Сергей Н. Горячев[1], Николай С. Кобяков[2]
Пермский военный институт войск национальной гвардии Российской Федерации,
ул. Гремячий Лог, 1, Пермь, 614112, Россия
[1]*e-mail: sergory@mail.ru, https://orcid.org/0000-0002-6994-8559*
[2]*e-mail: kkobyakov1234@gmail.com, https://orcid.org/0000-0002-4950-7879*

ОЦЕНКА СОСТОЯНИЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ОТ ВРЕДОНОСНЫХ ПРОГРАММ

DOI: http://dx.doi.org/10.26583/bit.2022.1.05

Аннотация. В данной статье рассмотрены основные виды вредоносных программ и их деструктивное воздействие на информационные системы. Целью работы является разработка математической модели для оценки состояния защищенности информационных систем на основе структурно-функционального анализа. Для достижения цели работы проанализированы существующие математические модели адаптивного управления защитой информации, построен граф вероятности состояний и переходов системы. Определены понятия состояний системы и их зависимость от необходимых и достаточных условий возникновения и протекания процесса заражения вредоносной программой. Исследована зависимость состояния информационной системы от различных детерминированных и стохастических событий. Разработана модель системы защиты информационной системы от вредоносных программ, определены допустимые значения опасных факторов вредоносных программ. Данная модель может использоваться специалистами в области защиты информации для оценки защищенности как введенных в эксплуатацию информационных систем, так и при разработке систем.

Ключевые слова: информационная система, вредоносная программа, структурно-функциональный анализ, защита систем.

Для цитирования: ГОРЯЧЕВ, Сергей Н.; КОБЯКОВ, Николай С. ОЦЕНКА СОСТОЯНИЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ОТ ВРЕДОНОСНЫХ ПРОГРАММ. Безопасность информационных технологий, [S.l.], т. 29, № 1, с. 44–56, 2022. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1401. DOI: http://dx.doi.org/10.26583/bit.2022.1.05.

Sergey N. Goryachev[1], Nikolai S. Kobyakov[2]
Perm military Institute of National Guard Troops,
Gremyachiy Log Str., 1, Perm, 614112, Russia
[1]*e-mail: sergory@mail.ru, https://orcid.org/0000-0002-6994-8559*
[2]*e-mail: kkobyakov1234@gmail.com, https://orcid.org/0000-0002-4950-7879*

Assessment of the state of protection of information systems against malware

DOI: http://dx.doi.org/10.26583/bit.2022.1.05

Abstract. This paper discusses the main types of malware and their destructive effects on information systems. The current work develops a mathematical model for assessing the state of security of information systems based on structural and functional analysis. To achieve the goal of this work, we analyzed existing mathematical models of adaptive information security management, and built a probability graph of system states and transitions. We define the concept of system states and their dependence on the necessary and sufficient conditions for the emergence and duration of the process of destruction by malware. The dependence of information system states on various deterministic and stochastic events has been studied. A model of a system for protecting an information system from malicious programs has been developed, and the permissible values of dangerous factors of malicious programs have been determined. The result of this work is a mathematical model for assessing the state of protection of an information system from malware. This model can be used by specialists in the field of information security to assess the security of both the operating information systems and those under development.

Keywords: information system, malware, structural and functional analysis, protection of an information system.
For citation: GORYACHEV, Sergey N.; KOBYAKOV, Nikolai S. Assessment of the state of protection of information systems against malware. IT Security (Russia), [S.l.], v. 29, n. 1, p. 44–56, 2022. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1401. DOI: http://dx.doi.org/10.26583/bit.2022.1.05.

Введение

Информационная система (ИС) – это совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.[1] В настоящее время в связи с увеличением количества хакерских атак на российские государственные органы есть необходимость использовать информационные системы специального назначения (ИССН). Поскольку российские государственные органы являются органами государственной исполнительной власти, то циркулирующая в ИС информация представляет интерес для многих сторон, начиная с криминальных группировок, и заканчивая отдельными физическими лицами, имеющими корыстные или иные цели [1]. В этих условиях все больше востребованными в повседневной деятельности российских государственных органов становятся вопросы управления обеспечением защиты ИС, исходя из требований конфиденциальности, целостности и доступности к информации. Вместе с тем в документах государственных регуляторов сегодня отсутствуют требования к управлению безопасностью ИССН в части касающейся защиты от угрозы применения вредоносных программ (ВП). Действующие нормативные документы, например, ФСТЭК России, регламентируют применение положений ГОСТ Р ИСО/МЭК ТО 13335-5-2006 «Информационная технология. Руководство по менеджменту безопасности» и ряда других ГОСТов, где декларируются обязанности должностных лиц и требования к информационным системам в целом. При этом в этих положениях не учитывается динамичность информационных процессов реализации угроз и защита от них. В частности, в них не учитывается динамика опасных последствий (нарушения работы прикладных программ, разрушение, искажение файлов и т.д.) от деструктивных функций ВП. В [2, 3] рассмотрены вопросы создания моделей управления системой защиты информации, а в [4, 5] разработаны модели оценки эффективности функционирования подсистем системы защиты информации, но, не рассмотрена возможность использования структурно-функционального анализа для решения задачи оценки состояния защищенности.

1. Основная часть исследования

Учет динамики процессов внедрения ВП со своевременной реакцией управления защитой информации в ИССН может не только существенно повлиять на эффективность защиты информации, но и изменить требования к защите. Однако для такого учёта необходимо иметь модели адаптивного управления защитой информации, направленной на своевременное обнаружение, нейтрализацию и прогнозирование последствий от деструктивных функций ВП в ИССН в условиях динамики реализации угроз ее безопасности.

Решением задачи является разработка модели адаптивного управления защитой информации в ИССН. Далее рассмотрим задачу определения показателя безопасности ИС при воздействии ВП на основе применения системного подхода.

[1]Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»// СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 01.12.2021).

Сущность системного подхода состоит в том, что объект проектирования или управления рассматривается как система, т.е. как единство взаимосвязанных элементов, которые образуют единое целое и действуют в интересах реализации единой цели [6].

Основные положения системного подхода:

1) любой объект – это открытая система, взаимодействующая с внешней средой;
2) эффективность функционирования системы определяется ее системными качествами и условиями окружающей среды;
3) элементы системы рассматриваются в их взаимосвязи.

Защита информации в ИССН от деструктивного воздействия ВП представляет собой постоянный процесс, выполняемый на всех этапах жизненного цикла информации (хранение, обработка и передача) при комплексном использовании всех имеющихся средств и методов защиты. При этом все средства, методы и мероприятия, применяемые для защиты информации, объединяются в единый целостный механизм.

Объектом в данном случае является ИС, в которой поставленные цели могут быть полностью достигнуты в результате решения следующих задач: выявление ВП, определение и прогнозирование последствий от деструктивных функций ВП, воздействующих или могущие воздействовать на защищаемую информацию. Решение данных задач составляет основу для эффективного управления защитой информации в конкретных условиях.

2. Построение графа модели состояний

ВП могут иметь следующие особенности:

– скрытие признаков своего присутствия;
– маскирование себя под прикладное программное обеспечение;
– перенос своих фрагментов в области оперативного и постоянного запоминающих устройств;
– нечеткая идентификация кода ВП;

На основе анализа указанных особенностей развития и реализации угроз ВП в ИС, построена модель взаимосвязей элементов исследуемой ИС.

Для формализации элементов системы введем следующие множества (рис. 1):

$C = \{ c_1, c_2, ..., c_n \}$ – множество информационных систем;

$V = \{v_1, v_2, ..., v_n\}$ – семейство вредоносных программ;

$E = \{e_1, e_2, ..., e_n\}$ – множество элементов сетевой инфраструктуры;

$U = \{u_1, u_2, ..., u_n\}$ – множество элементов управления.

Данного набора множеств достаточно, для описания основных элементов, от которых зависит функционирование ИССН.

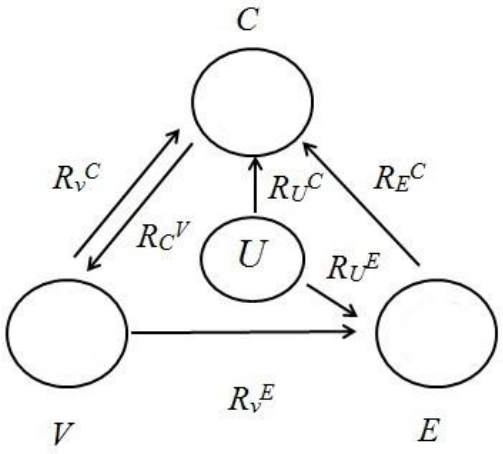


Рис. 1. Взаимосвязь элементов исследуемой системы
Fig. 1. The relationship of the elements of the system studied

Элементы системы S будут взаимосвязаны бинарными отношениями R (1), под которыми можно понимать функциональные отношения, предпочтения, следования и другие, отражающие существо взаимосвязи элементов системы. Например, семейство вредоносных программ V воздействует на ИС C отношением $VR_V^C C$, реагирование C на V определяется $CR_C^V V$:

$$VR_V^C C,\ VR_V^E E,\ CR_C^V V,\ ER_E^C C,\ UR_U^C C,\ UR_U^E E. \quad (1)$$

Разложим бинарные отношения R на два подмножества: незараженный (1) и зараженный (2) файл [7]. Файл, как структурированный объект, находится в некоторых условиях, определяемых операционной системой сервера или пользователем ИС. В этом случае система (1) преобразуется следующим образом:

$$VR_V^{C1}[S_C^V, C^1],\ S_C^V R_V^{C2} C^2\ ;\ VR_V^{E1}[S_E^V, E^1],\ S_E^V R_V^{E2} E^2;\ ER_E^{C1}[S_V^E, C^1],\ S_V^E R_E^{C2} C^2;$$
$$CR_C^{V1}[S_{V1}^C, V^1],\ S_{V2}^C R_C^{V2} V^2;\ UR_U^{C1}[S_{C1}^U, C^1],\ S_{C2}^U R_U^{C2} C^2;\ UR_U^{E1}[S_{E1}^U, E^1],\ S_{E1}^U R_U^{E2} E^2. \quad (2)$$

Состояния системы S каждого элемента зависят от их свойств, которые изменяются во время жизненного цикла системы. Состояние безопасности ИС S_C зависит от собственных свойств Q_C –наличие уязвимостей, настройки разграничений прав доступа пользователей (администратора), архитектуры и программной реализации ИС, наличие антивирусной программы, параметров сетевой инфраструктуры и деструктивных возможностей ВП

$$S_C = F_1[\{Q_C\}, S_C^E, S_C^V]. \quad (3)$$

Состояние сетевой инфраструктуры S_E зависит от собственных свойств инфраструктуры Q_E – топологии сети, состава сетевого оборудования, функциональных возможностей ВП

$$S_E = F_2\{Q_E\}, S_E^V. \quad (4)$$

Состояние ВП S_V зависит от собственных свойств ВП Q_V – скорости и способа распространения, состава деструктивного функционала

$$S_V = F_3\{Q_V\}. \quad (5)$$

Состояние ИС определяется свойствами элементов S_C, S_E, S_V. Характер изменения этих свойств в процессе жизненного цикла ИС, как правило, изменяется из-за обработки, хранения и передачи информации между пользователями. Таким образом, модель оценки состояния элементов системы *CE* опишется некоторым функционалом $\Im$

$$S_{CE} = \Im\,[S_C, S_E, S_V]. \tag{6}$$

3. Исследование модели оценки состояния информационной системы

Исследуем более подробно безопасность ИС. Под безопасностью ИС понимается непрерывная функция в диапазоне от 0 до 1, дифференцируемая на всей области определения. Изменение состояния безопасности файловой структуры (*P*) ИС опишется следующей зависимостью, (взаимосвязь данных элементов представлена на рис. 1)

$$S_C = \Delta P_C\left(Q_C\right) + \Delta P_C\left(E\right) + \Delta P_C\left(V\right), \tag{7}$$

где $\Delta P_C(Q_C)$ – изменение показателя безопасности ИС от выявленных собственных уязвимостей, $\Delta P_C(E)$ – изменение показателя безопасности ИС от сетевой инфраструктуры, $\Delta P_C(V)$ – изменение показателя безопасности ИС от воздействий ВП.

Под уязвимостями безопасности ИС можно понимать свойства элементов файловой структуры ИС: тип *Tp*, атрибуты *At*, настройки матрицы доступа *Mt* и размеры *Ob* файлов

$$\Delta P_C\left(Q_C\right) = \frac{\partial P_C}{\partial Q_{Tp}}\Delta Q_{Tp} + \frac{\partial P_C}{\partial Q_{At}}\Delta Q_{At} + \frac{\partial P_C}{\partial Q_{Mt}}\Delta Q_{Mt} + \frac{\partial P_C}{\partial Q_{Ob}}\Delta Q_{Ob}. \tag{8}$$

От параметров сетевой инфраструктуры зависит активность ВП, например, демилитаризованной зоны *Dmz*, межсетевого экрана *Mn*, криптографических защищенных сетевых протоколов *Kvp*

$$S_E = \Delta P_C\left(E\right)$$

$$\Delta P_C\left(E\right) = \frac{\partial P_C}{\partial E_{Dmz}}\Delta E_{Dmz} + \frac{\partial P_C}{\partial E_{Mn}}\Delta E_{Mn} + \frac{\partial P_C}{\partial E_{Kvp}}\Delta E_{Kvp}. \tag{9}$$

Изменение показателя опасности $\Delta Q_C(V)$ зависит от группы вредоносных программ и опишется уравнением

$$S_V = \Delta Q_C(\mathrm{V})$$

$$\Delta Q_C\left(V\right) = \frac{\partial Q_C}{\partial v_1}\Delta v_1 + \frac{\partial Q_C}{\partial v_2}\Delta v_2 + \frac{\partial Q_C}{\partial v_3}\Delta v_3 + \frac{\partial Q_C}{\partial v_4}\Delta v_4 \tag{10}$$

где:

v_1={файловые вирусы, макровирусы, загрузочные вирусы} – множество ВП 1-го типа;

v_2={программные закладки} – множество ВП 2-го типа;

v_3={ВП, распространяющиеся по сети } – множество ВП 3-го типа;

v_4={ другие вредоносные программы } – множество ВП 4-го типа.

Современные ВП основаны на использовании уязвимостей системного и прикладного программного обеспечения, технологий обработки информации, протоколов передачи данных. Они обладают широким спектром деструктивных возможностей [8].

Пример работы вредоносных программ представлен на рис. 2 [9].

Рис. 2. Результат действия вредоносных программ
Fig. 2. The result of the action of malware

Обобщённый функционал деструктивных функций (dsf) вредоносных программ может быть представлен в следующем виде

$$\Delta v\ (\mathrm{dsf}) = \frac{\partial v}{\partial(\mathrm{dsf}_1)}\Delta\mathrm{dsf}_1 + \frac{\partial v}{\partial(\mathrm{dsf}_2)}\Delta\mathrm{dsf}_2 + \frac{\partial v}{\partial(\mathrm{dsf}_3)}\Delta\mathrm{dsf}_3 + \frac{\partial v}{\partial(\mathrm{dsf}_4)}\Delta\mathrm{dsf}_4 +$$
$$+ \frac{\partial v}{\partial(\mathrm{nsp}_5)}\Delta\mathrm{dsf}_5 + \frac{\partial v}{\partial(\mathrm{dsf}_6)}\Delta\mathrm{dsf}_6 + \frac{\partial v}{\partial(\mathrm{dsf}_7)}\Delta\mathrm{dsf}_7 + \frac{\partial v}{\partial(\mathrm{dsf}_8)}\Delta\mathrm{dsf}_8 + \frac{\partial v}{\partial(\mathrm{dsf}_9)}\Delta\mathrm{dsf}_9 + \quad (11)$$
$$+ \frac{\partial v}{\partial(\mathrm{dsf}_{10})}\Delta\mathrm{dsf}_{10} + \frac{\partial v}{\partial(\mathrm{dsf}_{11})}\Delta\mathrm{dsf}_{11} + \frac{\partial v}{\partial(\mathrm{dsf}_{12})}\Delta\mathrm{dsf}_{12},$$

где:
dsf_1 – уничтожение данных в секторах постоянного запоминающего устройства;
dsf_2 – исключение возможности загрузки операционной системы;
dsf_3 – искажение кода загрузчика операционной системы;
dsf_4 – форматирование логических дисков постоянного запоминающего устройства;
dsf_5– закрытие (открытие) доступа к портам (COM, USB, RJ-45 и др.);
dsf_6 – закрытие (открытие) логических портов компьютера;
dsf_7 – замена символов при печати текстов;
dsf_8 – создание звуковых (визуальных) эффектов на экране монитора;
dsf_9 – искажение файлов данных;
dsf_{10} – перезагрузка системы;
dsf_{11} – шифрование файлов данных пользователя (.doc, .docx, .docm, .dot, .xls, .pptx, .ppt, .jpg, .jpeg и др.);
dsf_{12} – шифрование системных файлов (.drv, .sys, .com, .exe, csr, .pem, .key и др.).

4. Разработка графа состояний и переходов

Необходимым условием для реализации угрозы заражения вредоносной программой является наличие вредоносной программы S_V на автоматизированном рабочем месте, а достаточным – отсутствие антивирусной программы и файрвола b, отсутствие контроля над подключением съемных носителей r и времени воздействия o.

Наличие вредоносной программы необходимо для реализации угрозы, так как если ее не будет, то и не будет существовать угрозы заражения вредоносной программой. В свою очередь, если на автоматизированном рабочем месте будут реализованы меры

защиты (установлены файрвол, антивирусная программа, осуществлен контроль над подключением съемных носителей), то угроза заражения вредоносной программой будет минимизирована. Кроме того, вредоносной программе для деструктивного воздействия необходимо время.

В табл. 1 представлены необходимые и достаточные условия возникновения и протекания процесса заражения вредоносными программами в информационной системе.

Таблица 1. Необходимые и достаточные условия возникновения и протекания процесса заражения вредоносной программой

Вероятность состояния	Вид состояния	Параметры
p_1	Безопасное состояние (отсутствие необходимого и достаточных условий)	$\mathrm{C}^1 = \begin{pmatrix} S_V < S_V^d \\ b < b^d \\ o < o^d \\ r < r^d \end{pmatrix}$
p_2	Опасное состояние воздействия на информационную систему (есть необходимое (S_V), но отсутствуют достаточные условия)	$\mathrm{C}^2 = \begin{pmatrix} S_V > S_V^d \\ b < b^d \\ o < o^d \\ r < r^d \end{pmatrix}$
p_3	Состояние заражения вредоносной программой (присутствие необходимого (S_V) и достаточных условий (b,r))	$\mathrm{C}^3 = \begin{pmatrix} S_V < S_V^d \\ b > b^d \\ o < o^d \\ r > r^d \end{pmatrix}$
p_4	Состояние нарушения работоспособности информационной системы (присутствие необходимого (S_V) и достаточных условий (b, o, r))	$\mathrm{C}^4 = \begin{pmatrix} S_V < S_V^d \\ b > b^d \\ o > o^d \\ r < r^d \end{pmatrix}$

где S_V^d, b_d, o_d, r_d предельно допустимые параметры распространения вредоносной программы.

Для модели переходных состояний предлагается использовать полумарковские процессы, так как они характеризуются произвольными функциями распределения p_i. Под воздействием активности вредоносной программы с вероятностью перехода λ_{ij} происходит переход системы из состояния C_i в состояние C_j. Определение вероятности $p_i(t)$ состояния системы определяется решением системы уравнений Колмогорова.

$$\frac{\partial p_i}{\partial t} = \sum_{j=1}^{n} \lambda_{ij} p_j(t) - p_i(t) \sum_{j=1}^{n} \lambda_{ij}, (i = 1,2,3,\ldots,n) \qquad (12)$$

с начальными условиями $p_i(0) \geq 0$, $\sum_{i=1}^{n} p_i(0) = 1$.

Исходя из вышеприведенного, система с точки зрения безопасности информационной системы к заражению вредоносными программами может находиться в одном из четырех состояний:

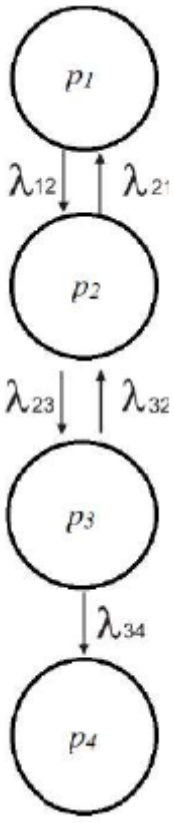
C^1 – безопасное состояние, когда в системе отсутствуют необходимые условия заражения вредоносной программой;

C^2 – состояние опасной ситуации, когда в системе существует вредоносная программа, но отсутствуют достаточные условия заражения вредоносной программой;

C^3 – состояние зараженного компьютера, когда программа начинает свою деятельность;

C^4 – состояние нарушения работоспособности информационной системы.

Взаимосвязи между вероятностными состояниями системы представлены на рис. 1, из которого видно, что система может переходить из безопасного состояния p_1 в опасное p_2 и далее в зараженное p_3 состояния или обратные переходы при установке антивирусного программного обеспечения и принятия своевременных мер по уничтожению вредоносных программ. Переход из зараженного состояния в состояние нарушения работоспособности p_4 – конечный, так как работа информационной системы в этот момент нарушена. Система дифференциальных уравнений для графа вероятностей состояний p_i и переходов λ_{ij} системы показана на рис. 3.



$$\frac{\partial p_1(t)}{\partial t} = \lambda_{21} p_2(t) - \lambda_{12} p_1(t)$$

$$\frac{\partial p_2(t)}{\partial t} = \lambda_{12} p_1(t) + \lambda_{32} p_3(t) - \lambda_{21} p_2(t) - \lambda_{23} p_2(t)$$

$$\frac{\partial p_3(t)}{\partial t} = \lambda_{23} p_2(t) - \lambda_{32} p_3(t) - \lambda_{34} p_3(t)$$

$$\frac{\partial p_4(t)}{\partial t} = \lambda_{34} p_3(t)$$

Рис. 3. Граф вероятности состояний p_i и переходов λ_{ij} системы
Fig. 3. Graph of the probability of constructing p_i and transitions λ_{ij} of the system

5. Построение модели системы защиты информации информационных систем

Формализация пространства параметров опасности *i* вредоносной программы позволяет оценить степень безопасности информационной системы уравнением

$$\theta_i = \begin{cases} \frac{1}{4}\left(\frac{S_{V\,i}^{\,d} - S_{V\,i}}{S_{V\,i}^{\,d}} + \frac{b_i - b_i^d}{b_i^d} + \frac{r_i^d - r_i}{r_i^d} + \frac{o_i^d - o_i}{o_i^d} \right), \text{при } \left(S_{V\,i} < S_{V\,i}^{\,d}\right) \wedge \left(b_i > b_i^d\right) \wedge \left(r_i < r_i^d\right) \wedge \left(o_i < o_i^d\right); \\ 0, \quad \text{при } \left(S_{V\,i} \geq S_{V\,i}^{\,d}\right) \vee \left(b_i < b_i^d\right) \vee \left(o_i > o_i^d\right) \vee \left(r_i > r_i^d\right). \end{cases} \quad (13)$$

Таким образом, общий показатель для множества источников вредоносных программ рассчитывается как среднее арифметическое или равен нулю, если хотя бы один из источников вредоносных программ опасен (14).

$$\Theta = \begin{cases} \frac{1}{N}\sum_{i=1}^{N} \theta_i, \forall\, i = \overline{1, N} : \theta_i > 0; \\ 0 \qquad , \exists\, i = \overline{1, N} : \theta_i = 0. \end{cases} \quad (14)$$

В процессе функционирования информационной системы параметры источников вредоносных программ (*c, b, r, o*) системы могут изменяться, как детерминировано, так и стохастически, и представлены [10]

$$S_V = S_V\left(\vartheta_{SV}(t), t\right),\ b = b\left(\vartheta_b(t), t\right),\ \ r = r\left(\vartheta_r\ (t), t\right),\ o = \left(\vartheta_o(t), t\right), \quad (15)$$

где $\vartheta(t)$ – случайное событие.

Дифференцируя сложные функции (16), получим

$$\begin{gathered} \frac{\partial cv(\vartheta_{SV}(t), t)}{\partial t} = \frac{\partial S_V(\vartheta_{SV}(t))}{\partial \vartheta_{SV}(t)} \cdot \frac{\partial(\vartheta_{SV}(t)}{\partial t} + \frac{\partial S_V(t)}{\partial t} \\ \frac{\partial b(\vartheta_b(t), t)}{\partial t} = \frac{\partial x(\vartheta_b(t))}{\partial \vartheta_b(t)} \cdot \frac{\partial \vartheta_b(t)}{\partial t} + \frac{\partial b(t)}{\partial t} \\ \frac{\partial r(\vartheta_r(t), t)}{\partial t} = \frac{\partial r(\vartheta_r(t))}{\partial \vartheta_r(t)} \cdot \frac{\partial \vartheta_r(t)}{\partial t} + \frac{\partial r(t)}{\partial t} \\ \frac{\partial o(\vartheta_o(t), t)}{\partial t} = \frac{\partial o(\vartheta_o(t))}{\partial \vartheta_o(t)} \cdot \frac{\partial \vartheta_o(t)}{\partial t} + \frac{\partial o(t)}{\partial t} \end{gathered} \quad (16)$$

где $\frac{\partial S_V\left(\vartheta_{SV}(t)\right)}{\partial \vartheta_{SV}(t)}, \frac{\partial b(\vartheta_b(t))}{\partial \vartheta_b(t)}, \frac{\partial r(\vartheta_r(t))}{\partial \vartheta_r(t)}, \frac{\partial t(\vartheta_o(t))}{\partial \vartheta_o(t)}$ - плотности распределения вероятностей случайной величины заражения вредоносной программой информационной системы;

$\frac{\partial S_V(t)}{\partial t}, \frac{\partial b(t)}{\partial t}, \frac{\partial r(t)}{\partial t}, \frac{\partial o(t)}{\partial t}$ - функции детерминированного изменения параметров вредоносной программы;

$\frac{\mathrm{d}\vartheta_{SV}(t)}{\mathrm{d}t}, \frac{\mathrm{d}\vartheta_b(t)}{\mathrm{d}t}, \frac{\mathrm{d}\vartheta_r(t)}{\mathrm{d}t}, \frac{\mathrm{d}\vartheta_o(t)}{\mathrm{d}t}$ - плотности распределения времени наступления заражения информационной системы.

В случае нормального закона распределения случайной величины при экспоненциальном законе времени нарушения работоспособности информационной системы λ получим следующие выражения:

$$S_V(t) = \int_0^t \frac{\partial S_V(\vartheta_{SV}(t), t)}{\partial t}\partial t$$

$$= \int_0^t \left(\frac{1}{\sigma_{cv}\sqrt{2\pi}} exp\left(-\left[\frac{\vartheta_{SV} - M(\vartheta_{SV})}{2\sigma_{cv}}\right]^2\right) exp(\lambda_{SV} t)\, \partial t + \int_0^t \frac{\partial S_V(t)}{\partial t}\partial t\right.$$

$$= S_V(t) + \frac{1}{\sigma_{cv}\sqrt{2\pi}} exp\left(-\left[\frac{\vartheta_{SV} - M(\vartheta_{SV})}{2\sigma_{cv}}\right]^2\right) \exp(-\lambda_{SV} t)$$

$$b(t) = b(t) + \left(-\left[\frac{\vartheta_b - M(\vartheta_b)}{2\sigma_b}\right]^2\right) \exp(-\lambda_b t) \quad (17)$$

$$r(t) = r(t) + \frac{1}{\sigma_r\sqrt{2\pi}}\left(-\left[\frac{\vartheta_b - M(\vartheta_b)}{2\sigma_b}\right]^2\right) \exp(-\lambda_r t)$$

$$o(t) = o(t) + \frac{1}{\sigma_o\sqrt{2\pi}} exp\left(-\left[\frac{\vartheta_b - M(\vartheta_b)}{2\sigma_b}\right]^2\right) \exp(-\lambda_o t)$$

При известных законах распределения случайной величины с помощью системы уравнений (17) можно определить вероятность заражения информационной системы вредоносной программой с целью принятия мер по созданию системы защиты [11, 12].

В настоящее время ведутся активные работы по защите информационных систем от вредоносных программ [13]. На рис. 4 приведена модель системы защиты информационной системы.

Защита L должна обеспечивать воздействие от опасных факторов вредоносных программ не выше допустимых значений:

$$L_{SV} * S_V(t), L_b * b(t), L_r * r(t), L_o * o(t)\,. \quad (18)$$

Безопасность системы (рис. 4) по параметрам источника опасности вредоносных программ будет обеспечиваться в случае выполнения неравенств:

$$S_V^d - L_{SV} \cdot S_V(t) \geq 0, L_b \cdot b(t) - b^d \geq 0, r^d - L_r \cdot r(t) \geq 0, o^d - L_o \cdot o(t) \geq 0. \quad (19)$$

Оценка безопасности системы по i-му источнику опасности вредоносных программ с учетом коэффициентов защиты будет определяться по выражению (18) с учетом выполнения неравенств (19):

$$\theta_i = \frac{1}{4}\left[\left(\frac{S_{Vi}^d - L_{SVi} \cdot c_i(t)}{S_{Vi}^d}\right) + \left(\frac{L_{bi} b_i(t) - b_i^d}{b_i^d}\right) + \left(\frac{r_i^d - L_{ri} \cdot r(t)}{r_i^d}\right) + \left(\frac{o_i^d - L_{oi} \cdot o(t)}{o_i^d}\right)\right]$$

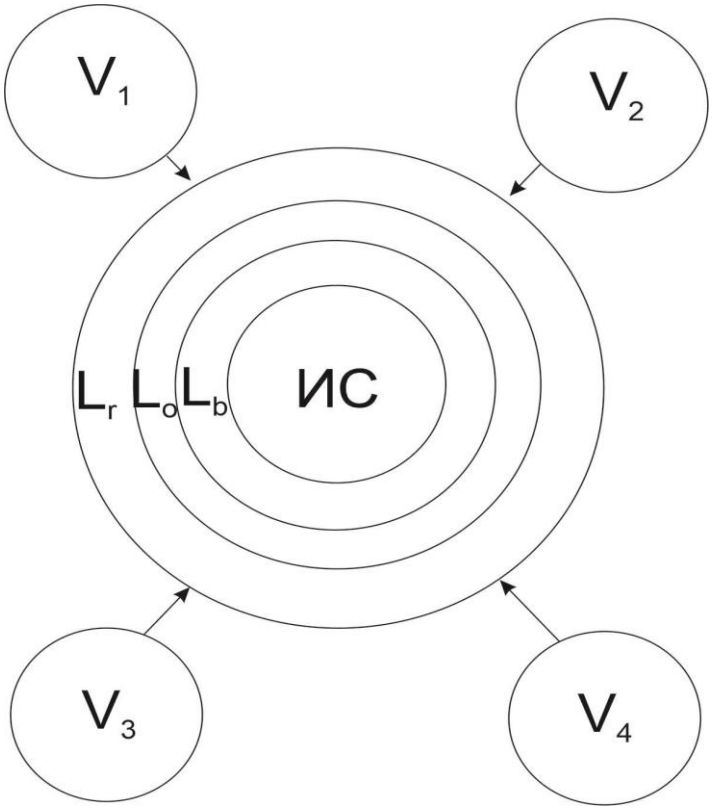


Рис. 4. Модель системы защиты информационной системы
Fig. 4. Model of the system to protect the information system

Защита L должна обеспечить воздействие опасных факторов вредоносных программ не выше допустимых значений, ее можно определить как средства и мероприятия борьбы с вредоносными программами, снижающие значения параметров до допустимых значений (20)

$$L_b \geq \frac{\theta_i^d}{\theta_i},\ L_r \leq \frac{\theta_i^d}{\theta_i},\ L_{SV} \leq \frac{\theta_i^d}{\theta_i},\ L_r \leq \frac{\theta_i^d}{\theta_i}, \quad (20)$$

где θ_i^d – допустимое значение величины источника вредоносных программ.

