Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.056

Зуй
Андрей Константинович

Разработка методики противодействия современным угрозам информационной безопасности на базе деструктивного программного обеспечения

АВТОРЕФЕРАТ
на соискание степени магистра технических наук
по специальности 1-98 80 01 Методы и системы защиты информации, информационная безопасность

_____

Научный руководитель
Свирский Евгений Анатольевич
к.ф.-м.н., доцент ГУО «Институт повышения квалификации и переподготовки в области технологий информации и управления»

_____

Минск 2016

Введение

С деструктивным программным обеспечением сталкиваются практически все участники информационных отношений, использующие компьютерную технику. Решений способных раз и навсегда закрыть проблему борьбы с деструктивным программным обеспечением в настоящее время не существует. Системный подход при решении задач защиты информационных ресурсов позволяет в какой-то мере снизить вероятность реализации угроз создаваемых деструктивным программным обеспечением. Методики противодействия деструктивному программному обеспечению позволяют пользователям систематизировать деятельность по защите информации и снижению уровня урона (материального, морального и т.п.) при реализации угроз информационной безопасности.

Мировая экономика ежегодно несет много миллиардные убытки от преступлений в компьютерной сфере. Практически все преступления в компьютерной сфере реализуются с использованием деструктивного компьютерного обеспечения. Преступные группировки и отдельные лица целенаправленно трудятся над созданием методов и средств проникновения в информационные системы с целью получения доступа к конфиденциальной информации для незаконного извлечения выгоды. Для решения проблем противодействия деструктивному программному практически создана целая отрасль информационных технологий. Однако все усилия могут оказаться тщетными если пользователи не будут владеть элементарными знаниями в области защиты информации и соблюдать установленные требования. Необходимы методические материалы, позволяющие пользователям грамотно выстраивать свое взаимодействие с информационными системами. Однако таких разработок, ориентированных не только на конечных пользователей, но и для обслуживающего персонала информационных систем, сегодня крайне мало, да и к ним практически нет доступа.

Актуальность задачи защиты от деструктивного программного обеспечения возрастает из года в год. Помимо попыток выявления причин сложившейся ситуации с защитой от вредоносного ПО, приведен прогноз роста вредоносного ПО. В 2013 году выпущено порядка 50 млн. новых вредоносных программ, то есть 136 тысяч ежедневно, по его прогнозам в 2016 году количество новых вредоносных программ может превысить 200 млн.

Общая характеристика работы

Тема диссертационной работы соответствует подразделу 5.2. «Системные решения, архитектура, методологическое и аппаратно-программное обеспечение высокопроизводительных параллельных и распределенных информационно-коммуникационных процессов, сетей и систем, их информационная безопасность» приоритетных направлений фундаментальных и прикладных научных исследований Республики Беларусь на 2011–2015 гг., утвержденных Постановлением Совета Министров Республики Беларусь 19 апреля 2010 г., № 585.

Работа выполнялась в учреждении образования «Белорусский

государственный университет информатики и радиоэлектроники».

Объектом исследования является деструктивное программное обеспечение.

Предметом исследования являются методы и средства противодействия деструктивному программному обеспечению.

Целью диссертационной работы разработка методики противодействия деструктивному программному обеспечению

Задачи исследования.

– Классификация деструктивного программного обеспечения.

– Анализ признаков реализации угроз создаваемых деструктивным программным обеспечением.

– Разработка процедур противодействия деструктивному программному обеспечению

Научная новизна работы заключается в следующем:

Предложен общий подход к построению системы защиты от вредоносных программ на основе контроля доступа к файловым объектам по типам файлов, идентифицируемых по их расширениям.

Разработаны методы, позволяющие защищать информационную систему, как от загрузки, так и от исполнения бинарных и скриптовых вредоносных файлов.

Разработаны модели безопасной системы контроля доступа к файловым объектам, позволяющие оценить возможные способы утечки прав доступа и сформулировать требования, реализация которых обеспечивает эффективную защиту от вредоносных программ.

Основные положения диссертации обсуждались на XII Белорусско-российской научно-технической конференции «Технические средства защиты информации»

Основное содержание работы

Во Введении сформулированы актуальность работы, ее цель, решаемые задачи, основные научные результаты и положения, выносимые на защиту, приведены сведения о научной новизне и. практической ценности работы, описаны структура и объем работы.

В первой **главе «Исследование актуальности задачи защиты от деструктивного программного обеспечения»** рассмотрена классификация и проведено исследование существующих вредоносных программ и методов защиты от них. В результате показано, что в общем виде вредоносные программы следует делить на исполнимые и макро-программы, в свою очередь исполнимые делятся на бинарные, которые включают в себя загрузочные вредоносные программы, классические компьютерные вирусы, троянские программы, компьютерные черви, хакерские утилиты, потенциально нежелательные программы, и скриптовые вредоносные программы. На основании проведенного исследования существующей статистики сделан вывод в отношении того, что наиболее актуальными для защиты являются исполнимые бинарные и скриптовые файлы. Дополнительно проведено исследование способов

внедрения вредоносных программ, в результате которого сделан вывод, что рассматриваемые классы вредоносных программ предполагают обязательное сохранение файла на жестком диске перед его исполнением (чтением). Это позволило сделать вывод, что возможно использовать для зашиты от вредоносных программ методы, основанные на контроле доступа к файлам (разграничение прав доступа).

Проведено исследование существующих подходов к оценке эффективности методов и средств защиты от вредоносных программ, в результате которого сделаны выводы о невозможности с использованием известных подходов ни количественно оценить актуальность отдельной угрозы для информационной системы в целом (с учетом множества иных потенциальных угроз), в том числе угрозы занесения и запуска вредоносных программ, ни количественно оценить основные, стохастические характеристики безопасности системы от вредоносных: программ. В результате чего сформулирована задача разработки соответствующих математических моделей и последующего проведения на них исследований, позволяющих получить необходимые количественные оценки.

