Инженерный вестник Дона, №2 (2021)
ivdon.ru/ru/magazine/archive/n2y2021/6812

Моделирование процессов обработки информации в автоматизированных системах специального назначения в условиях применения антивирусных механизмов резидентного типа

Е.А. Конышев

Краснодарское высшее военное училище имени генерала армии С.М. Штеменко, Краснодар

Аннотация: Решается задача повышения эффективности обработки информации в автоматизированных системах специального назначения (АС СН) в условиях применения механизмов антивирусной защиты резидентного типа, посредством разработки функциональных и математических моделей информационных процессов в АС СН в условиях применения механизмов антивирусной защиты резидентного типа и методики нахождения оптимальных временных характеристик указанных механизмов антивирусной защиты. Представлены теоретические основания и методика оптимизации временных ресурсов АС СН в интересах реализации механизмов антивирусной защиты резидентного типа. Предложены функциональные и математические модели информационных процессов в АС СН в условиях применения механизмов антивирусной защиты резидентного типа и деструктивного воздействия вредоносного программного обеспечения. Приводятся результаты вычислительного эксперимента по оценке повышения эффективности обработки информации в АС СН в условиях применения механизмов антивирусной защиты резидентного типа и деструктивного воздействия вредоносного программного обеспечения.

Ключевые слова: автоматизированные системы специального назначения, антивирусная защита, антивирусные механизмы, своевременность, защита информации, эффективность обработки информации, вычислительный эксперимент.

Непрерывное совершенствование информационных технологий, повсеместное повышение их роли, значимости и эффективности, необходимость обработки больших массивов разрозненной и разнородной информации способствуют расширению сферы применения автоматизированных систем специального назначения (АС СН) федеральными органами исполнительной власти. Данный факт требует постоянного внимания в части обеспечения своевременного выполнения возложенных на АС СН функций в различных условиях, в том числе и в условиях реализации различных деструктивных воздействий [1, 2]. Кроме того, с распространением услуг мобильного банкинга и управления счетами,

доступностью средств связи, накоплением электронных ресурсов, широким использованием облачных вычислений, наблюдается рост спроса в области услуг информационной безопасности среди различных представителей российского бизнеса [3].

В соответствии с Доктриной информационной безопасности Российской Федерации основными информационными угрозами являются:

- наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях;

- расширение масштабов использования специальными службами отдельных государств средств оказания информационно-психологического воздействия;

- широкое использование различными террористическими и экстремистскими организациями механизмов информационного воздействия на индивидуальное, групповое и общественное сознание;

- возрастание масштабов компьютерной преступности.

Высокий уровень информатизации АС СН и наличии такого широкого спектра информационных угроз, может повлечь за собой негативные последствия, выражающиеся в виде нарушения защищенности информации, циркулирующей в АС СН, что в дальнейшем, приводит к срыву выполнения задач, возложенных на федеральные органы исполнительной власти.

Наиболее распространённым средством деструктивного воздействия на информационные процессы в АС СН является применение вредоносного программного обеспечения, интенсивность воздействия которого с каждым годом возрастает. Согласно ежегодным отчетам «Kaspersky Security Bulletin», количество заблокированных уникальных вредоносных объектов в 2020 году, по сравнению с 2019 годом возросло на 35% [4, 5].

Необходимость обеспечения защиты АС СН от воздействия вредоносного программного обеспечения привела к внедрению в практику широкой номенклатуры антивирусных механизмов, условно разделяемых на следующие классы: антивирусные механизмы резидентного и сеансового типа [6].

Преимуществом технологии антивирусной защиты резидентного типа является своевременное реагирование на воздействия вредоносного программного обеспечения. Вместе с тем, резидентная технология антивирусной защиты влечет необходимость одновременного использования с программным обеспечением АС СН ее временного ресурса, что является предпосылкой конфликта по использованию данного ресурса указанными механизмами с различными целевыми функциями АС СН [7].

Указанные обстоятельства приводят к необходимости решения ряда оптимизационных задач, связанных с определением величины объема временного ресурса АС СН, необходимого для создания резидентной рабочей среды с целью использования антивирусными механизмами

Решение этих задач возможно на основе комплексного использования методов оптимизации, математического моделирования и теории информационной безопасности.

Формальная постановка задача исследования заключается в максимизации показателя эффективности реализации информационных процессов в АС СН в условиях применения механизмов антивирусной защиты резидентного типа и деструктивного воздействия вредоносного программного обеспечения:

$E \rightarrow max$, который представляет функциональную зависимость $f(\tau_{пот}, E_{(аз)}, X)$,

где E – эффективность обработки информации в АС СН;

$\tau_{пот}$ – потенциальное время реализации информационных процессов в АС СН в условиях отсутствия применения механизмов антивирусной защиты резидентного типа и деструктивного воздействия вредоносного программного обеспечения;

$E_{(аз)}$ – показатель возможностей по реализации процедур, реализуемых механизмами антивирусной защиты резидентного типа, $E_{(аз)} = k(\tau_{(аз)})$;

X – показатель возможностей по реализации угроз безопасности информации в АС СН реализуемых деструктивным воздействием вредоносного программного обеспечения;

$\tau_{(аз)}$ – время процедур, реализуемых механизмами антивирусной защиты резидентного типа.

Учитывая, что эффективность автоматизированной системы – свойство, характеризуемое степенью достижения целей, поставленных при ее создании, а эффективность деятельности федеральных органов исполнительной власти обусловлена не только тем, насколько качественная информация поступает в органы управления, а насколько своевременно и обоснованно осуществлена обработка этих данных [8], то показатели своевременности реализации соответствующих информационных процессов могут рассматриваться как показатели эффективности обработки информации в АС СН.

Таким образом, показатель E эффективности реализации информационных процессов в АС СН определяется как вероятность:

$$E=P(f(\tau_{пот}, E_{(аз)}, X)\leq \tau_{(д)}),$$

где $\tau_{(д)}$ – максимально допустимое время реализации информационных процессов в АС СН.

Сформулированная задача декомпозирована на ряд следующих частных задач:

- анализ информационных процессов в АС СН, как объекта угроз воздействия вредоносного программного обеспечения;

- формирование теоретических положений для оптимизации распределения временных ресурсов АС СН в условиях применения механизмов антивирусной защиты резидентного типа и деструктивного воздействия вредоносного программного обеспечения;

- разработка методики нахождения оптимальных временных характеристик механизмов антивирусной защиты резидентного типа;

- разработка функциональных и математических моделей информационных процессов в АС СН в условиях применения механизмов антивирусной защиты резидентного типа и деструктивного воздействия вредоносного программного обеспечения;

- проведение вычислительного эксперимента по оценке повышения эффективности обработки информации в АС СН в условиях применения указанных механизмов антивирусной защиты, за счет оптимального использования временного ресурса этих систем данными механизмами.

Рассмотрим кратко каждую из частных задач.

Используя Банк данных угроз ФСТЭК России [9], составлена характеристика 11 наиболее вероятных угроз безопасности информационным процессам в АС СН, реализуемых деструктивным воздействием вредоносного программного обеспечения.

В [10] с целью формирования теоретических положений для оптимизации распределения временных ресурсов АС СН сформулирован и доказан ряд теоретических положений.

Положение 1. Аналитическая модель характеристики полноты реализации процедур антивирусной защиты будет представлять собой монотонно возрастающую математическую функцию от величины объема временного ресурса АС СН, используемого резидентной рабочей средой.

Разработана аналитическая модель данной характеристики:

$$E_{(аз)} = 1 - \left(1 - \frac{log_2 c_{(аз)}}{log_2 C}\right)^{\frac{\tau_{(аз)}}{\tau_{(и1)}}},$$

где $\tau_{(и1)}$ – значение величины времени реализации процедуры идентификации одного признака воздействия вредоносного программного обеспечения;

$c_{(аз)}$ – число функциональных состояний вредоносного программного обеспечения, проявляющихся в виде одного контролируемого антивирусными механизмами признака;

C – число всех возможных функциональных состояний вредоносного программного обеспечения.

Положение 2. Существует оптимум величины объема временного ресурса АС СН, используемого ее резидентной рабочей средой для реализации механизмов антивирусной защиты.

При доказательстве данного положения определено выражение для вычисления среднего значения продолжительности информационных процессов, реализуемых в АС СН:

$$\tau_{(ип)1,2} = \left(\tau_{(ип)} + \tau_{(аз)}\right) + X \cdot \left(1 - E_{(аз)}\right) \cdot \tau_{(ущ)}, \qquad (1)$$

где $\tau_{(ущ)}$ - временная характеристика ущерба, наносимого деструктивным воздействием вредоносного программного обеспечения.

