УДК 004.491
doi: 10.26583/bit.2024.2.02

Игорь И. Корчагин[1], Ксения Е. Амелина[2], Александр Н. Стадник[3],
Антон О. Карецкий[4], Валерий С. Антонов[5]
[1]АО «Информационная внедренческая компания»,
ул. Бутырская, 75, Москва, 127015, Россия
[2]Московский государственный технический университет им. Н.Э. Баумана,
2-я Бауманская ул., 5, Москва, 105005, Россия
[3,4,5]Краснодарское высшее военное училище им. генерала армии С.М. Штеменко,
ул. Красина, 4, Краснодар, 350063, Россия
[1]e-mail: korchagin@ivk.ru, https://orcid.org/0009-0003-3714-0429
[2]e-mail: amelina@bmstu.ru, https://orcid.org/0009-0007-0047-4379
[3]e-mail: alstaff@yandex.ru, https://orcid.org/0000-0003-0870-8057
[4]e-mail: kaolegovich888@mail.ru, https://orcid.org/0009-0000-0842-2484
[5]e-mail: valerij.antonov.85@bk.ru, https://orcid.org/0009-0009-4910-6838

ФОРМАЛИЗОВАННОЕ ПРЕДСТАВЛЕНИЕ ЦЕЛЕВОЙ ФУНКЦИИ ВОЗДЕЙСТВИЯ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ НА ОПЕРАЦИОННУЮ СРЕДУ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Аннотация. В статье приводятся основные положения теории функционального моделирования применительно к решению важной и актуальной для методологии обеспечения информационной безопасности проблемы – разработки математических моделей, характеризующих динамические возможности вредоносного программного обеспечения по реализации деструктивного воздействия на объекты критической информационной инфраструктуры. В результате анализа моделей, представляющих угрозу безопасности информации за счет использования вредоносных объектов, таких как «цепочка кибервторжений», «унифицированная цепочка кибервторжений», базовая и расширенная модели анализа вторжений Diamond, модель ATT&CK, построен актуальный вариант функциональной модели в нотации IDEF0 процесса деструктивного воздействия ВПО на операционную среду автоматизированной системы управления специального назначения (АСУ СН). Проводится декомпозиция процесса воздействия ВПО на отдельные этапы, тактики и техники. Целью исследований являлась выработка варианта воздействия вредоносного программного обеспечения на АСУ СН как метода нарушения состояния защищенности информации и ее процессов рассматриваемой системы. Полученные результаты являются инструментом для формализованного представления описываемых процессов в терминах Марковских процессов и разработки аналитических моделей, соответствующих временных и вероятностных характеристик для количественной оценки возможностей нарушителя по реализации угроз состояния защищенности информации в АСУ СН, посредством воздействия ВПО.

Ключевые слова: автоматизированные системы управления специального назначения, вредоносное программное обеспечение, функциональное моделирование, нотация IDEF0, средства антивирусной защиты информации, защита информации, антивирусные механизмы.
Для цитирования: КОРЧАГИН, Игорь И. и др. ФОРМАЛИЗОВАННОЕ ПРЕДСТАВЛЕНИЕ ЦЕЛЕВОЙ ФУНКЦИИ ВОЗДЕЙСТВИЯ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ НА ОПЕРАЦИОННУЮ СРЕДУ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ. Безопасность информационных технологий, [S.l.], т. 31, № 2, с. 42–50, 2024. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1632. DOI: http://dx.doi.org/10.26583/bit.2024.2.02.

Igor I. Korchagin[1], Ksenia E. Amelina[2], Alexander N. Stadnik[3],
Anton O. Karetskiy[4], Valeriy S. Antonov[5]
[1]JSC «Information Implementation Company»,

Butyrskaya st., 75, Moscow, 127015, Russia
[2]Bauman Moscow State Technical University,
2nd Baumanskaya str., 5, Moscow, 105005, Russia
[3,4,5]Krasnodar Higher Military awarded School named after the general of the Army S.M. Shtemenko,
Krasina str., 4, Krasnodar, 350063, Russia
[1]e-mail: korchagin@ivk.ru, https://orcid.org/0009-0003-3714-0429
[2]e-mail: amelina@bmstu.ru, https://orcid.org/0009-0007-0047-4379
[3]e-mail: alstaff@yandex.ru, https://orcid.org/0000-0003-0870-8057
[4]e-mail: kaolegovich888@mail.ru, https://orcid.org/0009-0000-0842-2484
[5]e-mail: valerij.antonov.85@bk.ru, https://orcid.org/0009-0009-4910-6838

A formalized representation of the target function of the impact of malicious software on the operating environment of a special-purpose automated control system

Abstract. The article presents the main provisions of the theory of functional modeling in relation to solving an important and relevant problem for the methodology of information security managing – the development of mathematical models characterizing the dynamic capabilities of malware to implement destructive effects on critical information infrastructure objects. As a result of the analysis of the models that pose a threat to information security through the use of malicious codes, such as the "chain of cyber intrusions", the "unified chain of cyber intrusions", the basic and advanced models of Diamond intrusion analysis, the ATT&CK model, an up-to-date version of the functional model in the IDEF0 notation of the process of malware destructive impact on the operating environment of a special-purpose automated control system was built. The process of malware exposure is decomposed into individual stages, tactics, and techniques. The purpose of the research was to develop a variant of the malware impact on a special-purpose automated control system as a method of violating the state of information security and its processes of the system under consideration. The obtained results are a tool for the formalized presentation of the described processes in terms of the Markov processes and the development of analytical models, appropriate temporal and probabilistic characteristics for quantitative assessment of the intruder's ability to implement threats to the information security state in special-purpose automated control systems, through the malware impact.
Keywords: *automated control systems for special purposes, malicious software, functional modeling, IDEF0 notation, anti-virus information protection tools, data protection, antivirus mechanisms*.
For citation: KORCHAGIN, Igor I. et al. A formalized representation of the target function of the impact of malicious software on the operating environment of a special-purpose automated control system. IT Security (Russia), [S.l.], v. 31, no. 2, p. 42–50, 2024. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1632. DOI: http://dx.doi.org/10.26583/bit.2024.2.02.

Введение

Анализ ретроспектив развития средств антивирусной защиты (САВЗ) как инструмента противодействия вредоносному программному обеспечению (ВПО) позволяет выявить устойчивую тенденцию к целенаправленному совершенствованию способов и средств обнаружения и ликвидации последствий воздействия ВПО на автоматизированные системы управления специального назначения (АСУ СН) [1].

С учетом непрерывного возрастания требований к оперативности обработки информации в автоматизированных системах и передачи ее адресату, актуальность проблемы обеспечения безопасности информации стоит в настоящее время крайне остро.

Серьезным фактором снижения эффективности функционирования АСУ СН являются угрозы нарушения целостности, конфиденциальности и доступности информации [2]. Последствием воздействия этих угроз является перехват, искажение и блокирование информации в этих системах, что, в итоге, приводит к длительным временным задержкам

по восстановлению их работоспособности, и как следствие, срыву выполнения задач по предназначению.

1. ВПО, как угроза безопасности информации обрабатываемой в АСУ СН

АСУ СН определяется как система, предназначенная для управления и контроля конкретными процессами или операциями, имеющими критическое значение для национальной безопасности, экономики или социального благополучия [3].

АСУ СН характеризуются следующими особенностями:

- специализацией;
- автоматизацией;
- критичностью;
- защищенностью.

К защищенности предъявляются особые требования по безопасности информации от несанкционированного доступа, кибератак и иной топологии угроз. Однако, ни одно предприятие, программное или техническое средство, управленческие или организационные меры не могут гарантированно обеспечить защищенность обрабатываемых и хранимых данных в системе.

Под ВПО понимаются такие программы, которые прямо или косвенно дезорганизуют процесс обработки информации, способствуют утечке или искажению данных, за счет широкого разнообразия существующих тактик и техник деструктивного воздействия на технологические и информационные процессы АСУ СН [4]. Они включают в себя компьютерные вирусы, черви, троянские программы, вредоносные утилиты, подозрительные архиваторы, рекламное программное обеспечение, боты и др. Основные механизмы заражения АСУ СН базируются на использовании следующих ресурсов:

- съемные машинные носители информации;
- локальные сетевые ресурсы;
- электронная почта;
- системы обмена мгновенными сообщениями;
- веб-страницы;
- социальная инженерия и др.

Основными способами проникновения вредоносного объекта в периметр автоматизированной системы являются съемные машинные носители информации, а также внутренние локальные вычислительные сети, и как правило данные способы реализуются внутренними нарушителями (инсайдерами) [5]. При этом выявить зараженный объект автоматизированной системы возможно по характерным признакам:

- изменение характеристик файла (дата создания, объем, расширение и т.д.);
- ошибки аппаратного и программного обеспечения;
- недоступность портов интерфейса;
- увеличение частоты обращения к жёсткому и сетевому диску;
- появление ранее неизвестных ошибок системы;
- технологические задержки вычислительных ресурсов системы;
- самопроизвольная перезагрузка операционной системы;
- замедление работы процессора;
- появление неожиданных графических и звуковых эффектов;
- поступление уведомлений от средств антивирусной защиты и др.

Одним из направлений повышения эффективности информационного обеспечения АСУ СН в условиях воздействия ВПО является задача разработки моделей, позволяющих

сформировать варианты деструктивного воздействия ВПО на операционную среду (ОС) АСУ СН, декомпозировать процесс воздействия вредоносного объекта до нижнего уровня, необходимого для проведения детализированного анализа, как определения вектора формирования тактик и техник по его противодействию. Подобная декомпозиционная структура должна быть выполнена применительно к заданным параметрам функциональной структуры ВПО и типовым условиям функционирования АСУ СН, а также временным характеристикам ее информационного обеспечения и характеристикам угроз нарушения безопасности информации ВПО [6].

Адекватность моделирования угроз информационной безопасности АСУ СН является необходимым условием для корректного обоснования требований к применяемым способам и средствам защиты информации от воздействия ВПО в этих системах [7].

В соответствии с положениями методологии системного анализа [8] для оценки характеристик исследуемого процесса воздействия ВПО на ОС АСУ СН, необходимо формализовать рассматриваемые процессы.

Проведенный анализ моделей Cyber Kill Chain, Unified Kill Chain, Diamond и MITRE ATT&CK [5] позволил определить этапы, тактики и техники деструктивного воздействия ВПО на вычислительные системы и ресурсы. При функциональном моделировании рассматриваемого процесса будем опираться на указанные выше модели, при этом этапы, тактики и техники, применяемые ВПО, будут составлять единое множество признаков деструктивного воздействия на автоматизированные системы.

2. Формализованное представление деструктивного воздействия ВПО на операционную среду АСУ СН

Рассматриваемая функция Φ – воздействие ВПО на ОС АСУ СН будет иметь композиционный иерархический характер построения и предполагает множественное представление деструктивного процесса [8]. При этом реализация элементов этого множества определяется выполнением соответствующих целевых функций. Представление целевой функции в виде функциональных компонент обеспечивается ее декомпозицией, которая будет включать как функциональные, так и информационные связи между компонентами. Степень детализации декомпозиции целевой функции считается достаточной, если вариант функциональной декомпозиции позволяет идентифицировать признаки выполнения соответствующих данному уровню декомпозиции функций средствами антивирусной защиты.

На первом уровне декомпозиции процесса воздействия ВПО на ОС АСУ СН функция Φ будет представлена в виде множества $\Phi^{(1)}$, включающего в себя $\phi_i^{(1)}$ этапов процесса воздействия ВПО:

$$\Phi^{(1)} = \{\phi_i^{(1)}\}, \quad i = 1, 2, ..., I,$$

где i – количество этапов процесса воздействия ВПО на ОС АСУ СН.

Под этапами процесса реализации функции Φ будем понимать цели, которые необходимо достичь ВПО для успешных условий деструктивного воздействия на ОС АСУ СН.

На втором уровне декомпозиции на основе множества $\Phi^{(1)}$ каждый из этапов декомпозируется на отдельные тактики нарушителя $\phi_{ij}^{(2)}$, используемые ВПО для достижения этапов процесса деструктивного воздействия. Данные тактики в совокупности образуют множество функций второго уровня декомпозиции $\Phi^{(2)}$:

$$\Phi^{(2)} = \{\phi_{ij}^{(2)}\}, \quad i = 1,2,...,I, \quad j = 1,2,...J,$$

где i – количество этапов процесса воздействия ВПО на ОС АСУ СН; j – количество тактик на каждом этапе процесса воздействия ВПО на ОС АСУ СН.

Под тактиками будем понимать процедуры и операции, выполняемые ВПО в рамках отдельного этапа для осуществления деструктивного воздействия на ОС АСУ СН.