Во второй **главе «Оценка актуальности современных угроз на базе деструктивного программного обеспечения»** предложены подходы к количественному оцениванию актуальности угрозы (задачи защиты от вредоносных программ) и к количественному оцениванию эффективности средств защиты. Для оценивания актуальности задачи защиты от внедрения и запуска деструктивных программ была использована модель атаки, как последовательность реализаций угроз на орграфе (рисунок 1), где каждая угроза характеризуется вероятностью её отсутствия.

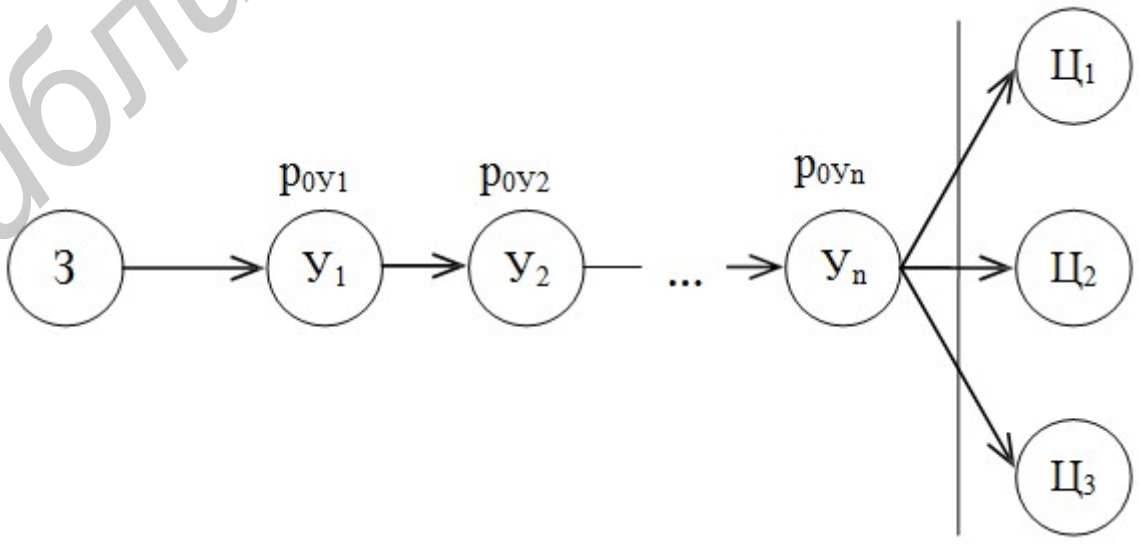

Рисунок 1 - Представление атаки на графе

На орграфе дуги указывают последовательность реализации угроз при совершении атаки, вершина «З» - злоумышленник, вершины «Уi» - угрозы

(потенциальные угрозы) с заданной (рассчитанной) вероятностью их отсутствия в системе в момент осуществления атаки (отсутствия реальной угрозы), вершины «Цi» - цели атаки - хищение (кража) информации, модификация информации или отказ в доступе.

Для того, чтобы совершить переход из начального состояния «З» в конечные состояния «$Ц_1$», «$Ц_2$» и «$Ц_3$» злоумышленник должен последовательно реализовать все угрозы (угрозы должны быть реальными) на его пути следования (реализовать все этапы атаки). В результате данное представление можно интерпретировать как схему параллельного резервирования, где каждый узел представляет собой резервирующий элемент. Из схемы, где была добавлена угроза преодоления средства зашиты информации (СЗИ), была получена следующая расчетная формула построенной модели, позволяющая оценить вероятность возможности успешного осуществления атаки:

$$p_{0осуща} = (1 - p_{0СЗИ}) * \prod_{i=1}^{n} (1 - p_{0уi})$$

где *Росзи*- вероятность отсутствия угрозы в средстве защиты информации;

p_{oyi} — вероятность отсутствия i-й угрозы в информационной системе, i=1,..., n.

Актуальность угрозы, определяемой на орграфе совокупности атак на вычислительную систему (рисунок 2) характеризуют число атак, позволяющих перейти в данное состояние и число атак, исходящих из данного состояния. Введем критерий актуальности угрозы, определяемы коэффициентом $К_а$.

$$К_а = U*S$$

где

U – количество атак, входящих в вершину угрозы на орграфе;

S – количество атак, исходящих из вершины угрозы на орграфе.

На основании информации, полученной из отчетов компаний ESET, Cisco, Лаборатории Касперского, большинством атак за прошедший 2013 год использовались вредоносные программы. Проиллюстрируем результаты проведенного исследования - представим наиболее часто реализуемые атаки соответствующим орграфом (рисунок 2).

