ГКУ НСО ЦСПН Усть-Таркского района.

1.2. ГКУ НСО ЦСПН Усть-Таркского района назначает администратора безопасности ИС соответствующим внутренним документом ГКУ НСО ЦСПН Усть-Таркского района.

1.3. Администратор безопасности ИС в своей деятельности руководствуется Федеральными законами от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и от 27.07.2006 № 152-ФЗ «О персональных данных», постановлениями Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», главой 14 Трудового кодекса Российской Федерации, пунктом 8 Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных приказом ФСТЭК России от 18.02.2013 № 21, пунктом 20 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 № 17, иными нормативными правовыми актами Российской Федерации в области защиты информации, в том числе персональных данных, настоящей инструкцией и иными нормативными правовыми актами ГКУ НСО ЦСПН Усть-Таркского района в области защиты информации, в том числе персональных данных.

1.4. Администратор безопасности ИС знакомится с настоящей инструкцией под роспись.

2. Обязанности администратора безопасности ИС

2.1. Администратор безопасности ИС обязан:

* применять технические меры защиты информации;
* обеспечивать функционирование и безопасность средств защиты информации;
* обучать пользователей работе на персональных компьютерах с установленными средствами защиты информации;
* контролировать выполнение установленных правил обеспечения защиты информации лицами, допущенными к обработке информации соответствующим внутренним документом ГКУ НСО ЦСПН Усть-Таркского района;
* инициировать проведение служебных расследований по фактам нарушения установленных правил обеспечения защиты информации, несанкционированного доступа к информации;
* разъяснять пользователям порядок использования машинных носителей информации и контролировать заполнение соответствующего журнала;
* информировать ответственного за организацию обработки информации об инцидентах и попытках несанкционированного доступа к защищаемой информации, элементам систем и средствам защиты информации;
* организовывать антивирусную защиту в соответствии с соответствующей Инструкцией;
* предоставлять доступ к ИС новым пользователям, предоставлять им возможность задать пароль, соответствующий требованиям «Инструкции по управлению правилами и процедурами идентификации и аутентификации»;
* производить мероприятия по внеплановой смене паролей;
* осуществлять периодическое резервное копирование баз информации и сопутствующей защищаемой информации, а также осуществлять внеплановое создание резервных копий по запросу пользователей ИС и/или в иных случаях, когда это необходимо для обеспечения сохранности информации;
* осуществлять восстановление информации из резервных копий по запросу пользователей ИС и/или в иных случаях, когда это необходимо для восстановления утраченных сведений;
* хранить дистрибутивы программного обеспечения, установленного в ИС, в том числе дистрибутивы средств защиты информации, в месте, исключающем несанкционированный доступ к ним третьих лиц;
* реализовывать контроль (анализ) защищенности информации ИС;
* осуществлять выявление компьютерных инцидентов, реагирование на них и проведение расследований;
* обеспечивать управление конфигурацией ИС и системы защиты информации ИС;
* вносить свои предложения по совершенствованию мер защиты информации в ИС, разработке и принятии мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению уровня защищённости информации.

2.2. Администратор безопасности ИС может выполнять свои обязанности с привлечением сотрудников иных организаций на основании заключенных соглашений.

3. Действия администратора безопасности ИС при обнаружении попыток несанкционированного доступа

3.1. К попыткам несанкционированного доступа относятся:

* действия третьего лица, пытающегося получить доступ (или уже получившего доступ) к ИС, при использовании учётной записи администратора или другого пользователя ИС, методом подбора пароля, использования пароля, разглашённого владельцем учётной записи или любым другим методом;
* сеансы работы с ИС незарегистрированных пользователей, или пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истёк, или превышающих свои полномочия по доступу к данным.

3.2. При выявлении факта несанкционированного доступа администратор безопасности ИС обязан действовать в соответствии с Инструкцией по выявлению компьютерных инцидентов и реагированию на них.

4. Настройка средств защиты информации ИС

4.1. Администратор безопасности ИС при настройке и администрировании средств защиты информации ИС руководствуется нормативно-правовыми актами Российской Федерации в области обработки персональных данных и защиты информации.

4.2. Действия администратора безопасности ИС по параметрам настройки средств защиты информации при необходимости согласовываются с государственным бюджетным учреждением Новосибирской области «Центр защиты информации Новосибирской области» (далее – ГБУ НСО «ЦЗИ НСО») и производятся согласно внутренних документов ГБУ НСО «ЦЗИ НСО».

5. Права администратора безопасности

Администратор безопасности ИС имеет право:

* требовать от работников выполнения установленных правил обеспечения защиты информации;
* требовать от работников прекращения обработки информации в случаях их неправомерного использования и нарушения правил обеспечения защиты информации;
* вносить предложения по совершенствованию технических мер по защите информации.

6. Ответственность

4.1. Администратор безопасности ИС несёт персональную ответственность за качество проводимых им работ по обеспечению безопасности информации.

4.2. Администратор безопасности ИС несёт ответственность за разглашение информации ограниченного доступа, ставшей известной ему по роду работы, в соответствии с законодательством Российской Федерации.

Лист ознакомления  
с Инструкцией администратора безопасности информационных систем

|  |  |  |  |
| --- | --- | --- | --- |
| №п\п | Ф.И.О. | Дата | Подпись |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |