|  |  |
| --- | --- |
|  | Приложение 15к приказу комитетапо культуре города Барнаулаот 29 июля 2021г. №64 |

ИНСТРУКЦИЯ

по организации парольной защиты в информационных системах

Перечень используемых определений, обозначений и сокращений

АИБ – администратор информационной безопасности.

ИС – информационная система.

ГИС – государственная информационная система.

НСД – несанкционированный доступ.

Администратор информационной безопасности – специалист или группа специалистов организации, осуществляющих контроль за обеспечением защиты информации в ИС, в том числе ИСПДн, а также осуществляющие организацию работ по выявлению и предупреждению возможных каналов утечки информации, потенциальных возможностей осуществления НСД к защищаемой информации.

1. Общие положения

1.1. Инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в ИС общего пользования, ГИС, ИСПДн, ИС, содержащих другие виды конфиденциальной информации, за исключением систем, содержащих сведения, составляющие государственную тайну, и систем, относящихся к объектам критической информационной инфраструктуры (далее – ИС) в комитете по культуре города Барнаула (далее – комитет), а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

1.2. Идентификация/аутентификация пользователей осуществляется посредством использования паролей, при технической возможности – средствами усиленной аутентификации.

1.3. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИС комитета и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на АИБа.

2. Порядок организации работы пользователя ИС с использованием пароля

2.1. Доступ к защищаемым информационным активам комитета должен производиться с использованием персональных учетных записей и периодически сменяемых буквенно-цифровых паролей, удовлетворяющих следующим требованиям:

пароль содержит не менее шести символов, включая буквы обоих регистров и цифры;

не является словом, присутствующим в словарях, или профессиональным термином, в т. ч. набранным в другой раскладке клавиатуры;

не основывается на семейной, служебной и другой легко доступной информации (фамилии, имена, даты рождения, клички животных, автомобильные и телефонные номера, названия организаций, адреса сайтов и т. п.);

не содержит легко угадываемые последовательности символов (123456, aaabbb, qwerty, q1w2e3 и т. п.);

не совпадает с номером помещения, названием подразделения, месяцем (312313, бухгалтерия, январь, март2011);

одним из способов создания безопасных, но легко запоминающихся паролей является кодирование стихотворной строки или осмысленного утверждения. Так, пароль, созданный на основе фразы: "Вот один пример надежного и запоминающегося пароля", может быть таким: «VotlPN&ZP».

2.2. Временный пароль, создаваемый при заведении учетной записи или смене забытого пароля, должен быть уникальным, передаваться способом, исключающим доступ к нему других лиц, и быть сменен пользователем при первом обращении к активу. Пароли, предустановленные производителем, должны сменяться до начала эксплуатации актива.

2.3. Пользователям запрещается:

сообщать свой персональный пароль другим лицам или записывать его на материальных носителях, доступных для других лиц (кроме предусмотренных случаев сохранения паролей ключевых учетных записей владельцем информационного актива);

сохранять пароль в программно-технических средствах в открытом виде или использовать средства его автоматического ввода;

использовать легко угадываемый алгоритм смены пароля (например, F%1hTR8 -\* F%2hTR8 -> F%3hTR8, или F%1hTR8 -\* Fl%hTR8 -\* F1h%TR8 и др.);

использовать учетные записи других лиц;

использовать вне комитета пароли, совпадающие с паролями доступа к его информационно-технологическим активам;

использовать в качестве паролей примеры, приведенные в Инструкции.

3. Порядок резервирования паролей

3.1. По решению председателя комитета или АИБа, может применяться резервирование некоторых паролей, таких, как пароли администраторов информационных систем (программистов), пароли ответственных должностных лиц, пароли отдельных пользователей, выполняющих важные функции, пароли обеспечивающие работу отдельных сетевых сервисов.

3.2. Для резервирования пароля выполняются следующие действия:

пароль записывается на лист бумаги – парольную карту (Приложение 13) и заверяется личной подписью;

лист с записью пароля вкладывается владельцем в конверт. Конверт не должен допускать просмотр записи пароля на просвет. Если конверт недостаточно плотный, в него может быть вложен лист темной бумаги. Конверт заклеивается, опечатывается;

на конверте владелец пароля указывает свою должность, фамилию и инициалы, наименование информационного средства, которое защищается этим паролем, текущие дату и время, при необходимости – другие данные, и заверяет запись личной подписью;

конверт передается председателю комитета или АИБу и учитывается в специальном разделе «Журнала учета парольных карт». Учетный номер (сквозной по Журналу) проставляется ответственным за хранение на конверте. Пример оформления конверта приведен в приложении 13.

Конверты с паролями хранятся в сейфе председателя комитета или АИБа и не реже, чем один раз в месяц он проверяет их наличие по журналу учета.

3.3. При замене пароля конверт передается владельцу пароля, который уничтожает лист с резервным паролем, о чем делается запись в «Журнале учета парольных карт». Новый резервный пароль подготавливает к хранению так, как указано выше. Новый конверт учитывается в «Журнале учета парольных карт» отдельной позицией.

3.4. Вскрытие конверта с паролем производится по решению руководителя структурного подразделения (начальника отдела) владельца в случае необходимости использования прав доступа его владельца в отсутствие самого владельца. Для вскрытия конверта назначается комиссия не менее чем из трех сотрудников Комитета. О вскрытии конверта комиссией составляется акт, утверждаемый председателем комитета или АИБом, который по окончании работы комиссии хранится не менее 1 года.

При появлении владельца пароля после факта вскрытия конверта пароль заменяется на новый и вновь сохраняется его копия, как описано выше.

4. Порядок смены паролей

4.1. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в три месяца.

4.2. Внеплановая смена личного пароля или удаление учетной записи пользователя ИС проводится в случае прекращения его полномочий (увольнение, переход на другую работу внутри территориального органа организации и т. п.) производится АИБом немедленно после окончания последнего сеанса работы данного пользователя с системой. Ответственность за своевременное предоставление сведений о перемещении сотрудников несет председатель комитета.

4.3. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри территориального органа организации и другие обстоятельства) АИБа.

4.4. В случае компрометации личного пароля пользователя ИС, проводится внеплановая смена пароля в зависимости от полномочий владельца скомпрометированного пароля.

5. Заключительные положения

5.1. Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на заместителя председателя комитета, периодический контроль – возлагается на АИБа.

5.2. В зависимости от критичности информационно-технологического актива, его владельцем могут быть установлены более высокие требования к сложности пароля и периодичности смены.

5.3. Процессы создания, изменения, использования, блокирования, удаления учетных записей, а также смены паролей должны быть регламентированы, протоколироваться и контролироваться.