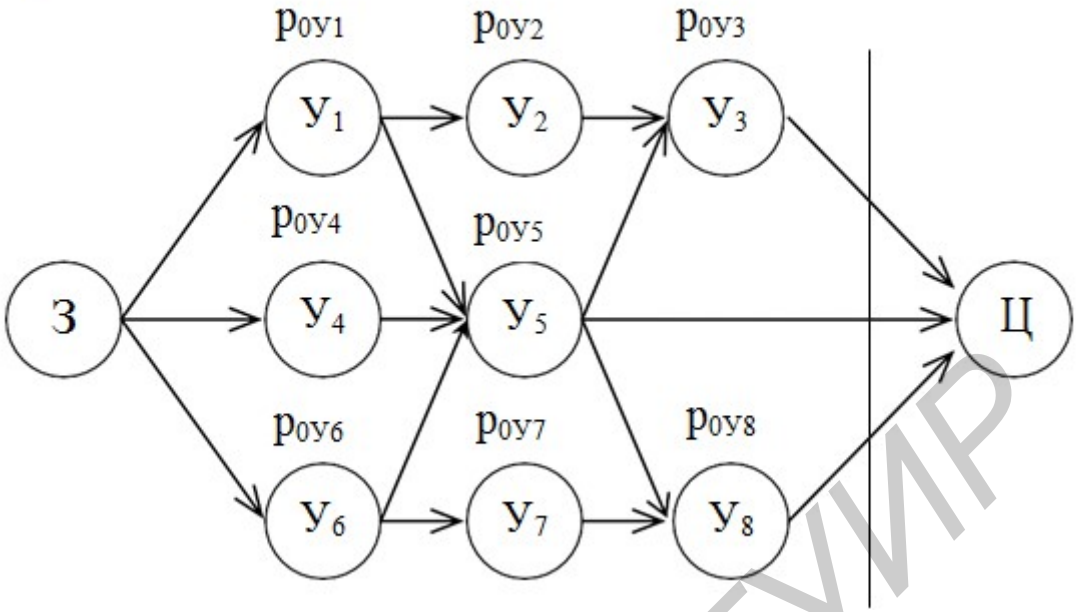

Рисунок 2 – Представление атак на вычислительную систему орграфом

На орграфе дуги указывают последовательность реализации угроз при совершении атак, вершина «З» - злоумышленник, вершины «Уi» - угрозы: «$У_1$» - угроза взлома веб-сайта или сервера, «$У_2$» — угроза вскрытия или перехватывания паролей, «$У_3$» — угроза компрометации файлов ОС, «$У_4$ - угроза социальной инженерии, «$У_5$» - угроза внедрения вредоносного ПО, «$У_6$» - угроза повышения привилегий, «$У_7$» - угроза уязвимости в протоколе сетевого взаимодействия, «$У_8$» - угроза уязвимости в сети, вершина «Ц» -хищение (кража) информации, модификация информации или отказ в доступе.

Представим, что средством защиты нивелируется первая угроза ($У_1$), тогда коэффициент $К_а$ будет равен 2, если же нивелировать пятую угрозу ($У_5$), коэффициент $К_а$ будет равен 9 и соответственно будет реализована защита от девяти потенциальных атак.

Полученный результат в отношении актуальности . угрозы деструктивных программ достаточно просто объясним, поскольку для того, чтобы злоумышленнику совершить атаку, ему нужен некий инструментарий для осуществления запланированных им действий. Именно вредоносная программа предоставляет злоумышленнику возможность дальнейшего осуществления атаки.

Для количественного оценивания эффективности современных антивирусных средств защиты была предложена математическая модель в виде системы массового обслуживания (СМО) M/M/C (пуассоновский входящий поток, экспоненциальное распределение, С — количество обслуживающих приборов — количество вирусных аналитиков, обеспечивающих выявление сигнатуры вредоносной программы - нивелирование угрозы), расчетная формула для которой:

$$p_0 = \left(\sum_{n=0}^{C} \frac{(\lambda/\mu)^n}{n!} + \frac{(\lambda/\mu)^{C+1}}{C!\,(C-\frac{\lambda}{\mu})}\right)^{-1}$$

где *ро* - вероятность отсутствия заявок в СМО, под заявками

понимаются новые обнаруженные вредоносные программы;

C - количество обслуживающих приборов — количество аналитиков, обеспечивающих выявление сигнатуры вредоносной программы;

λ - интенсивность поступления заявок на обслуживание в СМО (интенсивность обнаружения новых деструктивных программ);

μ - интенсивность обслуживания заявок, поступающих в СМО (выявления сигнатур новых деструктивных программ).

Из соответствующих аналитических отчетов была определена интенсивность появления новых деструктивных программ, для различного задаваемого количества обслуживающих приборов (работающих в антивирусной компании аналитиков) рассчитывалась вероятность отсутствия заявок в СМО и среднее время обслуживания заявки в условиях стационарности СМО. В результате проведенное исследование показало (рисунок 3), что если в системе 1000 обслуживающих приборов, то стационарное состояние достижимо в случае среднего, времени обслуживания одной заявки не более 13 минут, при этом средняя длина очереди составляет 7300 заявок. Если же среднее время, обслуживания одной заявки увеличивается до 65 минут, то для обеспечения стационарного, режима СМО уже необходимо 5000 обслуживающих приборов (5000 вирусных аналитиков в одной компании). В результате сделан вывод в отношении того, что моделируемая система антивирусной защиты должна описываться нестационарной СМО, для которой очередь заявок на обслуживание и время обслуживания заявок бесконечно возрастают.