Продифференцировав (1) по $\tau_{(аз)}$ и приравняв полученное выражение к нулю:

$$\frac{d(\tau_{(ип)1,2})}{d(\tau_{(аз)})} = 1 + X \cdot \tau_{(ущ)} \cdot \left(\frac{ln\left(1 - \frac{ln\, c_{(аз)}}{ln\, C}\right) \cdot \ln\left(1 - \frac{ln\, c_{(аз)}}{ln\, C}\right)^{\frac{\tau_{(аз)}}{\tau_{(и1)}}}}{\tau_{(и1)}}\right) = 0,$$

разрешим полученное выражение относительно $\tau_{(аз)}$ [11] и вычислим оптимальное значение $\tau^{(опт)}_{(аз)}$ объема временного ресурса АС СН, который

может быть использован для реализации механизмов антивирусной защиты резидентного типа.

Методика нахождения оптимальных временных характеристик механизмов антивирусной защиты резидентного типа представляет собой 9 последовательных шагов. Основными этапами указанной методики являются:

- вычисление оптимального значения временного ресурса $\tau^{(опт)}_{(аз)}$, который может быть использован для выполнения процедур реализуемых механизмами антивирусной защиты резидентного типа [11];

- постановка оптимизационной задачи распределения вычисленного значения временного ресурса $\tau^{(опт)}_{(аз)}$ между реализуемыми механизмами антивирусной защиты резидентного типа $\tau^{(аз)}_{j}$. – обеспечить максимальное значение линейной функции: $L^{(аз)} = \sum_j c_j \cdot \tau_j^{(аз)}$, при ограничениях на ресурсы $\sum_j a_j \cdot \tau_j^{(аз)} \le \tau_{(аз)}^{(опт)}$;

- определение коэффициента a_j потребности ресурса для реализации соответствующего j-го механизма антивирусной защиты резидентного типа;

- определение коэффициента c_j полезности используемого ресурса при реализации соответствующего j-го механизма антивирусной защиты резидентного типа;

- получение соответствующих значений $\tau^{(аз)}_{j}$ путем решения указанной оптимизационной задачи [11].

Моделирование информационных процессов в АС СН сопряжено с необходимостью их функционального описания. Такое описание возможно получить в рамках методологии функционального моделирования. В основу функционального моделирования положена декомпозиция предметной целевой функции, и ее последовательной детализации, начиная с общего

описания. Функциональная модель нулевого уровня представляет собой целевую (системную) функцию «Информационные процессы в АС СН в условиях применения механизмов антивирусной защиты резидентного типа и деструктивного воздействия вредоносного программного». Дальнейшая декомпозиция целевой (системной) функции, и ее иерархическая детализация позволяет выявить полный набор подфункций, в данном случае функциональная модель первого уровня содержит три частные функции: «Функционирование АС СН по целевому назначению» (*N*), «Деструктивное воздействие вредоносного программного обеспечения на информационные процессы в АС СН» (*Y*) и «Защита информации механизмами антивирусной защиты резидентного типа от воздействия угроз безопасности информации, реализуемых вредоносным программным обеспечением» (*Z*). Функциональная модель второго уровня содержит 10 локальных целевых функций. Третий уровень декомпозиции целевой (системной) функции будет являться конечным, и представляется 37 локальными целевыми функциями. Полученное функциональное описание позволяет сформировать соответствующие аналитические выражения для определения средних значений композиций случайных величин исследуемых характеристик. Построение указанных аналитических выражений основывается на аддитивности математического ожидания композиции случайных величин, обладающих свойством линейности [12].

Обобщенное выражение для определения среднего значения времени реализации соответствующих информационных процессов при их последовательном выполнении:

$$\tau^{(L)} = M\left(\tau_1^{(L+1)} * \tau_2^{(L+1)} * \ldots * \tau_N^{(L+1)}\right) = \sum_{n=1}^{N} \tau_n^{(L+1)},$$

при параллельном выполнении:

$$\tau^{(L)} = M\left(p_1^{(L+1)} \cdot \tau_1^{(L+1)} * p_2^{(L+1)} \cdot \tau_2^{(L+1)} * \ldots * p_N^{(L+1)} \cdot \tau_N^{(L+1)}\right) = \sum_{n=1}^{N} p_n^{(L+1)} \cdot \tau_n^{(L+1)},$$

где τ_n – случайная величина времени выполнения соответствующей функции (N, Y, Z);

$M(.)$ – математическое ожидание от композиции случайных величин;

* – знак композиции случайных величин:

p_n – вероятность выполнения соответствующей функции (N, Y, Z);

L – уровень декомпозиции соответствующей функции.

