Комлякова Марина Сергеевна, Студентка 2 курса
ОГАПОУ «Ульяновский авиационный колледж –
Межрегиональный центр компетенций»

Научный руководитель:
Дубовик Ирина Борисовна, преподаватель
ОГАПОУ «Ульяновский авиационный колледж –
Межрегиональный центр компетенций»

МЕТОДЫ ЗАЩИТА ОФИСНЫХ ФАЙЛОВ

Аннотация. В данной статье исследуются методы обеспечения безопасности офисной документации, в частности, файлов, сгенерированных в Microsoft Office, от неправомерного доступа, внесения изменений и утраты. Рассматриваются как административные и юридические механизмы защиты, так и специализированные технические решения и криптографические инструменты, применяемые в корпоративных сетях и системах хранения информации.

Ключевые слова: Информационная безопасность, Microsoft Office, защита данных, пароли, шифрование, права доступа, контроль версий, корпоративные системы.

ВВЕДЕНИЕ

В эпоху информационного общества, когда цифровые материалы занимают центральное место в бизнес-процессах, вопросы администрирования и обеспечения безопасности офисной документации становятся жизненно необходимыми. Эти файлы зачастую содержат секретные сведения, коммерческие тайны, личные данные и объекты интеллектуальной собственности, чья потеря, фальсификация или уничтожение могут привести к серьезным убыткам, ущербу репутации и юридическим проблемам.

Учитывая увеличение количества кибератак и усложнение структуры корпоративных сетей, задача защиты от неавторизованного доступа, непреднамеренных изменений и вредоносных программ, направленных на офисные документы, является приоритетной как для крупных компаний, так и для индивидуальных пользователей.

Данная статья рассматривает общие принципы защиты данных и подробно анализирует конкретные способы обеспечения безопасности офисных файлов, с особым акцентом на платформу Microsoft Office, как одну из наиболее популярных систем для создания и обработки документов.

В данной статье приводится полный алгоритм защиты офисных документов от несанкционированного доступа.

1 МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Информационная безопасность представляет собой многогранный подход, охватывающий использование различных методов и инструментов для поддержания секретности, сохранности и возможности использования информации. **Эти методы можно условно разделить на несколько категорий, ключевыми из которых являются организационные и технические меры. Их совместное и скоординированное применение формирует основу эффективной системы защиты.**

Организационные меры защиты определяют порядок работы с информацией, формируя основу для безопасной деятельности.

Политики и регламенты безопасности. Разработка и внедрение детализированных инструкций и правил использования информации, контроля доступа к системам, использования мобильных устройств, а также алгоритмов реагирования на инциденты.

Обучение и повышение осведомленности сотрудников. Проведение регулярных занятий для персонала по основам информационной безопасности, правилам безопасного поведения в интернете, выявлению фишинговых атак и методам социальной инженерии. Человеческий фактор – наиболее уязвимое звено в системе защиты.

Распределение ответственности и прав доступа. Четкое определение ролей и сфер ответственности сотрудников, а также строгий контроль доступа к информационным ресурсам, предоставляемый только в рамках необходимого для выполнения рабочих задач.

Резервное копирование данных и планирование восстановления. Систематическое создание резервных копий критически важных данных и разработка подробных планов восстановления после аварий (Disaster Recovery Plan) для минимизации ущерба в случае сбоев или кибератак.

Аудит и мониторинг безопасности. Непрерывный анализ журналов событий, сетевого трафика и действий пользователей для обнаружения потенциально опасной активности и нарушений.

Управление инцидентами. Разработка плана действий при возникновении инцидентов информационной безопасности, включая процессы обнаружения, анализа, локализации, устранения последствий и восстановления.

Физическая безопасность. Контроль физического доступа к помещениям, в которых размещено критически важное оборудование и хранится информация (системы видеонаблюдения, охранной сигнализации, контроля и управления доступом).

Технические меры защиты подразумевают использование специализированных программных и аппаратных инструментов для непосредственной защиты информации и информационных систем.

Антивирусное и антишпионское программное обеспечение. Защита, выявление и удаление вредоносных программ.

Межсетевые экраны (Firewalls). Контроль и фильтрация сетевого трафика между различными сегментами сети или между локальной сетью и интернетом.

Системы обнаружения и предотвращения вторжений (IDS/IPS): Мониторинг сетевого трафика и активности систем для выявления подозрительных действий и попыток проведения атак. IDS обнаруживает вторжения, а IPS активно их блокирует.

Шифрование данных. Преобразование информации таким образом, чтобы ее могли прочитать только авторизованные лица, обладающие ключом расшифровки. Шифрование используется для защиты данных как при хранении (на жестких дисках, в облачных хранилищах), так и при передаче (VPN, SSL/TLS).

Системы аутентификации и авторизации. Проверка подлинности пользователя (логин/пароль, биометрия, смарт-карты) и предоставление ему соответствующих прав доступа. Многофакторная аутентификация (MFA) значительно повышает безопасность.

Системы предотвращения утечек данных (DLP – Data Loss Prevention). Контроль за передачей конфиденциальной информации за пределы защищенного периметра.

Защита сетевой инфраструктуры. Использование VPN для безопасного удаленного доступа, сегментация сети для изоляции критически важных ресурсов, регулярное сканирование сети на наличие уязвимостей.

Системы управления информацией о безопасности и событиями безопасности (SIEM). Сбор, сопоставление и анализ журналов событий со всех устройств и систем для всестороннего мониторинга и выявления угроз.

Безопасная настройка систем и приложений. Отключение излишних сервисов, изменение стандартных паролей, применение принципа предоставления минимальных привилегий.

Регулярные обновления ПО. Своевременное установка патчей и обновлений для операционных систем, приложений и оборудования для устранения известных уязвимостей.

2 МЕТОДЫ ЗАЩИТЫ ОФИСНЫХ ФАЙЛОВ

Офисные пакеты "МойОфис" и "Microsoft office" включают текстовые процессоры, электронные таблицы и другие приложения. Эти пакеты располагает интегрированными инструментами защиты для контроля доступа к документам. Инструменты варьируются от паролей до систем управления правами, гарантирующих сохранность и секретность информации.

Установка пароля – это простой, но действенный способ защиты, однако крайне важно применять сложные и трудно угадываемые комбинации. Учтите, что утрата пароля от зашифрованного файла MS Office может привести к безвозвратной потере содержащихся в нем данных.

Пароль на открытие файла – предотвращает доступ к содержимому файла без его ввода и это обеспечивает конфиденциальность данных.

Чтобы установить защиту паролем на файл Word, Excel, PowerPoint следует придерживаться следующей инструкции.

1. Откройте соответствующий документ.
2. Перейдите на вкладку **"Файл"**.
3. Выберите **"Сведения"**.
4. Нажмите кнопку **"Защита документа/книги/презентации"**.
5. Выберите опцию **"Зашифровать с использованием пароля"**.
6. Введите желаемый пароль и нажмите "ОК".
7. Повторите ввод пароля для подтверждения и снова нажмите "ОК".
8. При следующем открытии файла потребуется ввод этого пароля.

Для снятия пароля действия 1-5 следует повторити удалить введенный пароль.

Пароль на сохранение изменений позволяет любому пользователю открыть файл для просмотра, но требует пароля для внесения и сохранения изменений.

Чтобы установить пароль для редактирования документа в Word, Excel или PowerPoint, выполните ряд шагов, приведенных по тексту ниже.

1. Откройте документ.
2. Перейдите на вкладку **"Файл".**
3. Выберите **"Сохранить как"** и выберите место сохранения (например, "Этот компьютер", затем "Обзор").
4. В диалоговом окне "Сохранение документа" (или "Сохранить как") рядом с кнопкой "Сохранить" нажмите **"Сервис".**
5. Выберите **"Общие параметры...".**
6. В поле **"Пароль для изменения"** введите желаемый пароль.
7. Нажмите "ОК", затем подтвердите пароль и еще раз нажмите "ОК".
8. Сохраните документ.

Для снятия пароля следует повторить шаги 1-5, удалите пароль из поля "Пароль для изменения" и сохраните документ.

Можно установить два отдельных пароля: один для открытия и ознакомления с содержанием, а другой – для редактирования и сохранения внесенных правок. Такая схема обеспечивает расширенные возможности контроля над доступом.

Ограничение доступа. Этот метод позволяет более тонко настраивать права пользователей, предотвращая нежелательные изменения или даже распространение документа, не требуя при этом пароля на открытие.

Защита документа Microsoft Word от редактирования (с возможностью просмотра и копирования) весьма популярным методом.

Для использования этого метода следует осуществить последовательность действий, приведенных ниже.

1. Откройте документ Word.
2. Перейдите на вкладку **"Рецензирование".**
3. В группе "Защита" нажмите **"Защитить документ"** и выберите **"Ограничить редактирование".**
4. В открывшейся правой панели "Ограничить редактирование" установите флажок напротив **"Разрешить только указанный способ редактирования документа".**
5. В выпадающем списке выберите **"Без изменений (только чтение)".**
6. Нажмите кнопку **"Да, включить защиту".**
7. Введите пароль (например, "123") для снятия защиты и подтвердите его.

Теперь документ будет открываться для просмотра, копирования и печати, но без пароля его нельзя будет удалить или изменить.

Для снятия защиты необходимо нажать кнопку "Отключить защиту" и введите пароль.

Защита на уровне книги Excel полностью защищищает от просмотра и внесения изменений в структуру книги.

1. Откройте книгу Excel.
2. Перейдите на вкладку **"Рецензирование".**
3. В группе "Изменения" нажмите кнопку **"Защитить книгу".**
4. В диалоговом окне "Защита структуры и окон" убедитесь, что флажок **"Структура"** установлен. (При необходимости можно также установить флажок "Окна", чтобы защитить размер и положение окон книги).
5. Введите пароль для снятия защиты и подтвердите его.

Теперь пользователи не смогут добавлять, удалять, переименовывать или перемещать листы в книге без ввода пароля.

Для снятия защиты необходимо на вкладке "Рецензирование" нажать "Защитить книгу" и ввести пароль.

Защита на уровне листа. Этот тип защиты позволяет контролировать изменения на конкретном листе документа, предоставляя гранулированный контроль над его содержимым.

Защитить элементы листа (например, ячейки с формулами), запретив доступ к ним всем пользователям. Можно также защитить форматирование ячеек, столбцов, строк.

1. Откройте книгу Excel и выберите лист, который хотите защитить.
2. Выделите ячейки, которые *должны оставаться редактируемыми*, после защиты листа. Щелкните правой кнопкой мыши, выберите **"Формат ячеек...",** перейдите на вкладку **"Защита"** и снимите флажок **"Защищаемая ячейка".** Нажмите "ОК".
3. Перейдите на вкладку **"Рецензирование".**
4. В группе "Изменения" нажмите кнопку **"Защитить лист".**
5. В диалоговом окне "Защита листа" выберите те действия, которые пользователи **могут** выполнять на этом листе. Все действия, для которых флажки не установлены, будут запрещены.
6. Введите пароль для снятия защиты и подтвердите его.

Теперь только разрешенные действия могут быть выполнены на листе; ячейки с формулами и другие защищенные элементы будут недоступны для изменения без пароля.

Для снятия защиты нажмите на вкладке "Рецензирование" на иконку "Снять защиту листа" и введите пароль.

Предоставить доступ отдельным пользователям к определённым диапазонам. Это крайне полезный функционал для командной работы, позволяющий нескольким участникам редактировать разные разделы файла, защищая остальной контент.

1. Откройте книгу Excel и выберите лист.
2. Перейдите на вкладку "Рецензирование".
3. В группе "Изменения" нажмите "Разрешить изменение диапазонов".
4. В диалоговом окне "Разрешить изменение диапазонов" нажмите "Создать...".
5. Введите "Название" для диапазона, укажите "Ссылки на ячейки" и, при необходимости, установите "Пароль диапазона".
6. Нажмите "ОК". Повторите для всех диапазонов.
7. После настройки всех диапазонов нажмите "Защитить лист..." в этом же диалоговом окне.
8. Выберите разрешенные действия на листе (как описано в пункте 1 выше) и установите общий пароль для снятия защиты листа.

Теперь пользователи смогут редактировать только назначенные им диапазоны (возможно, после ввода пароля для диапазона), а остальная часть листа будет защищена.

Для снятия защиты нажмите на вкладке "Рецензирование" на иконку "Снять защиту листа" и введите общий пароль.

ЗАКЛЮЧЕНИЕ

В цифровую эпоху безопасность офисных документов – важнейший аспект информационной защиты. Эффективное использование средств защиты гарантирует конфиденциальность, целостность и доступность информации, минимизируя риски утечек или порчи данных.

Комплексный подход, объединяющий технические, административные и юридические методы с встроенными функциями MS Office, создаёт надёжную защиту. Использование паролей, детальное разграничение доступа (на уровне книг, листов и диапазонов ячеек) – это мощные инструменты контроля цифровых активов.

Осознанное применение этих методов и постоянное повышение осведомлённости о киберугрозах являются залогом эффективной защиты офисных файлов и безопасной рабочей среды.

Список литературы:

1. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности: учебное пособие. – М.: Горячая линия – Телеком, 2019.
2. Будников С.А., Паршин Н.В. Информационная безопасность автоматизированных систем: учебное пособие. – Воронеж: Издательство им. Е.А. Болховитинова, 2019.
3. Девянин П.Н., Садердинов А.А., Трайнев В.А. и др. Информационная безопасность предприятия: учебное пособие. – М.: Горячая линия – Телеком, 2019. – 335 с.
4. Петраков А.В. Основы практической защиты информации: учебное пособие. – М.: Горячая линия – Телеком, 2019. – 281 с.
5. Стрельцов А.А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы. – М.: Горячая линия – Телеком, 2019. – 304 с.
6. Хорев А.А. Защита информации от утечки по техническим каналам: учебное пособие. – М.: МО РФ, 2019.
7.Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. – СПб.: Горячая линия – Телеком, 2019. – 384 с.
8. Язов Ю.К. Основы методологии количественной оценки эффективности защиты информации в компьютерных сетях. – Ростов-на-Дону: Издательство СКНЦ ВШ, 2019.