Разработка и внедрение данной модели позволит своевременно и надежно отслеживать состояние информационной системы.

Заключение

Вопрос защиты информационных систем становится все более актуальным с развитием информационных технологий. Для качественной оценки состояния защищенности информационных систем необходимо в руководящих документах определить требования к управлению безопасностью в ИССН. В данной работе определены взаимосвязи элементов, участвующих в процессе обработки и защиты информации, представлен граф состояний и переходов с учетом достаточных и необходимых условий для заражения вредоносной программой. Разработана математическая модель для оценки состояния защищенности информационной системы от вредоносных программ с учетом коэффициентов защиты. По результатам работы

может быть разработана методика оценки состояния защищенности информационных систем от вредоносных программ.

СПИСОК ЛИТЕРАТУРЫ:

1. Смирнов В.М., Киселёв С.А. Вредоносные программы как опасность ОВД. Shape * MERGEFORMAT. Евразийский Союз Ученых. 2020, № 3-1 (72), с. 43–44. URL: https://cyberleninka.ru/article/n/vredonosnye-programmy-kak-opasnost-ovd-shape-mergeformat (дата обращения: 01.12.2021).
2. Голдобина А.С., Исаева Ю.А., Селифанов В.В., Климова А.М., Зенкин П.С. Построение адаптивной трехуровневой модели процессов управления системой защиты информации объектов критической информационной инфраструктуры. Доклады ТУСУР. 2018, № 4, с. 51–58. URL: https://cyberleninka.ru/article/n/postroenie-adaptivnoy-trehurovnevoy-modeli-protsessov-upravleniya-sistemoy-zaschity-informatsii-obektov-kriticheskoy (дата обращения: 01.12.2021).
3. Бабенко А.А., Козунова С.С. Модель управления защитой информации в государственных информационных системах. NBI-technologies. 2018, № 4, с. 16–22. URL: https://cyberleninka.ru/article/n/model-upravleniya-zaschitoy-informatsii-v-gosudarstvennyh-informatsionnyh-sistemah (дата обращения: 01.12.2021).
4. Бацких А.В., Дровникова И.Г. Модель и алгоритм оценки эффективности функционирования подсистемы управления доступом системы защиты информации от несанкционированного доступа в автоматизированных системах органов внутренних дел. Вестник ВИ МВД России. 2021, № 2, с. 34–45. URL: https://cyberleninka.ru/article/n/model-i-algoritm-otsenki-effektivnosti-funktsionirovaniya-podsistemy-upravleniya-dostupom-sistemy-zaschity-informatsii-ot (дата обращения: 01.12.2021).
5. Бацких А.В. Имитационная модель процесса функционирования модифицированной подсистемы управления доступом системы защиты информации от несанкционированного доступа в программном окружении CPN TOOLS. Вестник ВИ МВД России. 2020, № 3, с. 96–106. URL: https://cyberleninka.ru/article/n/imitatsionnaya-model-protsessa-funktsionirovaniya-modifitsirovannoy-podsistemy-upravleniya-dostupom-sistemy-zaschity-informatsii-ot (дата обращения: 01.12.2021).
6. Антонов А.В. Системный анализ: учеб. для вузов. А.В. Антонов. М.: Наука и технологии, 2008. – 177 с.
7. Курош А.Г. Курс высшей алгебры. А.Г. Курош. СПб.: Лань, 2006. – 432 с.
8. Смирнов В.М., Цыганкова Я.В., Нестеров И.А. Состояние и тренды сетевой безопасности. Евразийский Союз Ученых. 2019, № 9-2 (66), с. 42–43. URL: https://cyberleninka.ru/article/n/sostoyanie-i-trendy-setevoy-bezopasnosti (дата обращения: 30.11.2021).
9. Вирус-шифровальщик. xakep.ru. URL: https://xakep.ru/2019/02/04/chrome-js-reversing/ (дата обращения: 01.12.2021).
10. Горячев С.Н. Применение системного анализа для совершенствования методологии управления защитой информации. Применение современных информационных технологий в служебно-боевой деятельности: Материалы XIV Межвузовской научно-практической конференции, Пермь, 15 апреля 2020 года. Пермь: Федеральное государственное казенное военное образовательное учреждение высшего образования «Пермский военный институт войск национальной гвардии Российской Федерации», 2020. – 101 с. URL: https://www.elibrary.ru/item.asp?id=42793953&selid=42794079.
11. Макарова Ольга С., Поршнев Сергей В. Оценивание вероятностей компьютерных атак на основе метода анализа иерархий с динамическими приоритетами и предпочтениями. Безопасность информационных технологий, [S.l.], т. 27, № 1, с. 6–18, 2020. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2020.1.01.
12. Чеботарев Сергей В. О распределении сумм случайных величин с инвариантными связями и их моделировании. Журнал СФУ. Математика и физика. 2019, № 5, с. 628–636. URL: https://cyberleninka.ru/article/n/on-distribution-of-sums-of-random-variables-with-invariant-links-and-their-modeling (дата обращения: 03.12.2021).
13. Макарова Ольга С.; Поршнев Сергей В. Определение параметров, влияющих на возможность реализации компьютерной атаки нарушителем. Безопасность информационных технологий, [S.l.], т. 28, № 2, с. 6–20, 2021. DOI: http://dx.doi.org/10.26583/bit.2021.2.01.