Результатом комплексного моделирования информационных процессов в АС СН, являются представленные функциональные, математические модели и показатели эффективности информационных процессов в АС СН, позволяющие выполнить вычислительный эксперимент по оценке повышения эффективности обработки информации в АС СН, за счет оптимального использования временного ресурса этих систем механизмами антивирусной защиты резидентного типа. Результаты указанного эксперимента представлены на «рис.1».

Результаты проведенного эксперимента показывают, что при применении разработанных моделей и методики (Е пред.), при отсутствии угроз безопасности информации в АС СН, реализуемых деструктивным воздействием вредоносного программного обеспечения, наблюдается незначительное снижение (около 1 %) показателя эффективности E. Однако, при наличии такого рода угроз, применение разработанных моделей и методики позволяет повысить показатель эффективности E по сравнению со случаем, когда процессы обработки информации не оптимизированы (Е сущ.), следующим образом:

на 3,5 % при одной угрозе безопасности информации в АС СН, реализуемой деструктивным воздействием вредоносного программного обеспечения за период наблюдения;

на 7,6 % при двух угрозах безопасности информации в АС СН, реализуемых деструктивным воздействием вредоносного программного обеспечения за период наблюдения;

на 11 % при трех угрозах безопасности информации в АС СН, реализуемых деструктивным воздействием вредоносного программного обеспечения за период наблюдения;

на 14 % при более четырех угроз безопасности информации в АС СН, реализуемых деструктивным воздействием вредоносного программного обеспечения за период наблюдения.

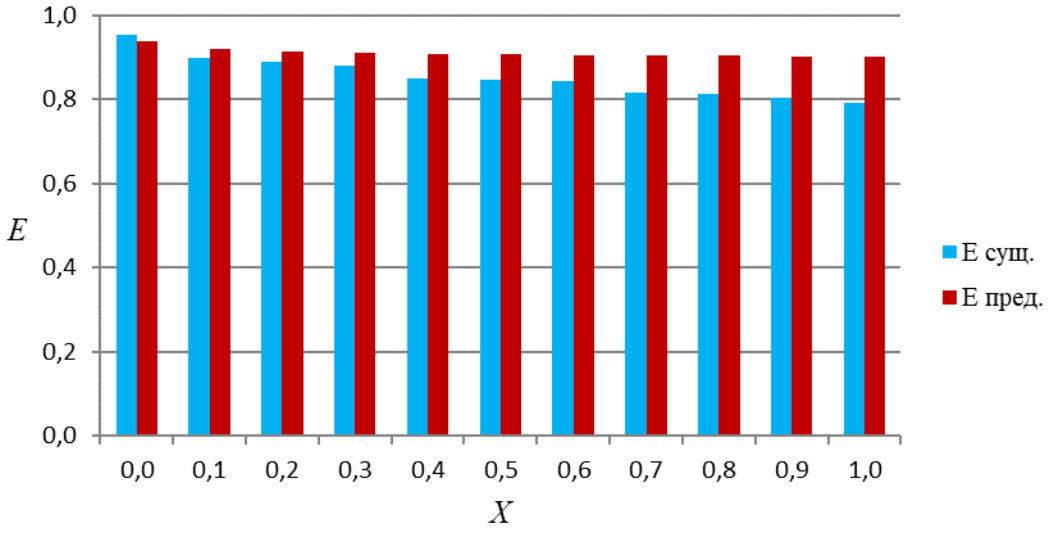

Рис. 1. – Гистограмма зависимости показателя *E* эффективности реализации информационных процессов в АС СН от показателя *X* возможностей по реализации угроз безопасности информации в АС СН реализуемых деструктивным воздействием вредоносного программного обеспечения

Таким образом, применение указанных моделей и методики позволит повысить эффективности обработки информации в АС СН в условиях применения механизмов антивирусной защиты резидентного типа и

деструктивного воздействия вредоносного программного обеспечения, за счет оптимального использования временного ресурса указанных систем рассмотренными антивирусными механизмами.

Литература

1. Дроботун Е.Б., Бердышев В.П. Защита автоматизированных систем управления военного назначения от разрушающих программных воздействий // Военная Мысль. 2016. № 10. С. 15-19.

2. Ефремова О.А. Применение системного подхода к исследованию проблемы использования пространственной информации для поддержки принятия решений региональными органами исполнительной власти // Инженерный вестник Дона, 2014, №2. URL: ivdon.ru/ru/magazine/archive/n2y2014/2371/.

3. Берёза Н.В. Современные тенденции развития мирового и российского рынка информационных услуг // Инженерный вестник Дона, 2012, №2. URL: ivdon.ru/ru/magazine/archive/n2y2012/758/.

4. Kaspersky Security Bulletin 2019. Statistics // URL: securelist.com/ksb-2019/.

5. Kaspersky Security Bulletin 2020. Statistics // URL: securelist.com/ksb-2020/.

6. Зайцев О. Rootkits, SpyWare/AdWare, Keyloggers & BackDoors. Обнаружение и защита. – СПб.: Издательство «БХВ-Петербург», 2006. – 304 с.

7. Скрыль С.В., Голубков Д.А., Сычев А.М., Хворов Р.А. Методические основы оптимизации механизмов антивирусной защиты резидентного типа. // Приборы и системы. Управление, контроль, диагностика. – М.: Издательство «Научтехлитиздат», 2015. - № 4. – С. 7 – 13.

8. Сенокосов А.А., Баринов В.М. Методика оценки функциональных подсистем единого информационного пространства органов военного управления // Военная Мысль. 2020. № 10. С. 30-36.

9. Банк данных угроз безопасности информации ФСТЭК России // URL: bdu.fstec.ru/threat.

10. Скрыль С.В., Щербаков А.В., Конышев Е.А., Домрачев Д.В. Теоретические основания для оптимизации временных ресурсов компьютерных систем в интересах реализации технологии антивирусной защиты резидентного типа // Телекоммуникации. - Москва: ООО «Наука и технологии», 2020, № 7, С. 28 – 32.

11. Конышев Е.А. Программа расчета оптимальных временных характеристик механизмов антивирусной защиты резидентного типа в автоматизированных системах специального назначения: свидетельство о государственной регистрации программы для ЭВМ от 08.12.2020 № 2020666354 – Москва : ФИПС, 2020.

12. Корн Г., Т. Корн. Справочник по математике (для научных работников и инженеров). Москва : Наука, 1974. – 832 с.

References

1. Drobotun E.B., Berdyshev V.P. Voennaya Mysl'. 2016. № 10. pp. 15-19.

2. Efremova O.A. Inzhenernyy vestnik Dona, 2014, №2. URL: ivdon.ru/ru/magazine/archive/n2y2014/2371/.

3. Bereza N.V. Inzhenernyy vestnik Dona, 2012, №2. URL: ivdon.ru/ru/magazine/archive/n2y2012/758/.

4. Kaspersky Security Bulletin 2019. Statistics URL: securelist.com/ksb-2019/.

5. Kaspersky Security Bulletin 2020. Statistics URL: securelist.com/ksb-2020/.

6. Zaytsev O. Rootkits, SpyWare/AdWare, Keyloggers & BackDoors. Obnaruzhenie i zashchita [SpyWare/AdWare, Keyloggers & BackDoors. Detection and protection]. SPb.: Izdatel'stvo «BKhV-Peterburg», 2006. 304 p.

7. Skryl' S.V., Golubkov D.A., Sychev A.M., Khvorov R.A. Pribory i sistemy. Upravlenie, kontrol', diagnostik. 2015. № 4. pp. 7 – 13.

8. Senokosov A.A., Barinov V.M. Voennaya Mysl'. 2020. № 10. pp. 30-36.

9. Bank dannykh ugroz bezopasnosti informatsii FSTEK Rossii [Databank of information security threats of the Federal Service for Technical and Export Control of Russia] URL: bdu.fstec.ru/threat (accessed 29/01/21).

10. Skryl' S.V., Shcherbakov A.V., Konyshev E.A., Domrachev D.V. Telekommunikatsii. 2020. № 7, pp. 28 – 32.

11. Konyshev E.A. Programma rascheta optimal'nykh vremennykh kharakteristik mekhanizmov antivirusnoy zashchity rezidentnogo tipa v avtomatizirovannykh sistemakh spetsial'nogo naznacheniya [Program for calculating the optimal time characteristics of resident-type anti-virus protection mechanisms in special-purpose automated systems]: svidetel'stvo o gosudarstvennoy registratsii programmy dlya EVM ot 08.12.2020 № 2020666354. Moskva: FIPS, 2020.

12. Korn G., Korn T. Spravochnik po matematike (dlya nauchnykh rabotnikov i inzhenerov) [Mathematics Handbook (for Scientists and Engineers)]. Moskva: Nauka, 1974. 832 p.