ВЫБОР ПРОГРАММНО-АППАРАТНОГО СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

SELECTION OF SOFTWARE AND HARDWARE MEANS OF INFORMATION PROTECTION

УДК 004.45

Акулов Артем Алексеевич, магистрант, Донской государственный технический университет, г. Ростов-на-Дону

Akulov A.A. artkulov_ww@mail.ru

Аннотация

В большинстве организаций не используется защитное программное обеспечение. Данная работа посвящена мотивации к внедрению и описанию имеющегося функционала трех основных средств защиты информации от несанкционированного доступа и их сравнению с целью выбора наиболее подходящего. Так как большинство ошибок пользователей происходит из-за неосторожности и отсутствия понимания сути работы конкретного средства защиты информации, то возникает необходимость анализа предложенных нами средств защиты информации с точки зрения удобства использования и возможных ошибок. Представлено практическое применение выбранного средства защиты информации и выводы по его использованию.

Annotation

Most organizations do not use security software. This work is devoted to the motivation for the implementation and description of the available functionality of the three main means of protecting information from unauthorized access and their comparison with

the purpose of choosing the most appropriate one. Since the majority of user errors occur due to carelessness and lack of understanding of the essence of a particular information security tool, it becomes necessary to analyze the information security tools we have proposed in terms of usability and possible errors. The practical application of the chosen information security tool and conclusions on its use are presented.

Ключевые слова: информационная безопасность, информационная система, средство защиты информации, несанкционированный доступ.

Keywords: information security, information system, information security tool, unauthorized access.

Была поставлена задача, заключающаяся в выборе наиболее подходящего средства защиты информации от несанкционированного доступа (СЗИ НСД). Перед нами стоит выбор между тремя СЗИ:

- Secret Net от компании «Код безопасности»;
- Страж NT от НПЦ «Модуль»;
- Dallas Lock от ООО «КОНФИДЕНТ».

Все представленные нам программы примерно схожи по своим характеристикам и основному функционалу, вопрос об использовании конкретного СЗИ решается на основе возможности установки в целевую систему.

Под возможностью установки понимаются различия в архитектуре СЗИ и возможные требования присутствия аппаратной части. К примеру, Dallas Lock или Страж NT берут на себя весь контроль компьютером еще в момент его загрузки, ограничивая запуск ОС до тех пор, пока пользователь не идентифицируется. Однако существует различие в реализации данного механизма — Страж NT, например, использует дополнительную PCI-плату, которая устанавливается внутрь ПК. Соответственно, на ноутбук такое СЗИ не подойдет.

В большинстве организаций сетевые версии защитного ПО не используются. Если рассматривать автономные версии, то здесь на первое место можно поставить Dallas Lock за его дружелюбный к пользователю интерфейс и весьма удобную и простую настройку. Второе место занимает Страж NT, по причине более сложной

настройки и механизма мандатного контроля доступа, который немного непонятен пользователям. Третье место занимает Secret Net за его усложненный интерфейс и наибольшее число ошибок в сравнении с его конкурентами.

Ниже подробно распишем анализ, по которому были распределены представленные нам СЗИ.

Так как большинство ошибок пользователей происходит из-за неосторожности и отсутствия понимания сути работы конкретного СЗИ, то возникает необходимость анализа предложенных нам СЗИ с точки зрения удобства использования и возможных ошибок.

Secret Net.

У данного СЗИ фундаментальным свойством является создание папок с уровнем секретности «несекретно», а файлы создаются с текущим уровнем секретности сессии. Из-за этого свойства возникает множество ошибок пользователей.

Часто возникает проблема конфликта СЗИ с офисным пакетом OpenOffice.org, что нарушает работу с такими программами как Word и Excel.

В случае, когда на компьютере разрешено использовать USB-флеш-накопители, иногда возникает проблема во время копирования больших объемов данных, рассортированных по папкам. В случае если использование флэшек запрещено, то при попытке ее использования компьютер будет заблокирован.

Страж NT.

В представленном СЗИ меньше возможных проблем чем в предыдущем, что говорит о более дружелюбном к пользователю механизму защиты.

Во время использования данного ПО непонимание возникает из-за важности выбора уровня секретности для каждого приложения отдельно и невозможности передавать какие-либо права стандартному проводнику, что требует установки дополнительного лицензированного ПО.

Также при открытии документа Word/Excel первым делом появляется окно выбора уровня секретности, а далее появляется окно выбранного редактора, однако без запрошенного нами документа.

Dallas Lock.

Как и предыдущее СЗИ, Dallas Lock имеет небольшое количество ошибок таких как: система иногда отрицает правильные пароли, пропадает параметр «категория конфиденциальности» с окна логина и ошибка во время привязки электронного идентификатора.

Первая ошибка возникает из-за использования двух паролей — для Dallas Lock и Windows.

Вторая связана со стандартным скрытием поля для выбора грифа сеанса.

В случае с электронным идентификатором, то во время его привязки может возникать ошибка, если эту операцию делают для администратора, или при использовании токена, не подходящего по версии.

Таким образом, на основе представленного выше анализа, по функционалу Dallas-Lock является лидером среди выбранных СЗИ. Также особенностью этой системы является более дружелюбный интерфейс, что создает образ более надёжного продукта. Также Dallas-Lock имеет более привлекательную стоимость.

Для организации контроля доступа, регистрации и учета событий, и обеспечения целостности выберем Dallas Lock 8.0-K, который представляет собой систему защиты конфиденциальной информации от несанкционированного доступа в процессе её хранения и обработки, программное сочетание всевозможных средств по защите информации в ОС Windows, которое имеет возможность подключить аппаратные идентификаторы.

К основным функциональным возможностям СЗИ от НСД Dallas Lock относятся:

– разграничение прав доступа пользователей к объектам;

– установка требований к сложности паролей;

– контроль доступа к ресурсам осуществляется в соответствии со списками пользователей и их правами доступа;

– ограничение количества объектов файловой системы, доступных пользователю;

– обеспечение целостности ресурсов файловой системы и аппаратной и программной среды как при загрузке компьютера, так и по расписанию;

– запись действий пользователей;

– гарантированное удаление остаточной информации;

– разграничение доступа к съемным запоминающим устройствам;

– возможность установки замкнутой программной среды;

– возможность создания «черного списка» расширений файлов;

– возможность самостоятельно диагностировать основные функции и проверить все ли параметры совпадают;

– двухфакторная аутентификация с использованием электронных идентификаторов.

Пример использования выбранного СЗИ НСД

Приведем пример настройки некоторых функций данного СЗИ.

Для настройки входа в систему, установки атрибутов пароля, аппаратных считывателей необходимо выбрать вкладку «Параметры безопасности», закладку «Вход» (Рисунок 1).



Рисунок 1 – Параметры входа в систему

Для настройки параметров аудита необходимо выбрать вкладку «Параметры безопасности» – «Аудит». Требуемые параметры показаны на рисунке ниже (Рисунок 2).



Рисунок 2 – Параметры аудита

Для настройки параметров контроля целостности всех объектов машины необходимо открыть вкладку «Параметры безопасности» и перейти в категорию «Контроль целостности» (Рисунок 3).

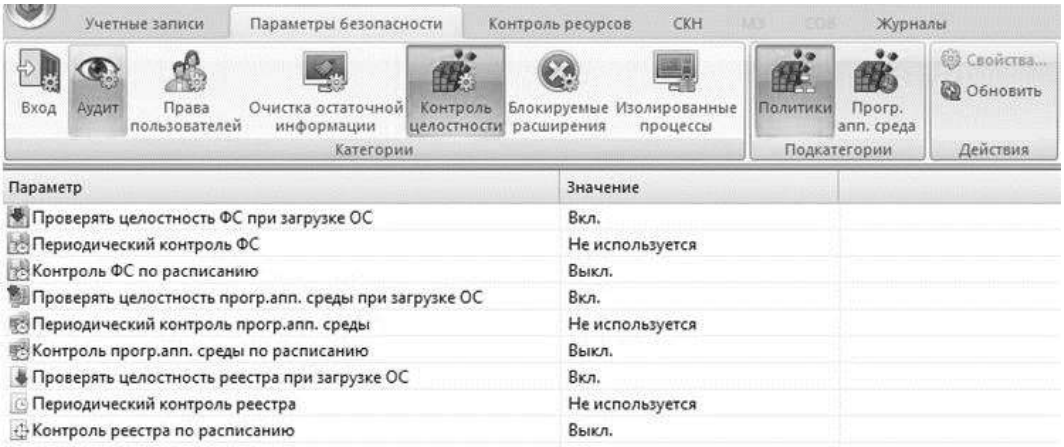

Рисунок 3 – Обеспечение контроля целостности ресурсов.

С помощью данных параметров необходимо настроить периодичность проверки целостности. По умолчанию проверка целостности машины установлена только при загрузке ОС.

- Проверять целостность машины при загрузке ОС

Параметр проверки целостности при загрузке ОС может иметь следующие значения: «включен» или «выключен».

- Периодический контроль целостности

Данный параметр позволяет производить проверку целостности через указанный промежуток времени: от 1 минуты до 5 часов. Для отключения необходимо выбрать значение «Не используется».

- Контроль по расписанию

Данный параметр позволяет настроить проверку целостности по гибкому расписанию. В окне настройки расписания необходимо установить флаг в поле «Использовать расписание», и составить расписание.

Каждое событие нарушения целостности сопровождается всплывающим сообщением на панели задач и записью в журнале, при этом в графах «Событие» и «Результат» отображается значение параметра контроля целостности.

Выбранное нами СЗИ полностью удовлетворяет потребности отдела в обеспечении двухфакторной аутентификации, ведении журнала действий пользователей, обеспечении целостности и предупреждении о различных нарушениях характерных для НСД, что позволяет значительно повысить степень защищенности данного объекта.

Литература

1. Системы защиты информации Страж NT [Электронный ресурс]. – Режим доступа: https://guardnt.ru/gnt_40.html
2. СЗИ от НСД – Разграничение доступа Secret Net [Электронный ресурс]. – Режим доступа: https://www.securitycode.ru/products/secret_net/
3. Dallas Lock – линейка сертифицированных средств защиты информации [Электронный ресурс]. – Режим доступа: https://www.dallaslock.ru

Literature

1. Information security systems Sentinel NT [Electronic resource]. - Access mode: https://guardnt.ru/gnt_40.html
2. SPI from NSD-Access control Secret Net [Electronic resource]. - Access mode: https://www.securitycode.ru/products/secret_net/
3. Dallas Lock-a line of certified information security tools [Electronic resource]. - Access mode: https://www.dallaslock.ru