УДК 004.056

МЕТОДЫ ЗАЩИТЫ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ

Е.В. Ильинская, К.Е. Точоная
г. Белгород, Россия
Белгородский государственный национальный исследовательский университет

В данной статье рассматриваются ключевые методы защиты электронных документов. Приводится обзор существующих подходов с последующим выявлением коренных недостатков. Так же описываются характерные особенности применения каждого из методов. Результатом исследования является выбор оптимального подхода с использованием диаграммы Исикавы.

***Ключевые слова**: документ, электронный документ, методы защиты.*

METHODS OF PROTECTING ELECTRONIC DOCUMENTS

E.V. Ilinskaja, K.E. Tochonaja
Belgorod state national research University

This article discusses the key methods of protection of electronic documents. The review of existing approaches with the subsequent identification of fundamental shortcomings is given. The characteristic features of the application of each method are also described. The result of the study is the choice of the optimal approach using the Ishikawa diagram.

***Key words**: document, electronic document, methods of protection.*

По мере развития информационного общества каждая организация сталкивается с проблемой конфиденциальности электронных документов. Современные технологии обработки и хранения информации открывают новые возможности для пользователей, следовательно, требуют большего внимания к организации информационной безопасности.

Вне зависимости от сферы деятельности компании необходимость в защите электронных документов является ключевой потребностью, так как нарушения приватности может повлечь за собой катастрофические последствия. Во избежание ущерба каждая организация, использующая электронно-вычислительную технику, имеет возможность свести к минимуму любые поступающие угрозы.

Под электронным документом (ЭД) следует понимать структурированную информацию, которая представлена в электронно-цифровой форме. ЭД подразделяется на 2 типа: произвольные и официальные. Обычно, оказывать большую защиту требуется именно второму типу электронных документов.

В настоящее время для обеспечения комплексной защиты информации используется объединение следующих методов:

– Технический. Данный способ является универсальным, так как защита осуществляется с помощью всевозможных доступных технических средств. К данной методике относится: разграничение прав доступа, технология шифрования, цифровая подпись, резервное копирование и т.д.

– Организационный. Данный способ подразумевает правильное разграничение прав доступа к документам со стороны организации: наделение ответственных лиц особыми полномочиями.

– Правовой. Данный способ предусматривает возможность создания норм или правил внутри организации, в соответствии с которыми будет использоваться рабочая

документация. Данная методика должна основываться на законах действующего законодательства.

В данной статье рассматривается технический метод защиты информации, а именно: маркировка, пароль, доступ по цифровому ключу, системы управления правами доступа.

Для обеспечения безопасности конфиденциального документооборота используется технология скрытой маркировки. Этот способ представляет собой нанесение на документ информации, которая не видна при обычном освещении. Как правило, это: время, дата, данные о сотруднике и оборудовании. Такое внедрение в документ позволяет точно определять происхождение любого распечатанного файла.

Пароль является самым доступным и поэтому распространенным методом шифрования. Данный способ заключается в установке пароля на архив или конкретный документ. Для этого используются программы, имеющие встроенные инструменты, такие как: ограничение копирования, редактирования и печати содержимого.

Доступ по цифровому ключу подразумевает наличие у пользователя флешки или SD карты для расшифровки информации. В данном случае любой файл можно скопировать, но нельзя открыть без материального носителя.

Распространенным способом защиты электронных документов для пользователей корпоративных сетей является служба управления правами Active Directory. Документы, защищенные AD RMS, шифруются и администратор имеет возможность самостоятельно определить доступ должностного лица. К функциям данного типа шифрования относится: запрет на копирование, печать, пересылку, чтение, изменение и установление срока действия электронного документа.

Для выбора лучшего метода шифрования необходимо провести анализ каждого и выделить слабые и сильные стороны. Схема причинно-следственных связей представлена на рисунке.