При этом функции процесса воздействия ВПО на ОС АСУ СН будет соответствовать несколько этапов, а каждому этапу функции будет соответствовать несколько тактик.

Функциональная модель будет служить инструментом исследования этапов, тактик и техник деструктивного воздействия ВПО на ОС АСУ СН с целью нарушения состояния защищенности, циркулирующей в ней информации. Таким образом, для детализированного рассмотрения процессов деструктивного характера реализуемых угрозами воздействия ВПО, необходимо формализовать целевые функции воздействия ВПО [9] на ОС АСУ СН, инфильтрацию вредоносного кода в систему, выполнение операций вредоносным кодом по нарушения состояния защищенности информации и механизмы сокрытия следов деструктивного воздействия вредоносным кодом от детектирования средствами защиты информации.

Для представления функциональной модели целевой функции реализации угроз воздействия ВПО на ОС АСУ СН воспользуемся методологией функционального моделирования IDEF0 [8]. Согласно данной методологии, рассматриваемый процесс представляется в виде функции, имеющей:

- вход – процесс, который преобразуется функцией в выход;
- выход – результат, произведенный функцией;
- управление – условия, при выполнении которых, работа функции будет правильной;
- механизмы – средства для выполнения функции.

Рассматриваемой функцией Φ является целевая функция процесса воздействия ВПО на ОС АСУ СН (рис. 1).

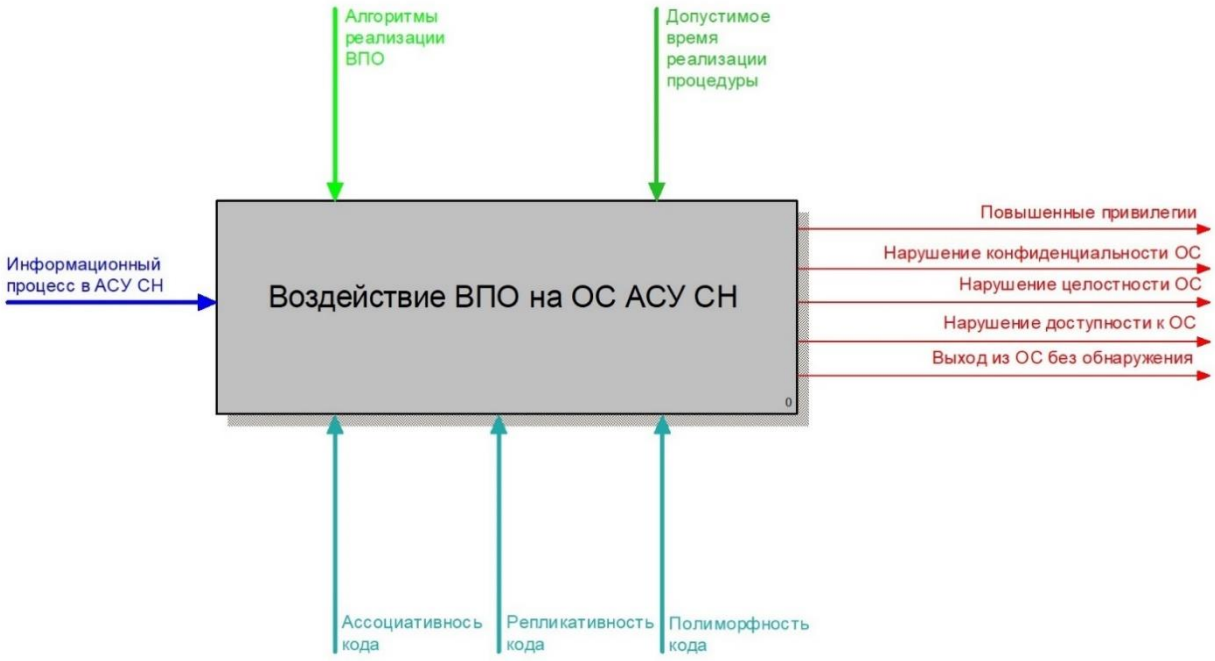

Рис. 1. Целевая функция процесса воздействия ВПО на ОС АСУ СН

На вход функции поступает информационный процесс в АСУ СН, заведомо содержащий в себе уязвимость к инфильтрации вредоносного объекта.

Управляющим воздействием функции являются:

- алгоритмы реализации ВПО;
- допустимое время реализации процедуры.

Механизмами, обеспечивающими выполнение целевой функции, являются:

Ассоциативность кода. Данное свойство позволяет вредоносному коду связывать себя с определенными типами файлов или расширениями файлов. Когда вредоносный объект ассоциирует себя с типом файла, он вносит изменения в операционную систему, чтобы каждый раз при открытии файла этого типа также запускался вредоносный код. Это позволяет вредоносному кода заражать другие файлы того же типа и достаточно эффективно распространяться по системе. Например, вредоносный код может ассоциировать себя с файлами .exe (исполняемыми файлами). Когда пользователь открывает файл .exe, вместе с ним запускается и вредоносный код;

Репликативность кода. Это способность вредоносного кода создавать свои копии. Свойство репликативности позволяет вредоносному коду распространяться и заражать файлы, программы или другие системы. Он может делать это разными способами, в зависимости от типа вредоносного объекта и операционной системы;

Полиморфность кода. Основными свойствами реализации данного механизма являются изменение собственного кода, генерации новых вариаций кода и уклонение от обнаружения, за счет приема обфускации или самоуничтожения вредоносного кода.

Выходом реализации функции воздействия ВПО на ОС АСУ СН будет считаться нарушения целостности, конфиденциальности и доступности операционной среды [10, 11, 12] рассматриваемой системы, повышение привилегии и выход из системы без обнаружения.

Реализация целевых функций воздействия ВПО также как осуществление процесса контролируемости операционной среды АСУ СН и своевременности реагирования на угрозы воздействия ВПО средствами антивирусной защиты будут характеризоваться степенью достижения своей цели [13].

На основании вышеизложенного, функциональные компоненты целевых функций можно представить в виде выполнения последовательности определенных функций.

На первом уровне декомпозиции функция воздействия ВПО на ОС АСУ СН будет представлена этапами: инфильтрация вредоносного кода, выполнение деструктивных действий вредоносным кодом и сокрытие следов воздействия вредоносного кода (рис. 2).

Инфильтрация вредоносного кода, как необходимое условие для горизонтального продвижения деструктивного воздействия, является первоначальным этапом воздействия ВПО на ОС АСУ СН.

Выполнение деструктивных действий является вторым этапом, на котором осуществляется непосредственное нарушение состояния защищенности информации вредоносным кодом.

Третьим этапом является сокрытие следов воздействия вредоносного кода [14] от обнаружения средствами антивирусной защиты информации.

На втором уровне декомпозиции осуществляется представление каждого из перечисленных этапов тактиками, которые реализует ВПО в процессе деструктивного воздействия.

Этап инфильтрация вредоносного кода декомпозируется на тактики осуществление первоначального доступа, выполнение и закрепление в ОС.

