АДМИНИСТРАЦИЯ ГОРОДА ВЛАДИМИРА

ПРИКАЗ

НАЧАЛЬНИКА ФИНАНСОВОГО УПРАВЛЕНИЯ

01.04.2013 № 50

Об утверждении инструкции парольной защиты информационных систем финансового управления администрации города Владимира

В целях обеспечения информационной безопасности в финансовом управлении администрации города Владимира **приказываю:**

1. Утвердить инструкцию парольной защиты информационных систем финансового управления администрации города Владимира согласно приложению.
2. Отделу правового обеспечения, работы с персоналом и делопроизводства довести данный приказ до сотрудников финансового управления.
3. Настоящий приказ подлежит размещению на официальном сайте органов местного самоуправления города Владимира.
4. Контроль за исполнением настоящего приказа оставляю за собой.

Начальник финансового управления В.А. Трусова

Приложение
УТВЕРЖДЕНО
приказом начальника
финансового управления
от_____№_____

ИНСТРУКЦИЯ
парольной защиты информационных систем финансового управления администрации города Владимира

Инструкция парольной защиты информационных систем финансового управления администрации города Владимира (далее - инструкция) регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действий паролей в информационных системах финансового управления администрации города Владимира (далее - ИС).

1. Правила формирования пароля

Личные пароли генерируются, распределяются и выдаются пользователям администратором ИС, либо выбираются пользователями ИС самостоятельно (в том числе из предложенных) с учётом следующих требований:

- длина пароля должна быть не менее 6 символов;
- в числе символов пароля рекомендуется использовать буквы в верхнем или нижнем регистрах, а также цифры;
- пароли могут содержать только символы латинской раскладки клавиатуры;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков (111, qwerty, abcd и т.д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетаний букв и знаков, которые можно угадать, основываясь на информации о пользователе;
- при смене пароля новое значение должно отличаться от предыдущего.

Пользователь ИС, выбравший пароль, должен сообщить пароль администратору ИС в течение рабочего дня.

2. Ввод пароля

При вводе пароля пользователю необходимо исключить возможность его подсматривания посторонними лицами (человек за спиной, наблюдение человеком за движением пальцев) и техническими средствами (встроенными в мобильные телефоны видеокамерами и т.п.).

3. Порядок смены личных паролей

Смена личного пароля или удаление учётной записи пользователя ИС в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться администратором ИС в 10-дневный срок после окончания последнего сеанса работы данного пользователя с системой на основании обращения заведующего отделом, эксплуатирующего ИС.

В случае компрометации (утери, передачи пароля третьим лицам) личного пароля должны быть немедленно предприняты меры по его смене.

Срочная (внеплановая) полная смена паролей должна производиться в случае прекращения полномочий (увольнение или переход на другую работу) администраторов ИС и других сотрудников, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты.

При необходимости смена пароля производится каждым пользователем самостоятельно или в соответствии с указанием системного администратора ИС.

При смене пароля пользователь должен сообщить новый пароль администратору ИС.

4. Хранение паролей

Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах.

Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

Администратор ИС хранит значение паролей пользователей на бумажном носителе в сейфе или на электронном носителе в зашифрованном виде.

5. Контроль и ответственность при организации парольной защиты

Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей в ИС и контроль за действиями пользователей при работе с паролями возлагается на администраторов ИС.

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.

Проект вносит отдел правового обеспечения, работы с персоналом и делопроизводства

ЗАВИЗИРОВАНО

Заведующий отделом правового
обеспечения, работы с персоналом
и делопроизводства
_____ А.И. Тонконогов
(подпись, дата)

Ведущий специалист отдела
правового обеспечения, работы с
персоналом и делопроизводства
_____ Д.В. Королёв
(подпись, дата)

Название файла: Приказ парольная защита.odt
Файл создан: 02.04.2013 13:46:11
Соответствие текста файла и оригинала подтверждаю Аксенов А.С., 12 02, 53 28 12
(Ф.И.О., контактные телефоны внутренней и городской связи, подпись)