Медникова Ирина Александровна

Подписано цифровой подписью: Медникова Ирина Александровна
Дата: 2024.03.18 21:28:00 +03'00'

УТВЕРЖДАЮ
Директор
МОУ Чуфаровская СОШ
_____ И. А. Медникова
«__» июля 2018

# Регламент
## регистрации событий безопасности в информационной системе «Автоматизированное рабочее место для подключения к защищенным образовательным ресурсам» Муниципального общеобразовательного учреждения Чуфаровской средней общеобразовательной школы

2018 г.

# 1 Общие положения

1.1 Настоящий Регламент регистрации событий безопасности (далее – Регламент) регламентирует порядок регистрации событий безопасности в информационной системе «Автоматизированное рабочее место для подключения к защищенным образовательным ресурсам» (далее ИС «Автоматизированное рабочее место для подключения к защищенным образовательным ресурсам») Муниципального общеобразовательного учреждения Чуфаровской средней общеобразовательной школы (далее – Оператор) в соответствии с законодательством Российской Федерации.

1.2 Настоящий Регламент разработан в соответствии с:

– Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

– Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

– Приказом ФСТЭК № 17 от 11 февраля 2013 г. «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

– Приказом ФСТЭК № 21 от 18 февраля 2013 г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– Приказом ФСТЭК № 27 от 15 февраля 2017 г. «О внесении изменений в требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом ФСТЭК от 11 февраля 2013 г.».

1.3 Для целей настоящего Регламента используются следующие основные понятия:

– персональные данные – любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных);

– несанкционированный доступ — доступ к информации в нарушение должностных полномочий сотрудника, доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации. Также несанкционированным доступом в отдельных случаях называют получение доступа к информации лицом, имеющим право на доступ к этой информации в объёме, превышающем необходимый для выполнения служебных обязанностей.

# 2 Порядок работы с электронными журналами протоколирования и аудита событий безопасности

2.1 Выполнение требований по безопасности для подсистемы «Регистрация событий безопасности» осуществляются организационными мерами и сертифицированными средствами защиты информации (далее - СЗИ).

2.2 Правила и порядок протоколирования и аудита значимых событий в ИС «Автоматизированное рабочее место для подключения к защищенным образовательным ресурсам» направлены на превентивную фиксацию и изучение действий субъектов и объектов в ИС «Автоматизированное рабочее место для подключения к защищенным образовательным ресурсам», а также на своевременное выявление фактов

несанкционированного доступа (далее - НСД) к защищаемой информации.

2.3 Все события, происходящие в операционной системе, критических приложениях и СЗИ, установленных на ПЭВМ, входящих в состав ИС «Автоматизированное рабочее место для подключения к защищенным образовательным ресурсам», должны протоколироваться в специальные электронные журналы аудита.

2.4 В перечень регистрируемых событий безопасности входят:

- вход (выход), а также попытки входа субъектов доступа в информационную систему;
- запуск (завершение) программ и процессов (заданий), связанных с обработкой защищаемой информации;
- изменение политики безопасности информационной системы;
- изменение состава привилегированных пользователей и привилегий учетных записей;
- попытки удаленного доступа;
- иная информация, необходимая при последующем разборе инцидентов информационной безопасности (в том числе полнотекстовая запись привилегированных команд (команд, управляющих системными функциями);

2.5 Срок хранения зарегистрированных событий – не менее 1 месяца.

2.6 На ПЭВМ, входящих в состав ИС «Автоматизированное рабочее место для подключения к защищенным образовательным ресурсам», на которых установлены СЗИ от НСД, проверка соответствующего электронного журнала событий, формируемых данными СЗИ, производится в соответствии с прилагаемой к ним эксплуатационной и технической документацией.

2.7 Аудит событий, зафиксированных в электронных журналах, должен анализироваться в плановом порядке на постоянной основе не реже одного раза в месяц Администратором ИБ ИС «Автоматизированное рабочее место для подключения к защищенным образовательным ресурсам».

2.8 Администратор ИБ обязан выполнять пересмотр перечня событий безопасности, подлежащих регистрации, не менее чем один раз в год, а также по результатам контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе.

2.9 Администратор ИБ обязан следить за выполнением требований по безопасности ПДн в ИС «Автоматизированное рабочее место для подключения к защищенным образовательным ресурсам» Муниципального общеобразовательного учреждения Чуфаровской средней общеобразовательной школы в соответствии с классом ИС и уровнем защищенности ПДн для подсистемы «Регистрация событий безопасности», приведенными в Приказе ФСТЭК № 17 от 11 февраля 2013 г. «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» с учетом изменений, изложенных в Приказе Федеральной службы по техническому и экспортному контролю № 27 от 15 февраля 2017 года «О внесении изменений в требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные Приказом Федеральной службы по техническому и экспортному контролю от 11.02.2013 №17»; Приказе ФСТЭК № 21 от 18 февраля 2013 г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

2.10 Ответственный за организацию обработки ПДн и Администратор ИБ обязаны реагировать на события безопасности в течение минимально возможного времени

2.11 Ответственный за организацию обработки ПДн и Администратор ИБ обязаны проводить своевременный мониторинг журналов безопасности

2.12 Ответственный за организацию обработки ПДн и Администраторы ИБ обязаны осуществлять при необходимости копирование и резервирование журналов безопасности

## 3 Ответственность при организации регистрации событий безопасности в информационной системе «Автоматизированное рабочее место для подключения к защищенным образовательным ресурсам»

3.1 Ответственность за организацию регистрации событий безопасности и установление порядка ее проведения в соответствии с требованиями настоящего Регламента возлагается на Администратора ИБ ИС «Автоматизированное рабочее место для подключения к защищенным образовательным ресурсам».

3.2 Ответственность за поддержание установленного порядка и соблюдение требований настоящего Регламента возлагается на Ответственного за организацию обработки ПДн в Муниципального общеобразовательного учреждения Чуфаровской средней общеобразовательной школы.

3.3 Периодический контроль за выполнением всех требований настоящих Регламента осуществляется Администратором ИБ ИС Муниципального общеобразовательного учреждения Чуфаровской средней общеобразовательной школы.

# Лист ознакомления

с Регламентом регистрации событий безопасности в информационной системе «Автоматизированное рабочее место для подключения к защищенным образовательным ресурсам» Муниципального общеобразовательного учреждения Чуфаровской средней общеобразовательной школы

| № п/п | Должность | Фамилия, Имя, Отчество | Дата ознакомления | Подпись |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |