Адъюнкт
Воронежского института МВД России
В.И. Арутюнова;
научный руководитель:
С.В. Скрыль

ПРОБЛЕМА ЗАЩИТЫ ИНФОРМАЦИИ В ЦЕНТРАХ ОБРАБОТКИ ДАННЫХ ОРГАНОВ ВНУТРЕННИХ ДЕЛ ОТ ВИРУСНЫХ АТАК

Наличие развитой инфокоммуникационной инфраструктуры органов внутренних дел (ОВД) определяет необходимость решения комплекса задач по защите информации элементов данной инфраструктуры от угроз несанкционированного доступа (НСД) к информации. В связи с этим становится актуальными вопросы защиты информации базовых элементов инфокоммуникационной инфраструктуры ОВД – центров обработки данных (ЦОД), аккумулирующих существенный объем информации, связанной со служебной деятельностью территориальных ОВД.

Проблема защиты информации в ЦОД ОВД серьезно актуализировалась в связи с активным применением нарушителями безопасности информации этих систем вредоносных программ, использующихся как в качестве инструмента НСД, так и в качестве инструмента для реализации так называемых вирусных атак, имеющих целью несанкционированное копирование, искажение и блокирование информации в ЦОД ОВД.

Возможности применения вредоносных программ обусловлены объективно существующими уязвимостями программного обеспечения ЦОД ОВД.

Основные этапы обеспечения безопасности ЦОД ОВД:

•построение модели угроз;

•выделение объектов, на которые могут быть направлены угрозы;

•построение модели действий нарушителя;

•оценка и анализ рисков;

•разработка и внедрение в системы ЦОД методов и средств защиты.

Согласно статистическим данным собранным за период с мая 2015 года по апрель 2016 г. компанией AVAST Software, за год база вирусных определений (видов вирусных атак) пополнилась на 3,5 млн.

Основными деструктивными действиями, выполняемыми вредоносными программами являются:

- уничтожение информации в секторах накопителей информации;
- исключение возможности корректной загрузки ОС;
- искажение кода загрузчика;
- форматирование накопителей информации;
- закрытие доступа к устройствам ввода - вывода;

- замена символов при печати текстов;

- искажение путей доступа к информации;

- создание псевдо сбойных элементов на носителях информации с целью скрытного и монопольного их использования;

- порча файлов данных;

- перезагрузка АРМ ДЛ;

- вывод на экран разнообразных сообщений, мерцаний экрана, нештатный запуск/остановка устройств и др. (компьютерное хулиганство);

- отключение периферийных устройств;

- блокирование экрана и перевод в режим ожидания ввода с клавиатуры;

- шифрование данных в системе (секторов винчестера либо отдельных файлов и файловых массивов);

- уменьшение объема оперативной памяти;

- фиксация содержимого экрана, нажатий клавиш (клавиатурные и экранные шпионы);

- блокирование записи на носители;

- уничтожение таблицы разбиения, после чего АРМ ДЛ можно загрузить только с внешнего носителя;

- блокирование запуска исполняемых файлов;

- блокирование доступа к носителям.

Реализация любым из рассмотренных способов воздействия вредоносных программ на информацию в ЦОД ОВД приводит к потенциальной возможности срыва выполнения задач, что может привести к значительному ущербу.

Антивирусные средства ЦОД ОВД входят в состав комплексов программных средств защиты информации этих систем. Применяемые в ЦОД ОВД антивирусные средства являются программными продуктами, сертифицированными ФСТЭК России и соответствуют всем нормативным требованиям по антивирусной защите.

Основными механизмами антивирусной защиты, применяемыми в ЦОД, являются: монитор, сканер, анализатор. При этом могут быть использованы механизмы антивируса Касперского, DrWeb, ESET и других производителей антивирусных средств.

Для оценки эффективности этих средств с целью обоснования требований к способам их применения одним из наиболее совершенных инструментов исследования такого рода процессов являются методы математического моделирования.

Вместе с тем анализ существующего аппарата математического моделирования процессов защиты информации от воздействия вредоносных программ дает основание констатировать, что на текущий момент в исследованиях проблем моделирования механизмов антивирусной защиты недостаточно проработаны вопросы моделирования вирусных атак. Такое по-

ложение является следствием упрощенного представления атак, как потока отказов, а характеристик механизмов защиты - как надежностных. Это, в свою очередь приводит к ошибкам в прогнозировании характеристик моделируемых антивирусных механизмов и как следствие - значительным ошибкам в оценке их возможностей.

Анализ содержания проблемы моделирования антивирусных механизмов в ЦОД ОВД позволяет утверждать, что основным фактором, оказывающим влияние на точность и адекватность моделей являются вопросы корректной математической интерпретации вирусных атак как угроз безопасности информации этих систем.

Решение данной проблемы напрямую связано с проработкой вопросов формализованного представления вирусных атак, как следствия противоправных действий по НСД к информации ЦОД ОВД. Одним из направлений исследования этих вопросов является использование методов функционального моделирования. В этой связи установлено, что в сценариях проведения нарушителями безопасности информации подобного рода противоправных действий существует ряд закономерностей, которые позволяют синтезировать функциональную модель всех возможных действий, осуществляемых с целью создания условий для возникновения и практической реализации НСД к информации ЦОД ОВД. Такая модель является основой для структурно-функционального анализа такого рода действий, позволяющих формализовать их как угрозы вирусных атак.

Несмотря на широкое использование методов теории моделирования в решении различных задач, в том числе и в решении задач обеспечения информационной безопасности, специальные исследования, связанные с разработкой методов формализации угроз вирусных атак носят крайне ограниченный характер, что требует серьезного развития данного направления теории информационной безопасности. Это предполагает разработку методической базы для исследования процессов функционирования ЦОД ОВД в условиях обеспечения их защищенности от воздействия вредоносных программ с целью обоснования эффективных мер антивирусной защиты.

Приведенный анализ проблемы формализованного представления информационных процессов в ЦОД ОВД в условиях реализации механизмов защиты информации от такого вида угроз является предпосылкой для разработки математических моделей.

Разработка математических моделей для оценки эффективности механизмов защиты информации в ЦОД ОВД от вирусных атак предполагает решение следующих задач:

1. Анализ уязвимостей информации ЦОД ОВД к воздействию вредоносных программ.

2. Разработка функциональной модели противоправных действий в отношении информации ЦОД ОВД, осуществляемых с использованием вредоносных программ.

3. Построение функциональной модели механизмов защиты информации в ЦОД ОВД от вирусных атак.

4. Разработка математической модели противоправных действий в отношении информации ЦОД ОВД, осуществляемых с использованием вредоносных программ, и математической модель механизмов защиты информации в ЦОД ОВД от вирусных атак.

5. Проведение вычислительных экспериментов по обоснованию адекватности разработанных математических моделей.

Из изложенного следует, что для достижения обозначенных целей определяются теоретические основы исследования (общая теория систем) и необходимые методики, а также выводится предполагаемый результат.