УДК 005.21:334.012.42

Авраменко Т. О.

ассистент кафедры экономической информатики, учёта и коммерции

Гомельский государственный университет имени Франциска Скорины

Республика Беларусь, г. Гомель

РАЗРАБОТКА КОМПЛЕКСА ИНСТРУМЕНТОВ ДЛЯ ФОРМИРОВАНИЯ МОДЕЛИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОММЕРЧЕСКИХ ОРГАНИЗАЦИЯХ

Аннотация:

В статье рассмотрен вопрос, касающиеся программного обеспечение информационной безопасности в коммерческих организациях. Предложен и описан вариант разработки комплексного программного менеджера безопасности, применение которого позволит закрыть все потребности организации в обеспечении безопасности её данных.

Ключевые слова: информационная безопасность, коммерческие организации, программное обеспечение информационной безопасности, кибербезопасность, менеджер безопасности.

Avramenko T.

Assistant, Department of Economic Informatics, Accounting and Commerce

Gomel State University named after Francis Skorina

Republic of Belarus, Gomel

DEVELOPMENT OF A COMPLEX OF TOOLS FOR FORMING A MODEL FOR INFORMATION SECURITY IN COMMERCIAL ORGANIZATIONS

Annotation:

The article deals with the issue of information security software in commercial organizations. A variant of developing a complex software security manager is

proposed and described, the use of which will cover all the needs of an organization in ensuring the security of its data.
Key words: information security, commercial organizations, information security software, cybersecurity, security manager.

Организация обеспечения информационной безопасности в коммерческой организации – многосторонняя комплексная задача, решение которой возможно только в ситуации, когда система грамотно организована, охватывает важнейшие направления деятельности организации и функционирует на каждом уровне управления, не допускает сбоев, ошибок и некорректной работы, а также не позволяет воздействовать на компьютерную систему (далее - КС) организации извне [1].

Для защиты КС организации предлагается разработка программного обеспечения – специализированного программного менеджера безопасности, который сможет закрывать все потребности коммерческой организации в обеспечении информационной безопасности.

Менеджер безопасности должен быть способен решать следующие задачи по обеспечению информационной безопасности:

– обеспечивать контроль входа в корпоративную информационную систему и КС, а также контроль загрузки баз данных;

– обеспечивать ограничения доступа пользователей к определенным компонентам корпоративной информационной системы и КС;

– защищать применяемое в организации программное обеспечение,;

– обеспечивать безопасность потоков конфиденциальных данных;

– обеспечивать защиту информации от воздействия вирусного программного обеспечения;

– уничтожать остаточные данные конфиденциального характера;

– хранить и своевременно заменять пароли и коды доступа пользователей;

– обеспечивать целостности данных;

– автоматически обеспечивать безопасность работы пользователей корпоративной информационной системы и КС на основе данных протоколирования информации.

Предлагаемый программный менеджер безопасности объединяет в себе три отдельных вида программ: менеджер доступа, антивирусное и шифровальное программное обеспечение (далее - ПО). Такой вариант объединения различных направлений защиты данных в одну программу при их совместной и согласованной работе будет более эффективен и надёжен по сравнению с использованием отдельного ПО для разных задач, т.к. позволит сразу контролировать всё аспекты защиты КС организации.

Рассмотрим каждую структурную единицу менеджера безопасности.

I Менеджер доступа – это структурная единица менеджера безопасности, которая непосредственно взаимодействует с пользователями КС организации. Выполняет функцию управления и хранения данных для идентификации и аутентификации сотрудников в КС организации и всемирной сети Интернет. Менеджер доступа обеспечивает и ограничивает доступ сотрудников к тем или иным ресурсам и файлам в зависимости от уровня доступа сотрудника. Уровень доступа назначается при приёме на должность. При увольнении сотрудника с должности или понижении уровня доступа, менеджер уведомляет администратора о необходимости смены паролей к ресурсам, с которыми взаимодействовал уволенный сотрудник. Менеджер также регулирует наличие у сотрудника возможности загружать, просматривать, изменять, копировать и удалять данные из КС организации в зависимости от его уровня.

Кроме того, в задачи менеджера доступа входит генерация одноразовых и долговременных уникальных паролей к тем или иным ресурсам КС организации и всемирной сети Интернет, а также их самостоятельный ввод при наличии подтверждения операции от сотрудника

и открытом доступе. Программа также отслеживает, какие данные и ресурсы использовались сотрудником, оценивает безопасность внешних ресурсов, предупреждая пользователя, а при нарушениях режима безопасности уведомляет администратора.

II Антивирусное ПО – программа для обнаружения, идентификации и устранения вирусов с компьютера или другого устройства. ПО обеспечивает безопасность организации совершении операций во всемирной сети при просмотре страниц, передаче и загрузке файлов и данных. Антивирусное ПО менеджера безопасности работает в фоновом режиме в КС организации, проверяя каждый открываемый и загружаемый файл. Также антивирусное антивирус выполняет «эвристическую» проверку, проверяя программы на наличие типов плохого поведения, которые могут указывать на новый неизвестный вирус. При этом файлы сканируются всякий раз, когда они используются. Кроме сканирования при доступе антивирусное ПО также производит полное сканирование или мониторинг КС организации. При обнаружении вредоносных программ антивирус может: попытаться «вылечить» файл, удалив вредоносный код, поместить файл в карантин, чтобы «вылечить» позже или удалить, удалить файл, если «вылечить» не удалось, получить отчёт об обнаружении вируса, но больше ничего не делать, игнорировать обнаруженный вирус. Также функционирует в виде браузерного расширения.

III Шифровальное ПО – это кодирует информацию, после чего ее нельзя прочесть без специального ключа. В коммерческих организациях шифрование необходимо использовать для защиты сообщений корпоративной электронной почты и сообщений, передаваемых по локальным каналам КС при открытом доступе в Интернет.

Шифрование работает по следующей схеме. Ясно читаемое сообщение шифруется и превращается программой в некий набор символов, затем полученный набор символов передаётся адресату через сеть

Интернет, где посторонние не смогут прочитать текст из-за кодирования и неизвестного ключа, когда адресат получает сообщение, оно дешифруется согласно имеющемуся ключу и набор символов превращается в ясно читаемое сообщение. В шифровальном ПО, для обеспечения максимально эффективной защиты корпоративной переписки, выбирается ассиметричный тип шифрования. Данная структурная единица менеджера безопасности работает полностью в фоновом режиме.

Менеджер безопасности устанавливается на сервер организации, может работать в автономном режиме, управляется администратором при согласовании некоторых операций по защите данных с лицом, ответственным за информационную безопасность в организации.

Таким образом, предлагаемый в качестве решения защиты информации менеджер безопасности закрывает все потребности компании по обеспечению информационной безопасности. Предлагаемое программное обеспечение позволяет контролировать доступ сотрудников к информации организации и уровень взаимодействия с ней, обеспечивает защиту КС от вредоносных программ, шифрует входящие и исходящие данные, защищая информацию от злоумышленного вмешательства со стороны.

Научное исследование выполнено в рамках темы «Информационная безопасность учётно-аналитической системы стратегического управления в бизнесе» при финансовой поддержке Белорусского республиканского фонда фундаментальных исследований.

Использованные источники

1. Диогенес, Ю. Кибербезопасность: стратегии атак и обороны / Ю. Диогенес, Э. Озкайя - М.: ДМК-Пресс, 2020. – 326 с.