REFERENCES:

[1] Smirnov V.M., Kiselev S.A. Malware as a threat to IAB Shape * MERGEFORMAT. Evraziiskii Soiuz Uchenykh 2020, no. 3-1 (72), p. 43–44. URL: https://cyberleninka.ru/article/n/vredonosnye-programmy-kak-opasnost-ovd-shape-mergeformat (accessed: 01.12.2021) (in Russian).
[2] Goldobina A.S., Isaeva YU.A., Selifanov V.V., Klimova A.M., Zenkin P.S. Building an adaptive three-level model of processes for managing the information protection system of critical information infrastructure

objects. Doklady TUSUR. 2018, no. 4, p. 51–58. URL: https://cyberleninka.ru/article/n/postroenie-adaptivnoy-trehurovnevoy-modeli-protsessov-upravleniya-sistemoy-zaschity-informatsii-obektov-kriticheskoy (accessed: 01.12.2021) (in Russian).

[3] Babenko A.A., Kozunova S.S. Information security management model in state information systems. NBI-technologies. 2018, no. 4, p. 16–22. URL: https://cyberleninka.ru/article/n/model-upravleniya-zaschitoy-informatsii-v-gosudarstvennyh-informatsionnyh-sistemah (accessed: 01.12.2021) (in Russian).

[4] Backih A.V., Drovnikova I.G. Model and algorithm for assessing the efficiency of functioning of the access control subsystem of the information protection system against unauthorized access in automated systems of the internal affairs bodies. Vestnik VI MVD Rossii. 2021, no. 2, p. 34–45. URL: https://cyberleninka.ru/article/n/model-i-algoritm-otsenki-effektivnosti-funktsionirovaniya-podsistemy-upravleniya-dostupom-sistemy-zaschity-informatsii-ot (accessed: 01.12.2021) (in Russian).

[5] Backih A.V. Simulation model of the functioning process of the modified access control subsystem of the information protection system against unauthorized access in the CPN TOOLS program environmentdostupa v programmnom okruzhenii CPN TOOLS. Vestnik VI MVD Rossii. 2020, no. 3, p. 96–106. URL: https://cyberleninka.ru/article/n/imitatsionnaya-model-protsessa-funktsionirovaniya-modifitsirovannoy-podsistemy-upravleniya-dostupom-sistemy-zaschity-informatsii-ot (accessed: 01.12.2021) (in Russian).

[6] Antonov A.V. System analysis: textbook. for universities.Antonov A.V. M.: Nauka i tekhnologii, 2008. – 177 p. (in Russian).

[7] Kurosh A.G. Kurs vysshej algebry. A.G. Kurosh. SPb.: Lan', 2006. – 432 s. (in Russian).

[8] Smirnov V.M., TSygankova IA.V., Nesterov I.A. State and trends of network security. Evraziiskii Soiuz Uchenykh. 2019, no. 9-2 (66), p. 42–43. URL: https://cyberleninka.ru/article/n/sostoyanie-i-trendy-setevoy-bezopasnosti (accessed: 30.11.2021) (in Russian).

[9] Virus-shifroval'shchik. xakep.ru. URL: https://xakep.ru/2019/02/04/chrome-js-reversing/ (accessed: 01.12.2021) (in Russian).

[10] Goryachev S.N. Application of system analysis to improve information security management methodology. Primenenie sovremennyh informacionnyh tekhnologij v sluzhebno-boevoj deyatel'nosti: Materialy XIV Mezhvuzovskoj nauchno-prakticheskoj konferencii, Perm', 15 aprelya 2020 goda. Perm': Federal'noe gosudarstvennoe kazennoe voennoe obrazovatel'noe uchrezhdenie vysshego obrazovaniya «Permskij voennyj institut vojsk nacional'noj gvardii Rossijskoj Federacii», 2020. – 101 s. URL: https://www.elibrary.ru/item.asp?id=42793953&selid=42794079 (accessed: 01.12.2021) (in Russian).

[11] Makarova Olga S., Porshnev Sergey V. Assessment of probabilities of computer attacks based on the method of analysis of hierarchies with dynamic priorities and preferences. IT Security (Russia), [S.l.], vol. 27, no. 1, p. 6–18, 2020. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2020.1.01.

[12] Chebotarev Sergey V. On distribution of sums of random variables with invariant links and their modeling. ZHurnal SFU. Matematika i fizika. 2019, no. 5, p. 628–636. URL: https://cyberleninka.ru/article/n/on-distribution-of-sums-of-random-variables-with-invariant-links-and-their-modeling (accessed: 01.12.2021) (in Russian).

[13] Makarova Ol'ga S., Porshnev Sergej V. Determination of parameters affecting the possibility of implementing a computer attack by an violator. IT Security (Russia), [S.l.], vol. 28, no. 2, p. 6–20, 2021. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2021.2.01.

Поступила в редакцию – 20 декабря 2021 г. Окончательный вариант – 28 февраля 2022 г.
Received – December 20, 2021. The final version – February 28, 2022.