- установка стороннего программного обеспечения для защиты информации;
- ограничения физического доступа к компьютеру;
- хранение важной информации на отдельных носителях.

Рассмотрим подробнее каждый пункт и сформулируем рекомендации для повышения уровня защищенности информации на компьютере.

Внутренние средства защиты Windows - прежде всего это использование разных учетных записей. Например, создать две учетные записи, с разными категориями прав. Тем самым, вы сможете иметь доступ к своей информации, другой же пользователь вашего компьютера не будет иметь достаточно прав. В качестве, защиты учетной записи можно использовать пароль. Помимо этого к внутренним средствам защиты будет относиться возможность установки пароля на определенную папку или сокрытие этой папки. Тем, самым случайно другой пользователь не сможет найти важную для вас информацию.

Установка стороннего программного обеспечения для защиты информации - это использование определенного программного обеспечения, которое разграничивает права доступа к различным файлам. В качестве идентификатора могут выступать различные устройства. Например, при установке такого ПО, имеется возможность распределить права с помощью обычной флеш-памяти, на которую будет записана определенная информация, позволяющая идентифицировать владельца компьютера. Без этой флеш памяти найти скрытые файлы будет невозможно.

Ограничение физического доступа к компьютеру - банальный отказ пустить человека за ваш компьютер.

Хранение важной информации на отдельном носителе. Для хранения важной для Вас информации используйте отдельные устройства, такие как:

- флеш-память;
- внешние жесткие диски;
- облачные хранилища.

Благодаря способам выше, вы сможете повысить уровень защищенности важной информации на вашем ПК.

***

1. Anti-malware / [Электронный ресурс] – Режим доступа: <https://www.anti-malware.ru>
2. Geektimes / [Электронный ресурс] – Режим доступа: <https://geektimes.ru>

Казыханов А.А., Казыханова Д.Р., Редников Д.В.

Устройства печати, как источник угроз для конфиденциальности информации

*Бакирский государственный университет
(Россия, Уфа)*

doi: 10.18411/lj-10-2018-191

idsp: 000001:lj-10-2018-191

Аннотация

Статья рассматривает проблему нарушения конфиденциальности информации злоумышленником с помощью использования уязвимостей в устройствах печати. Таким образом, устройство печати можно отнести к источникам угроз для конфиденциальности информации

Ключевые слова: устройства печати, информация, конфиденциальность, безопасность, злоумышленник

Abstract

The article addresses the issue of breach of confidentiality of information by an attacker by exploiting vulnerabilities in printing devices. Thus, the printing device can be attributed to the sources of threats to the confidentiality of information.

Keywords: printing devices, information, confidentiality, security, intruder

Обеспечение безопасности информации одна из первоочередных задач почти для любой организации или компании, ведь обеспечение безопасности информации гарантирует компании стабильную работу без перебоев. Также, компания не понесёт ущерб из-за инцидентов информационной безопасности, если их не будет.

Опасность устройств печати заключается в том, что перед тем как изображение или файл выходит на печать оно обрабатывается в самом устройстве печати (принтере / МФУ) и тем самым там сохраняется его остаточный след. Возможны также ситуации, при которых изображение или файл сохраняется в кеше устройства, именно в таких ситуациях злоумышленник может заполучить конфиденциальную информацию.

Рассмотрим ситуации при использовании устройства для печати, при которых существует угроза конфиденциальности информации:

- злоумышленник имеет возможность взять распечатанный материал;
- злоумышленник имеет возможность подключения к другому ПК, имеющим подключение к принтеру (в случаях, когда принтер сетевой);
- злоумышленник имеет физический доступ к принтеру.

Для обеспечения конфиденциальности информации при печати необходимо использовать защищенный сервер печати. В общем виде это может выглядеть так:

Рисунок 1. Обеспечение конфиденциальности при печати

Рассмотрим более подробно ситуацию, при которой невозможно установить для каждого пользователя отдельный принтер, решением данного вопроса является технология безопасной печати с авторизацией. С помощью данной технологии есть возможность разграничить доступ сотрудников к устройствам, распечатываемым документам, и избежать утечки информации.

При использовании данной технологии следуем шагам:

- пользователь отправляет электронный документ на определенный принтер;

- подходит к аппарату;
- авторизируется;
- печать документа обычно осуществляется через выделенный принт-сервер.

Решение представляет собой распределенную в ЛВС многокомпонентную систему защиты, состоящую из специализированного принт-сервера и устройств «Сетевой контроллер», которые устанавливаются в непосредственной близости с устройством печати. Распечатка документов осуществляется только после авторизации пользователя на «Сетевом контроллере». Такой механизм дает возможность визуально контролировать процесс печати и препятствует утечкам конфиденциальной информации через бумажные носители.

***

1. Нестеров, С.А. Информационная безопасность: Учебник и практикум для академического бакалавриата / С.А.Нестеров - М.: Юрайт, 2017.- 322 с.
2. Шишов, О. В. Современные технологии и технические средства информатизации: Учебник / О. В. Шишов. - М.: НИЦ ИНФРА-М, 2016. - 462 с.

Киселев В.В., Хохолов Ю.А.

Оценка температурных условий в теплоизолированных камерах ожидания рудников криолитозоны

*Институт горного дела Севера им. Н.В.Черского СО РАН
(Россия, Якутск)*

doi: 10.18411/lj-10-2018-192

idsp: 000001:lj-10-2018-192

Аннотация

Приведены результаты исследований по формированию микроклимата в камерах ожидания, предназначенных для временного укрытия горнорабочих, работающих смен рудников криолитозоны в чрезвычайных ситуациях, на период ликвидации последствий аварий и техногенных катастроф.

Ключевые слова: Чрезвычайные ситуации, камера ожидания, рудники, микроклимат, температура, теплоизоляция, криолитозона

Как известно, подземные горные работы по степени риска для жизни горнорабочих, травмоопасности, аварийности относятся к более высокой категории чем открытые. Особенно возрастает степень риска в случае возникновения чрезвычайных ситуаций (ЧС) природного и техногенного характера, вызываемых горными ударами, внезапными прорывами воды и газов, авариями, пожарами и т.д. В ряде ЧС как на поверхности, так и под землей (отсутствие электроэнергии, пожары и задымленность подъемных стволов, неисправности подъема и т.д.) исключается возможность своевременного подъема горнорабочих работающей смены на поверхность.

В связи с этим, в соответствии с существующими требованиями на строящихся рудниках должны быть предусмотрены камеры ожидания (КО), размещаемые в обязательном порядке в околоствольных дворах, предназначенные для временного укрытия горнорабочих под землей на время ведения аварийных работ, обладающих максимальной надежностью и вместимостью при минимуме затрат на строительство и эксплуатацию, обеспечивающих требуемые санитарно-гигиенические условия и необходимый минимум удобств обитания на длительный период (до 5 суток).

В этих целях специально для условий рудников ИГДС СО РАН была разработана оригинальная конструкция теплоизолированной легким бетоном КО, на которую получен патент РФ [1], так же разработаны требования по её строительству, оборудованию и