Приложение 6

УТВЕРЖДЕНО

приказом директора ЧОУ «СОШ «Истоки» от 29.11.2019г. № 26 «Об утверждении локальных актов, определяющих политику в отношении персональных данных»

ПОРЯДОК

работы с электронными журналами безопасности информационных систем персональных данных в ЧОУ «СОШ «Истоки»

1. Общие положения

Правила и порядок протоколирования и анализа (аудита) значимых событий в информационных системах (далее - ИС) персональных данных (далее - ПДн) направлены на превентивную фиксацию и изучение действий субъектов и объектов в ИСПДн наименование оператора.

Все события, происходящие в операционной системе, ИСПДн, других критических приложениях и средствах защиты информации должны протоколироваться в специальные электронные журналы аудита.

1. Настройки безопасности систем аудита

Проверке подлежат следующие электронные журналы:

- журнал событий, формируемых средствами защиты информации;

- журнал событий, формируемых программным обеспечением ИСПДн;

- журналы, формируемые операционной системой и прикладным программным обеспечением.

На персональных электронных вычислительных машинах, входящих в состав ИСПДн, на которых установлены средства защиты информации от несанкционированного доступа, проверка электронного журнала событий, формируемых данными средствами защиты, производится в соответствии с прилагаемым к указанным средствам защиты информации руководством.

Проверка электронных журналов обращений к ИСПДн проводится не реже 1 (Одного) раза в месяц администратором информационной безопасности ПДн.

Аудит событий, зафиксированных в электронных журналах, должен анализироваться в плановом порядке на постоянной основе не реже 1 (Одного) раза в месяц администратором информационной безопасности с обязательной регистрацией в соответствующем Журнале проверок электронных журналов информационных систем персональных данных ЧОУ «СОШ «Истоки», форма которого приведена в Приложении № 1 к настоящему Порядку.

Электронные журналы аудита должны записываться и вестись в автоматизированном режиме.

Настройки журналов аудита должны однозначно интерпретировать все значимые события ИСПДн.

1. Контроль

Нарушения в функционировании ИСПДн классифицируются в соответствии с Перечнем нарушений требований по обеспечению безопасности ПДн.

При выявлении нарушений I и II категории проводится служебная проверка в соответствии с Порядком проведения служебных проверок по фактам нарушения требований по обеспечению безопасности ПДн.

Приложение № 1

К Порядку

Форма ЖУРНАЛА

проверок электронных журналов информационных систем персональных данных ЧОУ «СОШ «Истоки»

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № п/п | Датапроверки  | Наименование ИСПДн, ПЭВМ, технического средства | Наименование проверяемого журнала | Выявленные нарушения требований безопасности, нештатные ситуации  | Подпись ответственного лица |  Примечание |
| 1 | 2 | 3 | 4 | s  | 6 | 7 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |