Организационные меры по информационной безопасности

Как защитить информацию от несанкционированного доступа?

ПОЛИГОН Про

ПЛАН ВЕБИНАРА

1. О «Полигон Про».
2. Требования по обеспечению информационной безопасности при использовании электронной подписи.
3. Ответы на вопросы.

ПРОГРАММНЫЙ ЦЕНТР

15

ЛЕТ УСПЕШНОЙ РАБОТЫ

48 000

СЧАСТЛИВЫХ ПОЛЬЗОВАТЕЛЕЙ ПРОГРАММ И ВЕБ-СЕРВИСОВ

32

МОДУЛЯ ПОЛИГОН ПРО

15 250

ЭЛЕКТРОННЫХ ПОДПИСЕЙ ВЫДАНО

1465

СЛУШАТЕЛЕЙ КУРСОВ УЧЕБНОГО ЦЕНТРА

МЕРЫ ПО ЗАЩИТЕ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

- Подготовить и применить политику назначения и смены паролей;
- Провести комплекс мероприятий по антивирусной защите и аудиту;
- Разработать требования по защите информации;
- Внедрить требования по обеспечению информационной безопасности при обращении с носителями ключевой информации, содержащими ключи ЭП;
- Обеспечить безопасность средств вычислительной техники с установленными средствами ЭП.

ПОЛИТИКА НАЗНАЧЕНИЯ И СМЕНЫ ПАРОЛЕЙ

Необходимо разработать и применить политику назначения и смены паролей (для входа в операционную систему, BIOS и т.д.) в соответствии с правилами:

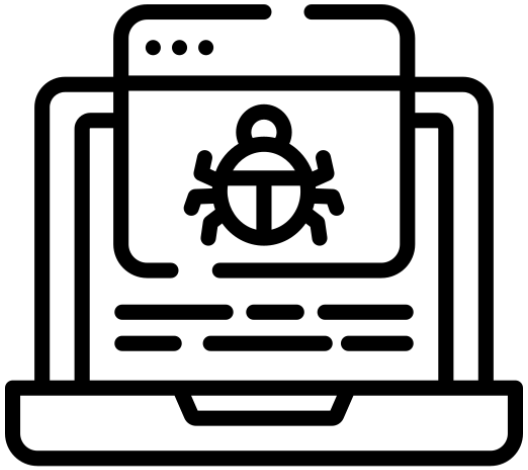
- длина пароля должна быть не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, номера телефонов, даты рождения и т.д.), а также сокращения (USER, ADMIN, root, и т.д.);

ПОЛИТИКА НАЗНАЧЕНИЯ И СМЕНЫ ПАРОЛЕЙ

Необходимо разработать и применить политику назначения и смены паролей (для входа в операционную систему, BIOS и т.д.) в соответствии с правилами:

- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;
- личный пароль пользователь не имеет права никому сообщать;
- периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 90 календарных дней.

СИСТЕМА АУДИТА И ЗАЩИТА ОТ ВИРУСОВ



Необходимо организовать и использовать:

- систему аудита, организовать регулярный анализ результатов аудита;
- комплекс мероприятий по антивирусной защите.

МЕРЫ ЗАЩИТЫ КЛЮЧА ЭЛЕКТРОННОЙ ПОДПИСИ

- ✓ Ключи квалифицированной ЭП при их создании должны записываться на типы ключевых носителей, которые поддерживаются используемым средством ЭП согласно технической и эксплуатационной документации к ним.
- ✓ Ключи квалифицированной электронной подписи на ключевом носителе должны быть защищены паролем (ПИН-кодом). При этом пароль (ПИН-код) формирует лицо, выполняющее процедуру создания ключей, в соответствии с требованиями на используемое средство ЭП.
- ✓ Ответственность за конфиденциальность сохранения пароля (ПИН-кода) возлагается на владельца ключа квалифицированной электронной подписи.

ЗАЩИТА ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Запрещается:

- осуществлять несанкционированное копирование ключевых носителей;
- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и иные средства отображения информации;
- использовать ключевые носители в режимах, не предусмотренных штатным режимом использования ключевого носителя;
- вносить какие-либо изменения в программное обеспечение средств ЭП;

ЗАЩИТА ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Запрещается:

- работать со средствами ЭП при включенных в техническое средство штатных средствах выхода в радиоканал;
- записывать на ключевые носители постороннюю информацию;
- оставлять средства вычислительной техники с установленными средствами ЭП без контроля после ввода ключевой информации;

ЗАЩИТА ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Запрещается:

- использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, который аннулирован, действие которого прекращено или приостановлено;
- удалять ключевую информацию с ключевого носителя до истечения срока действия, аннулирования или прекращения действия сертификата ключа проверки ЭП.

ОБРАЩЕНИЕ С КЛЮЧЕВОЙ ИНФОРМАЦИЕЙ И КЛЮЧЕВЫМИ НОСИТЕЛЯМИ

- Недопустимо пересылать файлы с ключевой информацией для работы в системах обмена электронными документами, по электронной почте сети Интернет или по внутренней электронной почте (кроме файлов квалифицированных сертификатов ключей проверки электронной подписи).
- Ключевая информация должна размещаться на сменном носителе информации (floppy-диск, USB flash-накопитель, e-Token, Рутокен, ESMART Token и др.).
- Размещение ключевой информации в реестре Windows, на локальном или сетевом диске, а также во встроенной памяти технического средства с установленными средствами ЭП, способствует реализации многочисленных сценариев совершения мошеннических действий злоумышленниками.