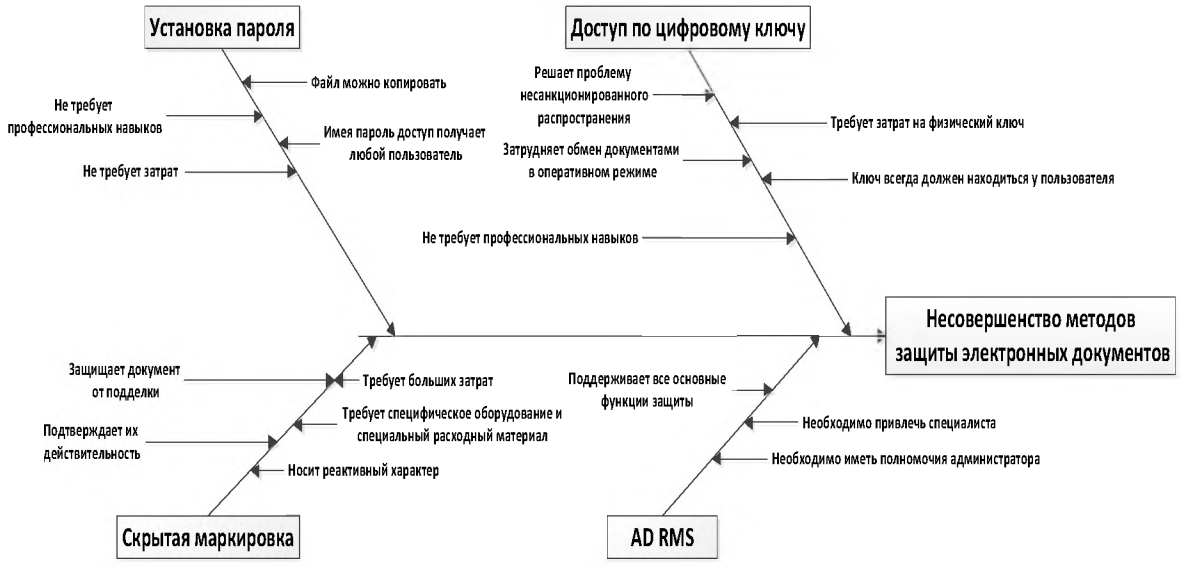

Рис. Диаграмма Исикавы

Во всех вышеперечисленных способах защиты документов есть свои достоинства и недостатки, которые отображены на диаграмме. Идеальным решением для пользователей была бы комбинация из положительных критериев, например:

– использование пароля, который можно передавать по электронной почте или каналам связи;

– отображение меток для обозначения режима распространения;

– предоставление прав доступа в режиме «онлайн»;

– использование уникального материального носителя, который не нужно часто покупать и доставлять конечному пользователю.

На сегодняшний день на рынке существует несколько решений, обеспечивающих комбинацию всех методов защиты электронных документов.

В результате данного исследования можно сделать вывод о том, что каждый пользователь должен опираться на собственные нужды и финансовые возможности: обычному пользователю незачем приобретать дорогостоящие сервисы, достаточно использовать пароли. Стоит объективно оценивать и то, что ни один из методов не может гарантировать полную и надежную защиту данных. Так же необходимо учитывать скорость работы центрального процессора, так производительность в больших компаниях может значительно снизиться.

ЛИТЕРАТУРА

1. Казакова М. Классификация и примеры современных методов защиты. Учебное пособие/ М. Казакова. – Ижевский государственный технический университет. 2010 г.

2. Электронный ресурс. Режим доступа: http://documentooborot.com.

3. Электронный ресурс. Режим доступа: https://studbooks.net/1300533/menedzhment/metody_zaschity_elektronnyh_dokumentov.

УДК 004.058

ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕГИОНА

Д.П. Коряков
г. Белгород, Россия
Департамент АПК и воспроизводства окружающей среды Белгородской области

А.С. Корякова
г. Белгород, Россия
Белгородский государственный национальный исследовательский университет

В данной статье рассмотрено понятие информационной безопасности региона. Изучены виды угроз информационной безопасности. Выделены группы лиц, оказывающих важную роль в информационной безопасности региона.

Ключевые слова: *информационная безопасность, информационная безопасность региона, регион, информация, ложная и сфальсифицированная информация, информационное пространство.*