УДК 004.491
doi: 10.26583/bit.2024.4.05

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

ФУНКЦИОНАЛЬНОЕ МОДЕЛИРОВАНИЕ ФОРМАЛИЗАЦИИ ТАКТИК РЕАЛИЗАЦИИ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Аннотация. Настоящая статья посвящена иллюстрации возможностей использования методологического аппарата функционального моделирования для решения проблемы формализованного представления угроз деструктивного воздействия вредоносного программного обеспечения на операционную среду автоматизированной системы управления специального назначения. В ней рассматривается последовательность действий нарушителя по нарушению конфиденциальности, целостности и доступности информации в этих системах с использованием в качестве инструмента деструктивного воздействия на их операционную среду вредоносного кода. В статье представлены результаты функциональной декомпозиции целевой функции угрозы на реализуемые нарушителем ее этапы – инфильтрацию вредоносного кода в операционную среду автоматизированной системы управления специального назначения, выполнение им деструктивных действий и сокрытие им следов деструктивного воздействия. Описываются выполняемые при этом тактики, а также используемые техники применения вредоносного программного обеспечения. Приводится формализованное представление множественной структуры декомпозиционного представления целевой функции. В терминах методологии IDEF0 приводятся функциональные диаграммы соответствующих функциональных компонент. Обосновываются предпосылки для разработки в терминах Марковского процесса математических моделей для определения временных характеристик отдельных функциональных компонент и целевой функции в целом. Разработанная функциональная модель служит инструментом для оценки возможности нарушителя по реализации такого рода угроз и ущерб объекту управления, наносимый за счет информационных отказов системы. Целью данной статьи является иллюстрация возможностей достижения требуемого уровня адекватности математических моделей для исследования угроз деструктивного воздействия вредоносных объектов на подобного рода системы.

Ключевые слова: автоматизированные системы управления специального назначения, вредоносное программное обеспечение, функциональное моделирование, графическая нотация IDEF0, средства антивирусной защиты, защита информации.

Для цитирования: КОРЧАГИН, Игорь И. и др. ФУНКЦИОНАЛЬНОЕ МОДЕЛИРОВАНИЕ ФОРМАЛИЗАЦИИ ТАКТИК РЕАЛИЗАЦИИ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ. Безопасность информационных технологий, [S.l.], т. 31, № 4, с. 87–98, 2024. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1717. DOI: http://dx.doi.org/10.26583/bit.2024.4.05.

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 str., 75, Moscow, 127015, Russia
[2]Bauman Moscow State Technical University,
2nd Bauman 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

Functional modeling of formalization malware implementation tactics

Abstract. This paper is devoted to illustrating the possibilities of using the methodological apparatus of functional modeling to solve the problem of formalized representation of threats of destructive impact of malicious software on the operating environment of an automated control system for special purposes. It examines an attacker's sequence of actions to compromise the confidentiality, integrity, and availability of information on these systems, using malicious code as a tool to destructively affect their operating environment to their operating environment with malicious code. The article presents the results of functional decomposition of the target function of the threat into its stages realized by the intruder - infiltration of malicious code into the operating environment of a special-purpose automated control system, its execution of destructive actions and concealment of traces of destructive impact. The tactics performed in this process are described, as well as the malware techniques used. A formalized representation of the multiple structure of the decomposition representation of the target function is given. Functional diagrams of the corresponding functional components are given in terms of the IDEF0 methodology. The prerequisites for the development of mathematical models in terms of the Markov process for determining the time characteristics of individual functional components and the objective function as a whole are substantiated. The developed functional model serves as a tool for assessing the ability of an intruder to implement such threats and damage to the object of control caused by information failures of the system. The purpose of this article is to illustrate the possibilities of achieving the required level of adequacy of mathematical models for studying the threats of the destructive impact of malicious objects on such systems.

Keywords: automated control systems for special purposes, malicious software, functional modeling, IDEF0 notation, anti-virus information protection tools, data protection.
For citation: KORCHAGIN, Igor I. et al. Functional modeling of formalization malware implementation tactics. IT Security (Russia), [S.l.], v. 31, no. 4, p. 87–98, 2024. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1717. DOI: http://dx.doi.org/10.26583/bit.2024.4.05.

Введение

В условиях широкого внедрения компьютерных технологий в процессы управления [1], так называемой критической инфраструктурой [2] к таким процессам предъявляется целый ряд специальных требований. Эта тенденция привела к интенсивному развитию класса систем управления, известных как автоматизированные системы управления специального назначения (АСУ СН) [3]. Касаясь существа указанных требований следует отметить, что к ним в первую очередь относится требование своевременности обработки информации [4] в этих системах. Вместе с тем наряду с широкими возможностями по обеспечению данного требования за счет повышения уровня информатизации процессов управления потенциально существует фактор снижения своевременности обработки информации в

АСУ СН ввиду наличия уязвимостей информации [5] к возникновению угроз ее безопасности. Среди такого рода угроз наиболее актуальной угрозой нарушения конфиденциальности, целостности и доступности информации [6] в АСУ СН в настоящее время является воздействие вредоносного программного обеспечения (ВПО) [7] на операционную среду (ОС) этих систем. Являясь такими же информационными объектами для обработки, как и легитимное программное обеспечение, ВПО, путем маскировки своего присутствия в ОС, реализует вредоносные функции на фоне выполнения программ системного и прикладного обеспечения АСУ СН [8, 9]. Основным негативным влиянием воздействия ВПО на информационные процессы в АСУ СН является создание условий, когда система в течение некоторого времени не может функционировать по своему целевому назначению. Это обстоятельство оказывает непосредственное влияние на существенное снижение основной характеристики АСУ СН – своевременности обработки информации, что позволяет рассматривать воздействие ВПО как один из важнейших факторов, влияющих на эффективность АСУ СН в целом.

Это обусловило разработку и внедрения в практику эксплуатации АСУ СН технологий противодействия такого рода угрозам безопасности информации, известных как антивирусные технологии [10, 11]. Объективное требование адекватности реагирования антивирусными средствами на воздействие ВПО приводит к необходимости постоянного совершенствования этих средств. Это ставит весьма актуальную как в научном, так и в практическом плане проблему – проблему научного обоснования требований к способам и средствам антивирусной защиты в АСУ СН. Одной из главных задач, решаемых в процессе обоснования, является проведение всесторонних исследований процессов функционирования АСУ СН в условиях воздействия ВПО и реализации технологий антивирусной защиты. В этой связи следует отметить, что АСУ СН не могут являться объектом натурных экспериментов, ввиду высокой степени риска нанесения ущерба тем предметным областям, в интересах которых функционируют эти системы. Альтернативой здесь могут служить лишь вычислительные эксперименты с применением математических моделей, отличающихся высокой степенью адекватности.

Исходя из классических основ математического моделирования требование высокой степени адекватности математических моделей рассматриваемых процессов может быть достигнуто за счет применения соответствующих методов их формализации. Практика моделирования в области защиты информации дает основание утверждать, что к таким методам следует отнести функциональное моделирование [12, 13]. При этом предпосылкой адекватности здесь является глубина детализации целевой функции исследуемого процесса.

В [14] рассмотрены принципы построения функциональной модели целевой функции воздействия ВПО на ОС АСУ СН путем детализации данной функции на три этапа и ее реализации: этап инфильтрации вредоносного кода в ОС, этап выполнения деструктивных функций вредоносным кодом и этап сокрытия следов деструктивного воздействия. Естественно полагать, что подобная одноуровневая степень детализации целевой функции не обеспечивает сколь либо приемлемую адекватность ее формализованного представления. Поэтому рассмотрим возможность дальнейшей ее детализации с целью достижения приемлемого уровня. При этом будем использовать приводимые в [14] термины и обозначения.

1. Формализованное представление функциональной структуры этапа реализации целевой функции воздействия ВПО на операционную среду АСУ СН

В соответствии с приводимой в [14] процедурой функциональной декомпозиции целевой функции Φ – «Воздействие ВПО на ОС АСУ СН» функциональными компонентами первого уровня ее детализации являются этапы, функциональными компонентами второго уровня детализации являются используемые нарушителем тактики, а функциональными компонентами третьего уровня – применяемые при этом техники. Как уже отмечалось функциональная модель первого уровня рассмотрена в [14]. По аналогии с формализованным представлением первого уровня декомпозиции целевой функции второй уровень декомпозиции является следствием детализации ее этапов. Образуемое в результате множество тактик действий нарушителя представляется в виде:

$$\left\{\phi_{ij}^{(2)}\right\},\ i = 1,\ 2,\ 3,\ j = 1,\ 2,\ \ldots,\ J_i, \tag{1}$$

где j – номер выполняемой нарушителям тактики;

J_i – число тактик, используемых нарушителем при реализации *i*-го этапа.

Аналогичным образом, образуемое в результате декомпозиции *j*-ой тактики множество применяемых нарушителем техник составляет третий уровень декомпозиции целевой функции *Ф*. Само множество формально представляется в виде:

$$\left\{\phi_{ijk}^{(3)}\right\},\ i = 1,\ 2,\ 3,\ j = 1,\ 2,\ \ldots,\ J_i,\ k = 1,\ 2,\ \ldots,\ K_{ij}, \tag{2}$$

где k – номер применяемой нарушителем техники при реализации *j*-ой тактики;

K_{ij} – число техник, применяемых нарушителем при выполнении *j*-ой тактики в процессе реализации *i*-го этапа.

Для представления функциональных моделей этапов и соответствующих им тактик воспользуемся графической нотацией IDEF0 [15] методологии функционального моделирования.

2. Функциональная модель этапа инфильтрации вредоносного кода в операционную среду АСУ СН

Тактиками, используемыми нарушителем при реализации этапа инфильтрации вредоносного кода в ОС АСУ СН, являются тактика осуществления первоначального доступа и тактика выполнение и закрепление в системе. В терминах выражения (1) указанные тактики представляются как $\phi_{11}^{(2)}$ и $\phi_{12}^{(2)}$, соответственно. Порядок реализации перечисленных функциональных компонент приводится на рис. 1.

2.1 Функциональная модель тактики осуществления первоначального доступа

Техниками, применяемыми нарушителем при выполнении тактики осуществления первоначального доступа в процессе реализации этапа инфильтрации вредоносного кода в ОС АСУ СН, являются техника использования существующих учетных записей, техника распространения через съемные носители и техника использования доверительных отношений. В терминах выражения (2) указанные техники представляются как $\phi_{111}^{(3)}$, $\phi_{112}^{(3)}$ и $\phi_{113}^{(3)}$, соответственно. Порядок реализации перечисленных функциональных компонент приводится на рис. 2.

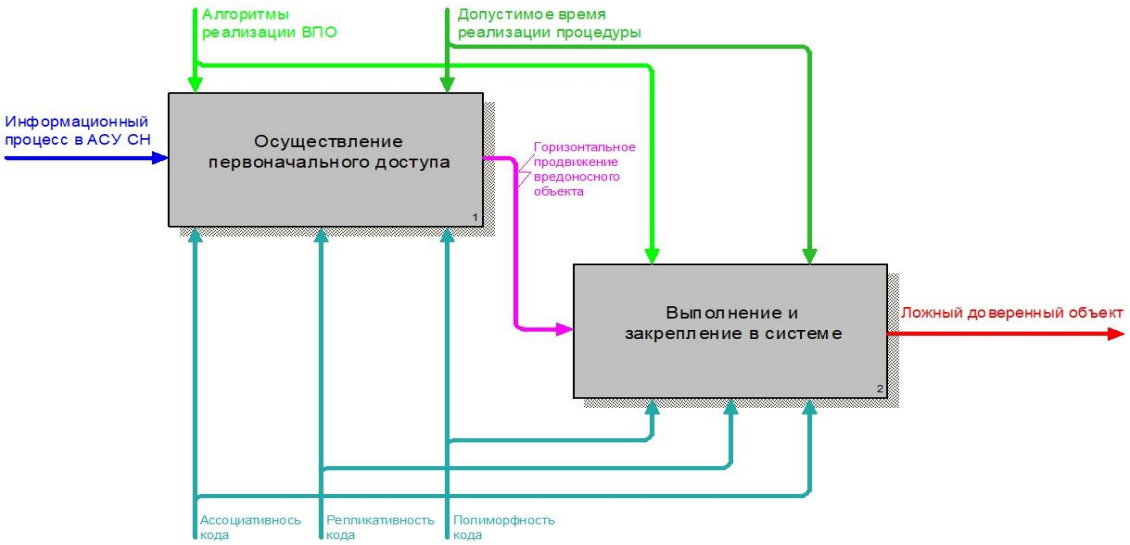

Рис. 1. Декомпозиционное представление этапа «Инфильтрация вредоносного кода в ОС АСУ СН»