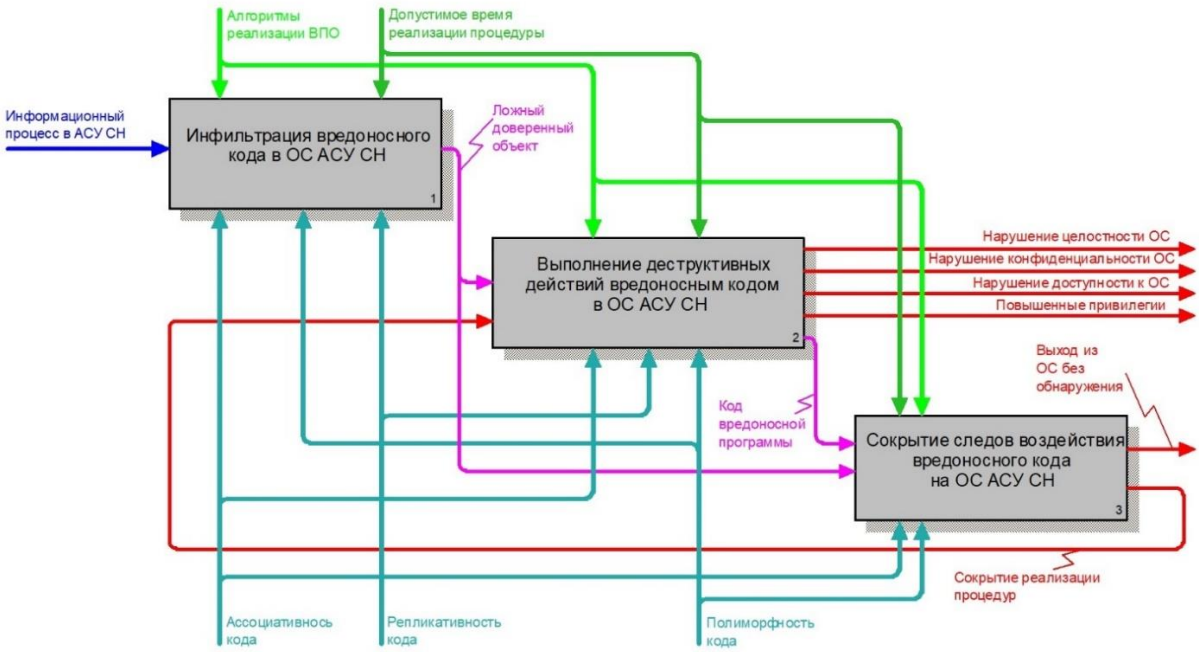

Рис. 2. Этапы воздействия ВПО на ОС АСУ СН

При реализации тактики осуществление первоначального доступа вредоносный код применяет техники использования существующих учетных записей, распространение через съемные носители информации и эксплуатацию доверительных отношений ОС.

Далее вредоносному коду необходимо выполнить закрепление в операционной среде АСУ СН [15], посредством применения техники воздействия на общие и таргетированные программные модули ОС.

Этап выполнения деструктивных действий вредоносным кодом декомпозируется на тактики уничтожение, эксфильтрацию и манипуляции с данными ОС.

При реализации тактики уничтожения данных вредоносный код использует следующие техники:

- сброс учетных записей ОС;
- внедрение вредоносного кода в процессы ОС;
- использование общих SMB- и административных ресурсов Windows;
- перезапись файлов случайно сгенерированными данными.

Эксфильтрация данных ОС вредоносным кодом осуществляется за счет применения техник изучения файлов и каталогов, передачи инструментов внутри периметра ОС и автоматизированного сбора данных.

Манипуляции с данными ОС осуществляется техниками воздействия на хранимые, передаваемые, обрабатываемые данные, а также нарушением целостности данных ОС.

Этап сокрытие следов воздействия вредоносного кода на ОС декомпозируется на тактики предотвращения обнаружения и самоуничтожение вредоносного кода.

При реализации тактики предотвращения обнаружения используются техники руткита и маскировки.

Тактика самоуничтожение вредоносного кода будет состоять из двух техник: установки тайм-бомбы вредоносным кодом и непосредственное уничтожение кода при обнаружении САВЗ или завершении алгоритма деструктивной процедуры.

Заключение

В статье проведен анализ процесса воздействия ВПО на операционную среду АСУ СН, разработана целевая функция и проведена ее декомпозиция на отдельные этапы, тактики и техники реализации. В дальнейших исследованиях будут установлены иерархические связи между отдельными этапами, тактиками и техниками и их представление в виде функциональных диаграмм.

СПИСОК ЛИТЕРАТУРЫ:

1. Скрыль Сергей В. и др. Технология soft tempest как объект функционального моделирования. Безопасность информационных технологий, [S.l.], т. 29, № 1, с. 125–144, 2022. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2022.1.11. – EDN: LUVPCQ.
2. Цимбал В.А., Стрельчук А.С. Разработка методики реконфигурации технических средств ЦХОИ АСУ СН для обеспечения устойчивости их функционирования при воздействии дестабилизирующих факторов. Радиотехника и связь: Известия Института инженерной физики. Серпухов: филиал Военной академии Ракетных войск стратегического назначения им. Петра Великого. 2022, № 1(63), с. 54–61. URL: https://www.elibrary.ru/download/elibrary_47988749_85481240.pdf (дата обращения: 08.05.2024).
3. Сычев М.П. и др. Киберустойчивость информационной инфраструктуры: Модели исследования: монография. М.: Под общей научной редакцией д.т.н., проф. С.В. Скрыля. 2023. – 256 с. – EDN: CZBYSE.
4. Стадник А.Н., Голубков Д.А., Домрачев Д.В. Гипотеза о параметрических соответствиях в проблематике антивирусной защиты сеансового типа. Охрана, безопасность и связь. Сборник материалов Международной научно-практической конференции. Воронеж: Воронежский институт МВД России. 2021, с. 284–291. – EDN: WTLLMS.
5. Котенко И.В., Хмыров С.С. Анализ моделей и методик, используемых для атрибуции нарушителей кибербезопасности при реализации целевых атак. Вопросы кибербезопасности. 2022, № 4(50), с. 52–79. URL: https://cyberleninka.ru/article/n/analiz-modeley-i-metodik-ispolzuemyh-dlya-atributsii-narushiteley-kiberbezopasnosti-pri-realizatsii-tselevyh-atak (дата обращения: 03.04.2024).
6. Никулин С.А., Хворов Р.А. Методическое обеспечение безопасности информации в АСУ специального назначения. Наукоемкие технологии в космических исследованиях земли. 2013, № 3, с. 34–40. – EDN: THBRBT.
7. Мазин А.В. и др. Теория информации как методологическая основа решения проблем адекватной оценки возможностей по обеспечению защиты информации. Известия Института инженерной физики. 2022, № 2(64), с. 64–68. – EDN: NXNGMV.
8. Мещерякова Т.В., Арутюнова В.И. Функциональная модель нарушения безопасности информации в результате вирусной атаки. Вестник Воронежского института МВД России: Информатика, вычислительная техника и управление. Воронеж: Воронежский институт МВД России. 2019, № 4, с. 80–89. – EDN: JCEZYW.
9. Семенова П.С. и др. Компьютерные вирусы, их классификация и средства борьбы с ними. Современные научные исследования. 2022, с. 24–32. – EDN: UQLVPU.
10. Мазин А.В. и др. Оптимизация антивирусной защиты в автоматизированных системах управления специального назначения: Формальные основания для распределения временного ресурса. Информатика, вычислительная техника и управление. Известия Института инженерной физики. Серпухов: филиал ВА РВСН им. Петра Великого. 2023, № 1(67), с. 59–63. – EDN: KRWURR.
11. Макаренко С.И. Модели системы связи в условиях преднамеренных дестабилизирующих воздействий и ведения разведки: монография. СПб: Наукоемкие технологии, 2020. – 337 с.
12. Скрыль Сергей В. и др. Актуальные вопросы проблематики оценки угроз компьютерных атак на информационные ресурсы значимых объектов критической информационной инфраструктуры. Безопасность информационных технологий, [S.l.], т. 28, № 1, с. 84–94, 2021. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2021.1.07. – EDN: NOWDER.
13. Конышев Е.А. Моделирование процессов обработки информации в автоматизированных системах специального назначения в условиях применения антивирусных механизмов резидентного типа. Инженерный вестник Дона – Ростов-на-Дону. 2021, № 2(74), с. 72–84. URL: https://cyberleninka.ru/article/n/modelirovanie-protsessov-obrabotki-informatsii-v-avtomatizirovannyh-sistemah-spetsialnogo-naznacheniya-v-usloviyah-primeneniya (дата обращения: 03.04.2024).
14. Маркина Т.А. и др. Методика количественной оценки антивирусных средств защиты на основе систем массового обслуживания. Технические науки: Научно-технический вестник Поволжья. СПб: Университет ИТМО, 2020, № 3, с. 103–106. – EDN: ZXUOCR.

15. Козлов З.С. Компьютерные вирусы и антивирусы. Научный сетевой журнал «Столыпинский вестник». Самара: Поволжский государственный университет телекоммуникаций и информатики. 2022, № 4. – EDN: JJVJYR.

REFERENCES:

[1] Skryl, Sergey V. et al. Soft tempest technology as an object of functional modeling. IT Security (Russia), [S.l.], v. 29, no. 1, p. 125–144, 2022. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2022.1.11 (in Russian). – EDN: LUVPCQ.

[2] Tsymbal V.A., Strelchuk A.S. Development of a methodology for reconfiguration of technical means of the IPSC of ACS SP to ensure the stability of their operation under the influence of destabilizing factors. Radio engineering and communications: Proceedings of the Institute of Engineering Physics. Serpukhov: branch of the Military Academy of the Strategic Missile Forces named after Peter the Great. 2022, no. 1(63), p. 54–61. URL: https://www.elibrary.ru/download/elibrary_47988749_85481240.pdf (accessed: 08.05.2024) (in Russia).