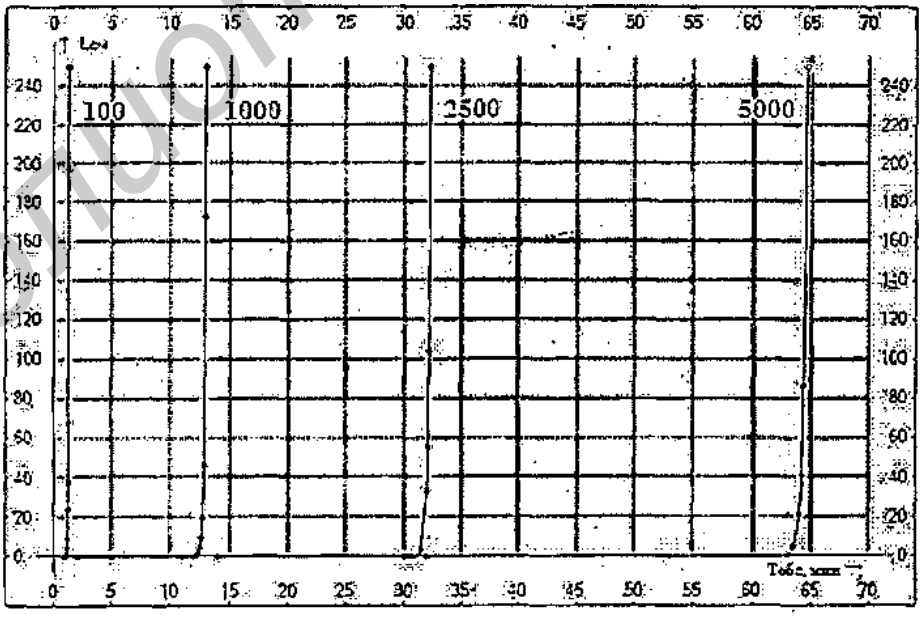

Рисунок 3 - Графики зависимости – средней длины очереди от среднего времени обслуживания заявок

Для количественной оценки значений основных характеристик антивирусных средств защиты — среднего времени ожидания новой вредоносной программы в очереди на обслуживание (выявление сигнатуры) $T_{оч}$ и средней длины очереди $L_{04)}$ проведено моделирование в условиях, близких к нестационарным. Расчет производился по формулам:

$$L_{оч} = \frac{(\lambda/\mu)^{C+1} p_0}{C * C! (1 - \lambda/C\mu)^2}$$

$$T_{оч} = \frac{L_{оч}}{\lambda},$$

где p_0 - вероятность отсутствия заявок в СМО, под заявками понимаются новые вредоносные программы

C — количество обслуживающих приборов - количество аналитиков, обеспечивающих выявление сигнатуры,

λ – интенсивность поступления заявок,

μ – интенсивность обслуживания заявок.

В результате моделирования получено, что, если среднее время обслуживания заявки (выявления сигнатуры) составляет 64,808 мин, с учетом интенсивности поступления заявок - 77,15 заявок в минуту (стационарность системы обеспечивается при числе обслуживающих приборов, равном 5000). средняя длина очереди равна 79529,91, а среднее время ожидания в очереди составляет 1030,85 мин. Если же среднее время обслуживания заявок увеличить лишь на 0,0007 мин (42 мс), то средняя длина очереди и время ожидания вырастут в 7 раз. Это наглядно иллюстрирует, что используемая сегодня на практике характеристика эффективности антивирусных средств защиты – среднее время обслуживания заявки (выявления сигнатуры) никоим образом не отражает реального положения дел.

На основании проведенных исследований сделан вывод о принципиальной невозможности построения эффективной защиты от деструктивных программ с использованием известных методов антивирусной защиты, что указывает на необходимость разработки новых подходов к защите, основанных на иных принципах, и новых методов, защиты от деструктивных программ.

В третьей **главе «Предлагаемые модели и методы защиты от деструктивных программ»** предложен общий подход к защите от деструктивных программ на основе контроля доступа к файлам по их типам. Основная идея предлагаемого подхода защиты состоит в том, что объекты доступа определяются по их расширениям (исполнимые, системные или информационные); исключается любая возможность несанкционированной модификации заданных объектов; исключается

любая возможность несанкционированного удаления заданных объектов; исключается любая возможность создания заданных объектов; только заданные объекты доступа разрешается исполнять.

Предложено строить защиту от деструктивных программ на основе дискреционной модели разграничения доступа к объектам файловой системы. Для анализа безопасности системы защиты, реализующую дискреционную политику безопасности, использовалась модель Харрисона — Руззо — Ульмана. Для заданной модели начальное состояние $Q_0 = (So, O_0, M_o)$ является безопасным относительно права г, если не существует применимой к Q_o последовательности команд, в результате которой право г будет занесено в ячейку матрицы М, в которой оно отсутствовало в состоянии Q_0. Другими словами это означает, что субъект никогда не получит право доступа г к объекту, если он не имел его изначально. Если же право г. оказалось в ячейке матрицы М, в которой оно изначально отсутствовало, то говорят, что произошла утечка критичного права г по объекту доступа. Также может произойти утечка права доступа по субъекту в случае повышения привилегий пользователя. Другими словами это означает, что субъект доступа, олицетворяясь с пользователем с административными правами, получает все права доступа соответствующие администратору, при этом изменения матрицы доступа не происходит. Модель строится для оценки; и формирования требований к построению безопасной системы и предотвращению утечки прав доступа.

В работе предлагаются семь методов, учитывающих возможность контроля расположения исполнимых файлов, возможность администрирования при работающей системе защиты, возможность контроля модификации объектов доступа, контроля переименования объектов доступа, возможность защиты от скриптовых деструктивных программ, в том числе с учетом возможности наделения вредоносными свойствами интерпретаторов (виртуальных машин).

Пример разработанной матрицы доступа М для метода защиты с дополнительной защитой от скриптовых исполнимых файлов:

M=	$O_{испл}$ … $O_{испq}$	$O_{систl}$ … $O_{систm}$	$O_{инфl}$ … $O_{инфn}$
S_1	Чт, В, ~~ЗпН~~, ~~ЗпС~~, ~~Пи~~, ~~ПвИ~~, ~~У~~	Чт, ~~ЗпН~~, ~~ЗпС~~, ~~Пи~~, ~~ПвИ~~, ~~У~~	Чт, ЗпН, ЗпС, ~~Пи~~, ~~ПвИ~~, ~~У~~
…	…	…	…
S_k	Чт, В, ~~ЗпН~~, ~~ЗпС~~, ~~Пи~~, ~~ПвИ~~, ~~У~~	Чт, ~~ЗпН~~, ~~ЗпС~~, ~~Пи~~, ~~ПвИ~~, ~~У~~	Чт, ЗпН, ЗпС, ~~Пи~~, ~~ПвИ~~, ~~У~~
А	Чт, Зп, В	Чт, Зп	Чт, Зп

В качестве субъектов доступа (СД) выступают пользователи системы

и отдельно Администратор S_i;: S = {S_1 ..., S_k, A}. Объекты доступа (ОД) делятся на исполнимые, системные и информационные: O = {$O_{исп1}$,…, $O_{испq}$, $O_{сист1}$,…, $O_{систm}$, $O_{инф1}$, ..., $O_{инфn}$}. Под исполнимыми ОД понимаются файлы, содержащие в себе готовые к запуску программы, то есть рассмотрим только бинарные исполнимые файлы. Под системными ОД понимается файл, необходимый для функционирования операционной системы или программного обеспечения, за исключением исполнимых ОД. В качестве системных объектов выступают файлы с расширениями: *.config,. *.manifest, *.fon., *.ttf, *.log. Под информационными ОД понимается любой файл, за исключением исполнимого и системного файла. В качестве объектов доступа выступают файлы с определенными расширениями, например: *.exe. Конечный набор прав включает в себя: R = {Чт, В, ~~ЗнН~~, ~~ЗнС~~, ~~Пи~~, ~~ПвИ~~, ~~У~~} (вычеркивание означает запрет). В предлагаемом методе право доступа «Запись» разделяется на создание нового объекта доступа и изменение- существующего объекта доступа путем переименование. Запрет создания нового обозначается «~~ЗнН~~» и изменение существующего — «~~ЗнС~~». Для учета различия между правом переименования существующего исполнимого файла от права переименования, например, информационного файла, запись которого. разрешена, в исполнимый файл был дополнительно добавлен запрет переименования существующего исполнимого файла (обозначается «~~Пи~~»), запрет переименования в исполнимый файл (обозначается «~~ПвИ~~»).

Предложенный метод заключается в следующем:

- для субъекта доступа Администратор:
  - разрешать чтение, запись (установка) и выполнение исполнимых ОД;
  - разрешать чтение, запись (установка) системных ОД;
  - разрешать чтение и запись информационных ОД;
  - все остальное запрещать.
- для всех остальных субъектов доступа:
  - разрешать чтение и выполнение только тех исполнимых ОД, которые уже находятся на системном диске;
  - запрещать создания нового ОД, изменения существующего ОД, переименование существующего исполнимого ОД и в существующий ОД, удаление существующих исполнимых ОД на системном диске;
  - разрешать чтение для системных ОД;
  - запрещать для системных ОД создание нового ОД, изменение существующего ОД, переименование существующего ОД и в существующий, удаление;
  - разрешать для информационных ОД чтение и запись;
  - запрещать для информационных ОД переименование существующего ОД и в существующий, удаление;

- все остальное запрещать.

На данной модели были исследованы возможные варианты утечки прав доступа. Было определено, что в общем случае их существует три варианта: при создании нового объекта доступа, при повышении прав доступа субъекта до административных, при существовании сущности «Владелец». Первый вариант утечки прав доступа невозможен, так как объекты доступа задаются их типами (расширениями). Для предотвращения второго варианта утечки прав доступа следует контролировать процесс олицетворения (смены имени пользователя при запросе доступа к файлу). Третий вариант утечки прав доступа невозможен, так как используется принудительное управление потоками информации и «Владелец» исключен из схемы администрирования.

Сформулированы требования к реализации механизмов защиты и к назначаемым разграничительной политикой. правилам доступа, выполнение которых позволит построить безопасную систему, что обосновано на построенных моделях. К подобным требованиям относится следующее: объекты доступа должны задаваться масками, как следствие, правила доступа должны назначаться не к объектам субъектов, в качестве их атрибутов, субъектам к объектам - матрица (таблица) прав доступа субъектов к объектам должна храниться в отдельном файле, для разделения объектов на исполнимые, системные и информационные по расширениям, должна использоваться маска «*.тип файла (расширение)», субъект доступа должен задаваться тремя сущностями первичный пользователь, эффективный пользователь и процесс, должны задаваться правила смены пользователя (первичного на эффективный) и их выполнение должно контролироваться при каждом запросе доступа, правило для объекта запрета на его переименование должно запрещать и переименование любого иного файлового объекта в данный файловый объект (в объект с данным расширением файла), а также создание нового объекта доступа с заданным расширением.

Четвертая **глава «Реализация разработанных методов защиты»** посвящена практической реализации предлагаемых методов защиты и разработке политик безопасности, обеспечивающих их практическое применение.

Предлагаемые методы реализованы в средстве защиты КСЗИ «Панцирь+» для ОС Microsoft Windows. Предлагаемые методы реализованы в двух механизмах защиты: «Управление олицетворением» и «Управление доступом к статичным объектам ФС».

Механизмом защиты «Управление олицетворением» реализуется правило, запрещающее олицетворение всех субъектов доступа с пользователем Администратор, для которого согласно предложенному методу разрешается запись исполнимых файлов (рисунок 4).

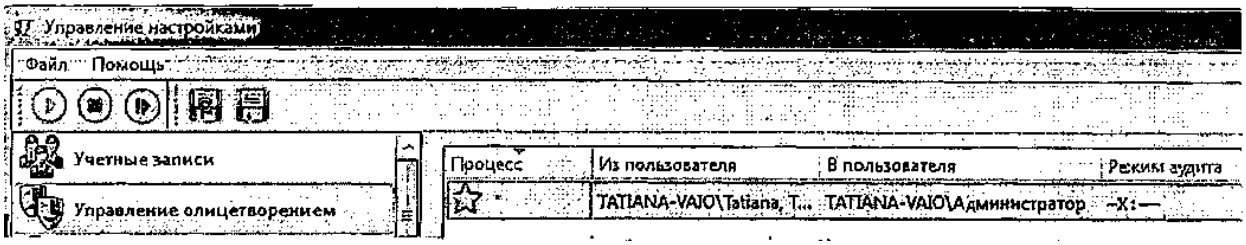

Рисунок 4 – Правило запрета олицетворения любого пользователя с пользователем- администратором

Механизмом защиты «Управление доступом к статичным объектам ФС» реализуются разграничительные политики доступа - задаваемые правила контроля доступа к файлам по их расширениям. Настройка апробированной разграничительной политики доступа состоит в следующем. Создаются два субъекта доступа, один является Администратором системы (первичный и эффективный пользователь - Администратор, процесс задается маской «*» – Любой процесс), другой предназначен для задания разграничительной политики доступа для всех остальных пользователей системы (первичный и эффективный пользователь задается маской «*» - Любой пользователь, процесс задается маской «*» - Любой процесс) (рисунок 5).

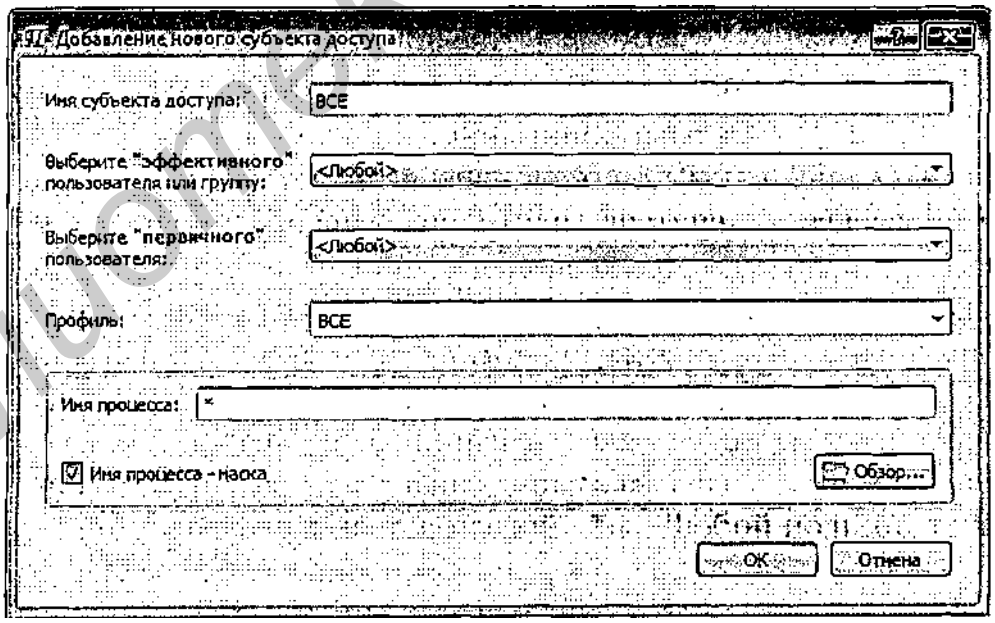

Рисунок 5 - Создание субъекта доступа и профиля защиты «Любой»

С использованием соответствующих масок создаются объекты доступа, к которым требуется соответствующим образом разграничивать права доступа субъектов (рисунок 6).

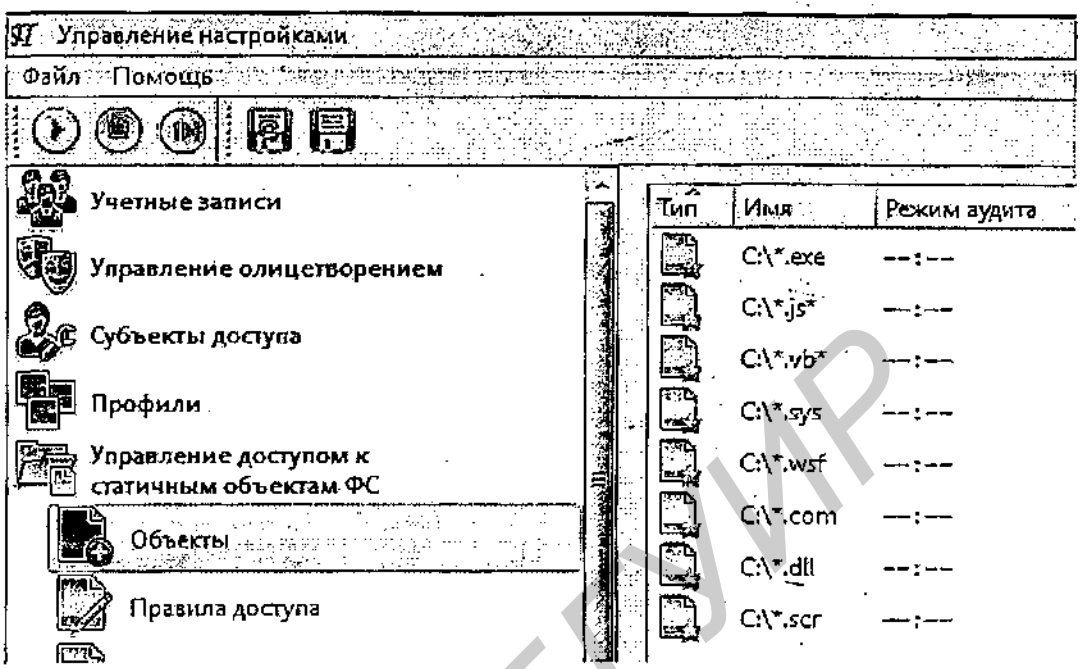

Рисунок 6 – Созданные объекты доступа

Назначаются правила доступа (разграничения прав доступа) субъектов к объектам, направленные на реализацию • предлагаемых методов защиты (рисунок 7)

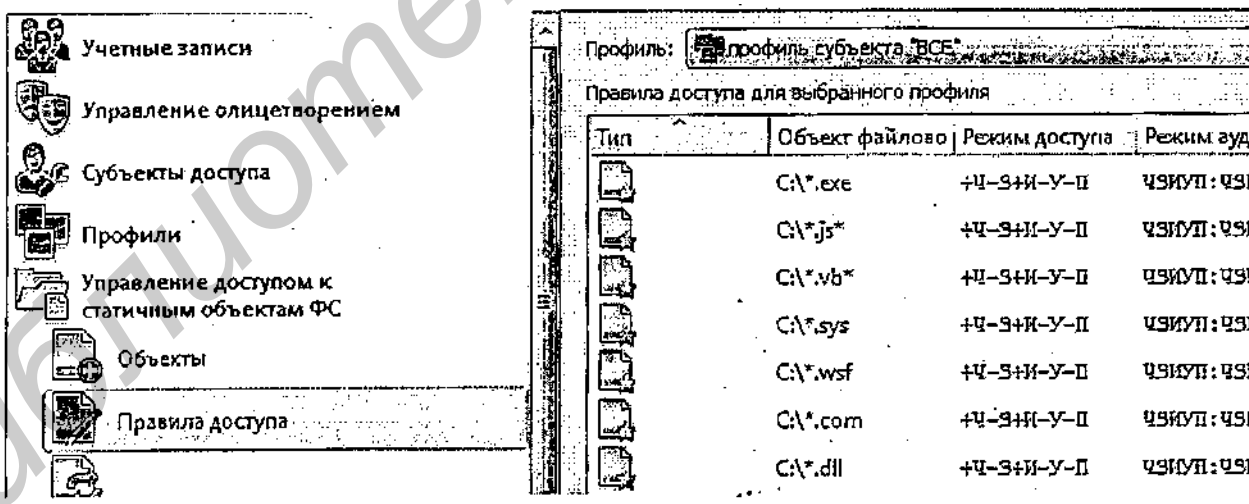

Рисунок 7 — Реализованная разграничительная политика доступа

Разработанные и апробированные разграничительные политики доступа подтверждают возможность практической реализации разработанных методов, а также иллюстрируют простоту администрирова ния, и эксплуатации реализующего их средства защиты.

В пятой **главе «Оценка эффективности защиты»** для оценки эффективности разработанных методов был определен обеспечиваемый ими потенциальный уровень защиты и условия, при

которых он будет обеспечен, кроме того определено, как скажется на загрузку вычислительных ресурсов внедрение в систему разработанных методов защиты.

Для оценки эффективности защиты был построен, орграф атаки, на котором были исследованы альтернативные варианты реализации защиты информации. В данном орграфе вершины, в том числе, включаемая в граф по одному из рассматриваемых вариантов вершина, соответствующая средству защиты, взвешены вероятностями отсутствия соответствующих угроз, дуги указывают последовательность использования угроз, в том числе, угроз, вносимых средством защиты, при совершении атаки; на информационную систему, иными словами показывают процесс использования уязвимостей и преодоления средства зашиты. Альтернативными рассмотренными вариантами использования СЗИ являются: средство защиты нивелирует угрозу, средство защиты предотвращает последствия реализации угрозы, средство защиты и нивелирует угрозу, и предотвращает последствия реализации угрозы. В нашем случае (при использовании разработанных методов защиты) функционал одного средства защиты информации включает в себя, как возможность предотвращения внедрения вредоносной программы (нивелирование угрозы), так и возможность предотвращения последствий от проведенной атаки -запуска внедренных деструктивных. программ. В результате была построена схема параллельного резервирования, с использованием которой был сделан вывод о том, что с точки зрения обеспечиваемого уровня безопасности. рассматриваемые альтернативные решения эквивалентны.

Для оценки потенциального уровня защиты, обеспечиваемого разработанными методами, и определения, при каких условиях он достижим, использована модель СМО M/M/C (пуассоновский входящий поток, экспоненциальное распределение, C – количество обслуживающих приборов), позволяющая сформулировать требования к эксплуатационным параметрам средства защиты – к интенсивности обнаружения уязвимостей в средстве защиты, позволяющих осуществить успешную атаку, и интенсивности их устранения, выполнение которых обеспечивает необходимые для современных информационных систем значения эксплуатационных характеристик средства защиты.

С использованием разработанной модели. средства защиты (исследовались худшие условия, определяемые равенством $C = 1$) показано, что при интенсивности обнаружения уязвимостей в средстве защиты – угроз преодоления защиты, составляющей *1* – 3 раза в год при продолжительности устранения уязвимости в средстве защиты, составляющей 3-7 суток (данные значения достижимы на практике), значение вероятности готовности средства защиты к безопасной эксплуатации составляет 0,96 - 0,99, значение же среднего времени наработки на отказ безопасности средства защиты при этом составляет от

полу года до двух лет.

Проведено, исследование влияния средства защиты, позволяющего реализовать разработанные методы, на загрузку вычислительных ресурсов информационной системы - на загрузку центрального процессора (ЦП) вычислительной системы. Показано, что дополнительная загрузка ЦП в режиме запуска, приложения не превышает 23%, а в штатном режиме работы приложения не превышает. 17%, при этом время запуска приложений увеличивается не более чем на 4 с, что является незначительным. Адекватность полученных результатов подтверждена статистической обработкой экспериментов.

В результате проведенных исследований сделан вывод о существенном превосходстве предлагаемых методов защиты от деструктивных программ, основанных на реализации контроля доступа к файловым объектам по их типам, над известными методами антивирусной защиты по обеим ключевым характеристикам: эффективность защиты и загрузка вычислительных ресурсов информационной системы.

Заключение

Главный научный результат выполненной диссертационной работы заключается в развитии методов защиты от деструктивных программ в современных информационных системах, состоящем в разработке методов защиты, основанных на реализации контроля доступа к файлам по их типам, идентифицируемым расширениями файлов, существенно превосходящих известные методы антивирусной защиты, как по эффективности защиты, так и по мере влияния на загрузку вычислительных ресурсов информационной системы.

В ходе решения поставленных задач было:

1. Исследована эффективность известных методов антивирусной защиты. С этой целью разработана математическая модель средства антивирусной защиты - модель системы массового обслуживания M/M/C. С использованием данной модели, с учетом существующей статистики выявления новых деструктивных программ, в частности показано, что при 1000 обслуживающих приборах (при 1000 вирусных аналитиков в компании) стационарное состояние СМО достижимо при средней продолжительности обслуживания заявки (выявления сигнатуры вредоносной программы) не превышающей 13 минут, при этом средняя длина очереди заявок на обслуживание (число деструктивных программ, для которых не выявлена сигнатура) составляет 7300 заявок, при увеличении же средней продолжительности обслуживания заявки до 65 минут, для обеспечения стационарного режима обслуживания, уже необходимо 5000 обслуживающих приборов (5000 вирусных аналитиков в одной компании). В результате проведенных исследований сделан вывод о крайне низкой эффективности известных методов защиты от

деструктивных программ.

2. Исследованы существующие способы внедрения и запуска деструктивных программ, в результате чего сделан вывод о том, что наиболее актуальными для защиты являются исполнимые бинарные и скриптовые файлы и о том, что данные классы деструктивных программ предполагают обязательное сохранение вредоносного файла на жестком, диске перед его исполнением (чтением). Это позволило сделать вывод, в отношении того, что. защита от деструктивных программ может строиться реализацией контроля (разграничения прав) доступа к файлам.

3. Предложен общий подход к реализации защиты от деструктивных программ, основанный на реализации контроля доступа к файлам по их типам, идентифицируемым расширениями файлов. Возможность использования подобного подхода обоснована проведенным исследованием способов

4. Разработаны методы защиты от деструктивных программ, позволяющие защищать информационную систему, как от загрузки, так и от исполнения бинарных и скриптовых деструктивных файлов, отличающиеся возможностью учета расположения исполнимых файлов, возможностью администрирования при работающей системе защиты, возможностью контроля модификации объектов доступа, переименования объектов доступа, возможностью защиты от скриптовых деструктивных программ, в том числе с учетом возможности наделения вредоносными свойствами интерпретаторов (виртуальных машин).

5. Разработаны модели контроля доступа, позволившие на построенных матрицах доступа сформулировать требования к построению безопасной системы, выполнение которых предотвращает утечку заданных прав доступа субъектов к объектам.

6. Оценена эффективность разработанных методов защиты. С этой целью разработана математическая модель средства защиты - модель системы массового обслуживания M/M/C , с использованием которой определены условия, при выполнении которых достигается высокий уровень эффективности защиты. В частности показано, что при интенсивности обнаружения уязвимостей в средстве защиты - угроз преодоления защиты, составляющей 1 - 3 раза в год, при продолжительности устранения уязвимостей в средстве защиты, составляющей 3 - 7 суток (данные значения достижимы на практике), значение вероятности готовности, средства зашиты к безопасной эксплуатации составляет 0,96 - 0,99 а значение среднего времени безопасной работы (наработки на отказ безопасности) средства защиты – от полугода до двух лет.

7. Проведены испытания и оценено влияние средства защиты, реализующего разработанные методы, на загрузку вычислительного ресурса, в результате чего показано, что оно значительно ниже, чем влияние на загрузку вычислительного ресурса антивирусных средств, в частности, дополнительная загрузка центрального процессора в режиме запуска

приложения не превышает 23%, а в штатном режиме работы приложения не превышает 17%, при этом время запуска приложений увеличивается не более чем на 4 с., что незначительно сказывается на работе пользователя.

Таким образом получены следующие основные научные результаты:

I. Подход к построению системы защиты от внедрения и запуска деструктивных программ на основе контроля доступа к ресурсам по расширениям и типам файлов, модели и методы защиты информационной системы от бинарных и скриптовых деструктивных файлов на основе реализации разграничительной политики доступа к файловым объектам.

II. Модели безопасной системы, позволяющие оценить возможные способы утечки прав доступа в системе контроля доступа и сформулировать требования к построению безопасной системы. модели и методы количественной, оценки актуальности угроз и эффективности средств защиты.

Список опубликованных работ

1-А. Свирский Е.А., Бережной Ю.Г., Зуй А.К. Проблемы подготовки кадров в сфере защиты информационных ресурсов. Технические средства защиты информации. Тезисы докладов XII Белорусско-российской научно-технической конференции, 28-29 мая 2014 г., Минск. Минск БГУИР, 2014 – 80 с., стр. 74.