ОБРАЩЕНИЕ С КЛЮЧЕВОЙ ИНФОРМАЦИЕЙ И КЛЮЧЕВЫМИ НОСИТЕЛЯМИ

- Носители ключевой информации должны использоваться их владельцем либо уполномоченным лицом на использование данного носителя, и храниться в месте не доступном третьим лицам (сейф, опечатываемый бокс, закрывающийся металлический ящик и т.д.).
- Носитель ключевой информации должен подключаться в считывающее устройство только на время выполнения средствами ЭП операций формирования и проверки ЭП, шифрования и дешифрования.
- Размещение носителя ключевой информации в считывателе на продолжительное время существенно повышает риск несанкционированного доступа к ключевой информации третьими лицами.
- На носителе ключевой информации недопустимо хранить иную информацию (в том числе рабочие или личные файлы).

ОБЩИЕ ТРЕБОВАНИЯ ПРИ ИСПОЛЬЗОВАНИИ ЭП НА КОМПЬЮТЕРЕ

- На учетные записи пользователей ОС должны быть установлены пароли, удовлетворяющие требованиям, которые рассмотрели ранее;
- должно быть установлено только лицензионное ПО;
- должно быть установлено лицензионное антивирусное ПО с регулярно обновляемыми антивирусными базами данных;
- должны регулярно устанавливаться обновления операционной системы;
- должна быть включена автоматическая блокировка экрана после ухода ответственного сотрудника с рабочего места;

ОБЩИЕ ТРЕБОВАНИЯ ПРИ ИСПОЛЬЗОВАНИИ ЭП НА КОМПЬЮТЕРЕ

- должны быть отключены все неиспользуемые службы и процессы операционной системы Windows (в т.ч. службы удаленного администрирования и управления, службы общего доступа к ресурсам сети, системные диски и т.д.);
- должен быть исключен доступ (физический и/или удаленный) к техническим средствам с установленными средствами ЭП третьих лиц, не имеющих полномочий для работы в системе обмена электронными документами;
- в случае передачи (списания, сдачи в ремонт) сторонним лицам технических средств, на которых были установлены средства ЭП, необходимо гарантированно удалить всю информацию, использование которой третьими лицами может потенциально нанести вред организации.

ЭЛЕКТРОННАЯ ПОДПИСЬ

для физического лица – от 310 рублей

кадастрового инженера – 600 рублей

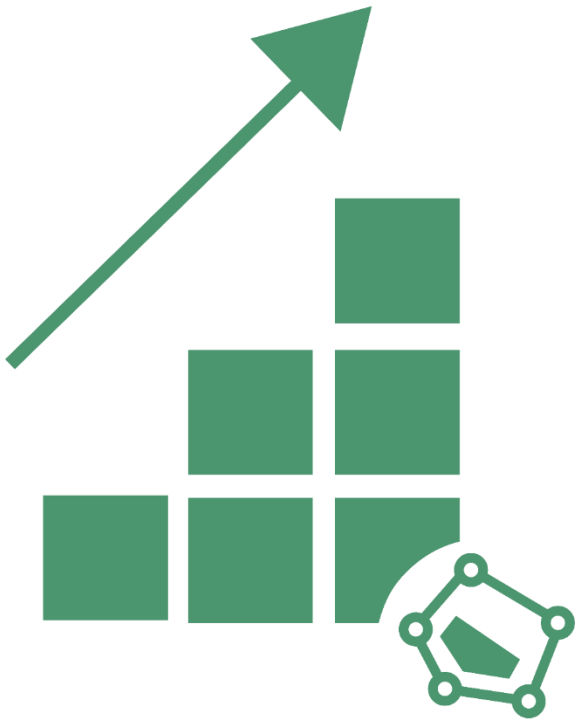
юридического лица – 1 000 рублей

органа местного самоуправления – 1 200 рублей

Оставьте заказ на sales@pbprog.ru

8-800-707-41-80 (звонок бесплатный)

ИНТЕНСИВ «ГРАФИЧЕСКАЯ ЧАСТЬ ЗА 15 МИНУТ»



НОВИНКА

Интенсив направлен на приобретение и развитие профессиональных навыков по подготовке чертежей межевых и технических планов, схемы ЗУ на КПТ и др.

- Свидетельство о прохождении курса
- 5 дней (72 часа)

Стоимость: 5 000 ₽
2 500 ₽ – для пользователей Полигон Про и студентов Академии Полигон

Старт курса: 25 марта 2019 г.

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

- Демо–версии программ
- Проверка пакета документов перед сдачей в ОКУ
- Рассмотрение приостановок
- Форум и статьи
- Бесплатные веб-сервисы «Полигон»
- Вебинары и видеоуроки
- Подробное руководство пользователя
- Индивидуальное обучение работе в программах

КОНТАКТНАЯ ИНФОРМАЦИЯ

ОТДЕЛ ПРОДАЖ

sales@pbprog.ru

8-800-707-41-80

ОТДЕЛ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ

help@pbprog.ru

8-800-100-58-90

МЫ В СОЦ. СЕТЯХ

Записи вебинаров
youtube.com/polygonkadastr

Актуальные новости кадастровой деятельности
vk.com/polygon_kadastr

Рабочие моменты компании
instagram.com/polygon_kadastr/

СЛЕДУЮЩИЙ ВЕБИНАР ПРОЙДЕТ

13 марта 2019 г. в 11:00 мск

Выдача ЭП заявителя для формирования документов
на ГКУ и ГРП

СПАСИБО ЗА ВНИМАНИЕ

pbprog.ru
sales@pbprog.ru
8-800-707-41-80

ПОЛИГОН Про