[3] Sychev V.M. et al. Cyber resilience of the information infrastructure: Research models : monograph. M.: under the general scientific editorship of dtn, Professor S.V. Skryl, 2023 (in Russian). – EDN: CZBYSE.

[4] Stadnik A.N., Golubkov D.A., Domrachev D.V. The hypothesis of parametric mapping in the issues of anti-virus protection, session. Collection of materials of the International Scientific and practical Conference. Voronezh: Voronezh Institute of the Ministry of Internal Affairs of Russia. 2021, p. 284–291 (in Russian). – EDN: CZBYSE.

[5] Kotenko I.V., Khmyrov S.S. Analysis of models and techniques used for attribution of cyber security violators in the implementation of targeted attacks. Network Security: Cybersecurity issues. Saint Petersburg: Military Academy of Communications. 2022, no. 4(50), p. 52–79. URL: https://cyberleninka.ru/article/n/analiz-modeley-i-metodik-ispolzuemyh-dlya-atributsii-narushiteley-kiberbezopasnosti-pri-realizatsii-tselevyh-atak (accessed: 03.04.2024) (in Russian).

[6] Nikulin S.A., Khvorov R.A. Methodological support of information security in a special purpose automated control system. High–tech technologies in space research of the Earth. 2013, no. 3, p. 34–40 (in Russian). – EDN: THBRBT.

[7] Mazin A.V. et al. Information theory as a methodological basis for solving problems of adequate assessment of information security capabilities. News of the Institute of Engineering Physics. 2022, no. 2(64), p. 64–68 (in Russian). – EDN: NXNGMV.

[8] Meshcheryakova, T.V., Frutyunova V.I. Functional model of information security violations as a result of viral attack. Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia: Informatics, Computer Science and Management. Voronezh: Voronezh Institute of the Ministry of Internal Affairs of Russia. 2019, no. 4, p. 80–89 (in Russian). – EDN: JCEZYW.

[9] Semenova P.S. et al. Computer viruses, their classification and means of combat them. Modern scientific research. 2022, p. 24–32 (in Russian). – EDN: UQLVPU.

[10] Mazin A.V. et al. Optimization of anti-virus protection in automated control systems for special purposes: formal grounds for the allocation of a temporary resource. Informatics, Computer Science and Management: News of the Institute of Engineering Physics. Serpukhov: branch of the VA Strategic Missile Forces named after. Peter the Great. 2023, no. 1(67), p. 59–63 (in Russian). – EDN: KRWURR.

[11] Makarenko S.I. Models of a communication system under conditions of deliberate destabilizing influences and reconnaissance: monograph. St. Petersburg: High Technology, 2020. – 337 p. (in Russian).

[12] Skryl', Sergey V. et al. Topical issues of the problem of assessment of threats of cyber attacks on information resources of significant facilities of critical information infrastructure. IT Security (Russia), [S.l.], v. 28, no. 1, p. 84-94, 2021. DOI: http://dx.doi.org/10.26583/bit.2021.1.07 (in Russian). – EDN: NOWDER.

[13] Konyshev E.A. Modeling of information processing processes in automated special-purpose systems in the context of the use of resident-type anti-virus mechanisms. Engineering Bulletin of the Don – Rostov-on-Don, 2021, no. 2(74), p. 72–84. URL: https://cyberleninka.ru/article/n/modelirovanie-protsessov-obrabotki-informatsii-v-avtomatizirovannyh-sistemah-spetsialnogo-naznacheniya-v-usloviyah-primeneniya (accessed: 03.04.2024) (in Russian).

[14] Markina T.A. A method of quantitative evaluation of anti-virus protection based on systems of mass service. Technical science: Scientific and technical bulletin of the Volga region. St. Petersburg: Leningrad Institute of Precision Mechanics and Optics. 2020, no. 3, p. 103–106 (in Russian). – EDN: ZXUOCR.

[15] Kozlov Z.S. Computer viruses and antiviruses. Scientific online journal "Stolypin Bulletin". Samara: Volga State University of Telecommunications and Informatics. 2022, no. 4 (in Russian). – EDN: JJVJYR.

Поступила в редакцию – 4 апреля 2024 г. Окончательный вариант – 20 мая 2024 г.
Received – April 4, 2024. The final version – May 20, 2024.