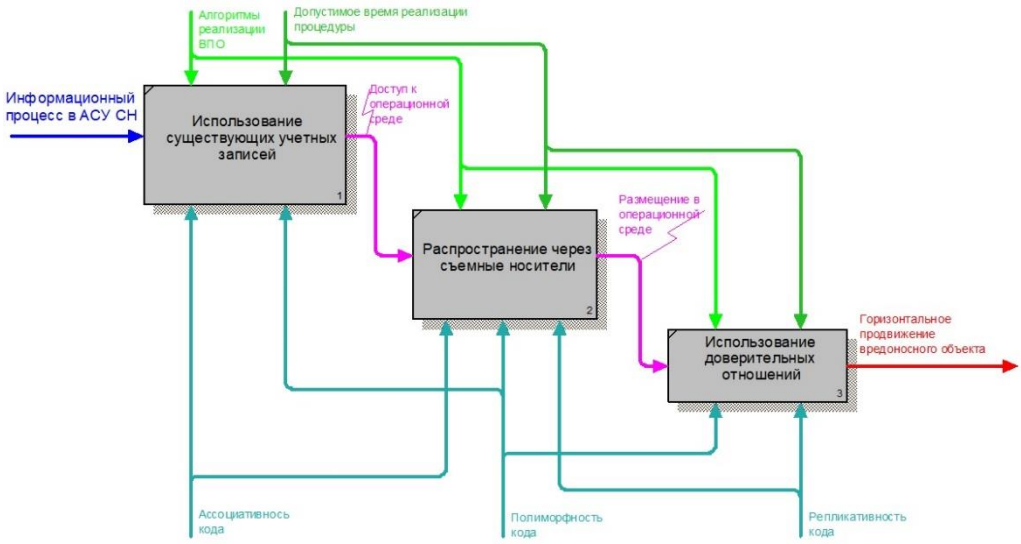

Рис. 2. Декомпозиционное представление тактики «Осуществление первоначального доступа»

2.2 Функциональная модель тактики выполнения и закрепления в системе

Техниками, применяемыми нарушителем при использовании тактики выполнения и закрепления в операционной среде в процессе реализации этапа инфильтрации вредоносного кода в ОС АСУ СН, являются техника воздействие на общие модули ОС и техника внедрения в определенные программные модули ОС. В терминах выражения (2) указанные техники представляются как $\phi_{121}^{(3)}$ и $\phi_{122}^{(3)}$, соответственно.

Порядок реализации перечисленных функциональных компонент приводится на рис. 3.

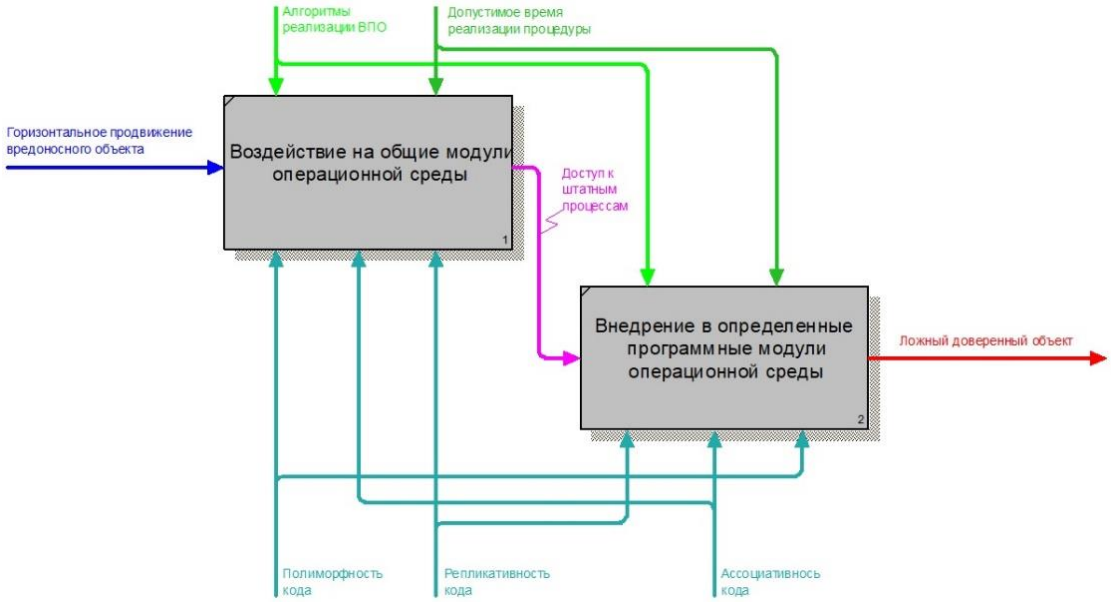

Рис. 3. Декомпозиционное представление тактики «Выполнение и закрепление в системе»

3. Функциональная модель этапа выполнения деструктивных действий вредоносным кодом в операционной среде АСУ СН

Тактиками, используемыми нарушителем при реализации этапа выполнения деструктивных действий вредоносным кодом в ОС АСУ СН, являются тактика уничтожение данных, тактика эксфильтрация данных и тактика манипуляции с данными. В терминах выражения (1) указанные тактики представляются как $\phi_{21}^{(2)}$, $\phi_{22}^{(2)}$ и $\phi_{23}^{(2)}$, соответственно.

Порядок реализации перечисленных функциональных компонент приводится на рис. 4.

