2022

ИНСТРУКЦИЯ

по организации парольной защиты
в ЧОУ «ШКОЛА «ТАУРАС»
г. Санкт-Петербург
ФЗ “О персональных данных” от 27.07.2006 №152-ФЗ

Лобанов А.А.
ЧОУ «ШКОЛА «ТАУРАС»
01.09.2022

ЧАСТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«ШКОЛА «ТАУРАС»
197229, г. Санкт-Петербург, Лахтинский проспект, д.102, к.3, стр.1
http://www.tauras-school.ru; info@tauras-school.ru
ОКПО 01281685 ОГРН 1157800002590 ИНН/КПП 7814237643/781401001

П Р И К А З

от 01.09.2022г. № 44

Об утверждении инструкции по организации парольной защиты в ЧОУ «ШКОЛА «ТАУРАС».

В соответствии в соответствии с Федеральным законом ФЗ “О персональных данных” от 27.07.2006 №152-ФЗ.»,

ПРИКАЗЫВАЮ:

1. Утвердить инструкцию по организации парольной защиты в ЧОУ «ШКОЛА «ТАУРАС».
2. Секретарю учебной части **Никитиной А.И.** ознакомить под роспись всех педагогических работников школы, а также вновь прибывающих при трудоустройстве в школу.
3. Секретарю учебной части **Никитиной А.И.** разместить данное положение на сайте школы в разделе «Сведения об образовательной организации» - «Документы» в срок до 05.09.2022

Директор ЧОУ «ШКОЛА «ТАУРАС» _____ А.А. Лобанов

С приказом ознакомлен:

№	Фамилия	Подпись	Дата
1	Никитина А.И.		

СОГЛАСОВАНО

Педагогическим советом
ЧОУ «ШКОЛА «ТАУРАС»»
(протокол №1 от 26.08.2022)

УТВЕРЖДЕНО

Приказом директора
ЧОУ «ШКОЛА «ТАУРАС»
от 01.09.2022 № 44

СОГЛАСОВАНО

Педагогическим советом
ЧОУ «ШКОЛА «ТАУРАС»»
(протокол №1 от 26.08.2022)

УТВЕРЖДЕНО

Приказом директора
ЧОУ «ШКОЛА «ТАУРАС»
от 01.09.2022 № 44

ИНСТРУКЦИЯ
организации парольной защиты в ЧОУ «ШКОЛА «ТАУРАС»

1 Общие положения

Настоящая инструкция устанавливает основные правила введения парольной защиты информационной системы персональных данных ЧОУ «ШКОЛА «ТАУРАС» (далее – Учреждение). Инструкция регламентирует организационно-техническое обеспечение генерации, смены и прекращения действия паролей в информационные системы персональных данных, а также контроль за действиями пользователей системы при работе с паролями. Настоящая инструкция оперирует следующими основными понятиями:

- **Идентификация** - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.
- **ИСПДн –** информационная система персональных данных.
- **Компрометация** - факт доступа постороннего лица к защищаемой информации, а также подозрение на него.
- **Объект доступа** - единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.
- **Пароль** – уникальный признак субъекта доступа, который является его (субъекта) секретом.
- **Правила доступа** - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.
- **Субъект доступа** - лицо или процесс, действия которого регламентируются правилами разграничения доступа.
- **Несанкционированный доступ** - доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или АС.

2 Правила генерации паролей

2.1 Персональные пароли должны генерироваться специальными программными средствами административной службы.

2.2 Длина пароля должна быть не менее 8 символов.

2.3 В составе пароля должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы.

2.4 Пароль не должен включать в себя:

- легко вычисляемые сочетания символов;
- клавиатурные последовательности символов и знаков;
- общепринятые сокращения;
- аббревиатуры;
- номера телефонов, автомобилей;
- прочие сочетания букв и знаков, ассоциируемые с пользователем;
- при смене пароля новое сочетание символов должно отличаться от предыдущего не менее чем на 2 символа.

2.5 Допускается использование единого пароля для доступа субъекта доступа к различным информационным ресурсам одной ИСПДн объекта образования.

1.1 которым по роду службы были предоставлены полномочия по управлению парольной зашитой.

1.2 Полная внеплановая смена паролей должна производиться в случае компрометации личного пароля одного из администраторов ИСПДн.

1.3 В случае компрометации личного пароля пользователя надлежит немедленно ограничить доступ к информации с данной учетной записи, до момента вступления в силу новой учетной записи пользователя или пароля.

2 Обязанности пользователей при работе с парольной защитой

2.1 При работе с парольной защитой пользователям запрещается:

– разглашать кому-либо персональный пароль и прочие идентифицирующие сведения;
– предоставлять доступ от своей учетной записи к информации, хранящейся в ИСПДн посторонним лицам;
– записывать пароли на бумаге, файле, электронных и прочих носителях информации, в том числе и на предметах.

2.2 Хранение пользователем своего пароля на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе.

2.3 При вводе пароля пользователь обязан исключить возможность его перехвата сторонними лицами и техническими средствами.

3 Случаи компрометации паролей

3.1 Под компрометацией следует понимать:

– физическая утеря носителя с информацией;
– передача идентификационной информации по открытым каналам связи;
– проникновение постороннего лица в помещение физического хранения носителя парольной информации или алгоритма, или подозрение на него (срабатывание сигнализации, повреждение устройств контроля НСД (слепков печатей), повреждение замков и т. п.);
– визуальный осмотр носителя идентификационной информации посторонним лицом;
– перехват пароля при распределении идентификаторов;
– сознательная передача информации постороннему лицу.

3.2 Действия при компрометации пароля:

– скомпрометированный пароль сразу же выводится из действия, взамен его вводятся запасной или новый пароль;
– о компрометации немедленно оповещаются все участники обмена информацией. Пароль вносится в специальные списки, содержащие скомпрометированные пароли и учетные записи.

4 Ответственность пользователей при работе с парольной защитой

4.1 Повседневный контроль за действиями сотрудников Учреждения при работе с паролями, соблюдением порядка их смены, хранения и использования, возлагается на ответственного за систему защиты информации в информационной системе персональных данных.

4.2 Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

4.3 Ответственность за организацию парольной защиты возлагается на ответственного за систему защиты информации в информационной системе персональных данных.

4.4 Ответственность в случае несвоевременного уведомлении ответственного за систему защиты информации в информационной системе персональных данных о случаях утери, кражи, взлома или компрометации паролей возлагается на владельца взломанной учетной записи.

Лист ознакомления с

ИНСТРУКЦИЯ
организации парольной защиты в ЧОУ «ШКОЛА «ТАУРАС»

№	Фамилия	Подпись	Дата
1	Битюков А.		
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			
26			
27			
28			
29			
30			
31			
32			
33			
34			
35			
36			
37			
38			
39			

40			
41			
42			
43			
44			
45			
46			
47			
48			
49			
50			
51			
52			
53			
54			
55			
56			
57			
58			
59			
60			
61			
62			
63			
64			
65			
66			
67			
68			
69			
70			
71			
72			
73			