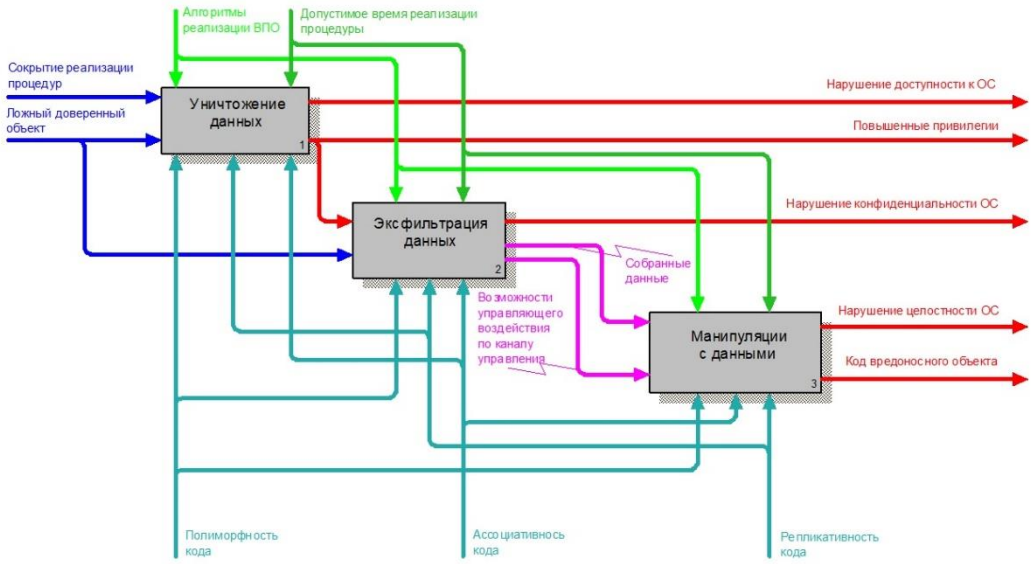

Рис. 4. Декомпозиционное представление этапа «Выполнение деструктивных действий вредоносным кодом в ОС АСУ СН»

3.1 Функциональная модель тактики уничтожение данных

Техниками, применяемыми нарушителем при использовании тактики уничтожение данных в процессе реализации этапа выполнения деструктивных действий вредоносным кодом в операционной среде АСУ СН, являются техника сброс учетных записей ОС, техника внедрения вредоносного кода в процессы, техника использования общих SMB- и административных ресурсов Windows, а также техника перезаписи файлов случайно сгенерированными данными. В терминах выражения (2) указанные техники представляются как $\phi_{211}^{(3)}$, $\phi_{212}^{(3)}$, $\phi_{213}^{(3)}$ и $\phi_{214}^{(3)}$, соответственно.

Порядок реализации перечисленных функциональных компонент приводится на рис. 5.

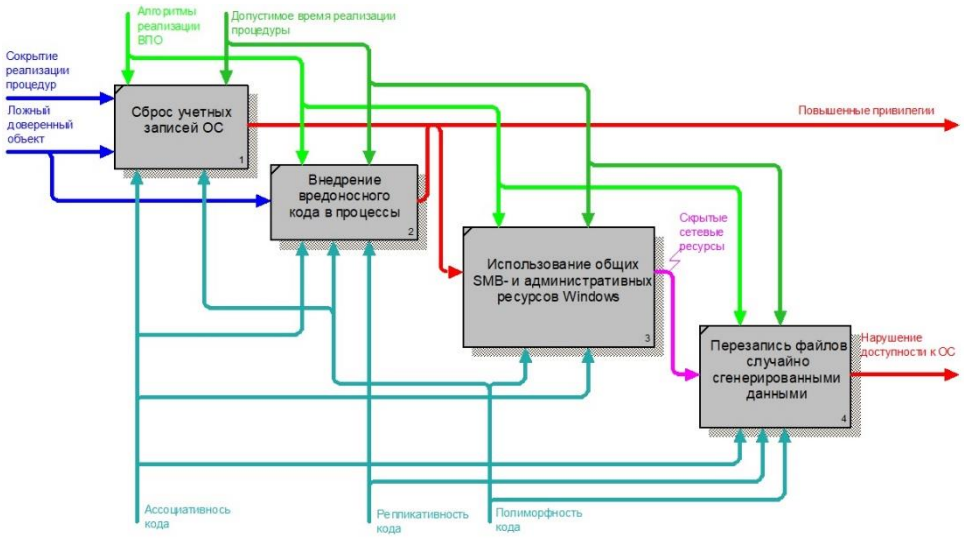

Рис. 5. Декомпозиционное представление тактики «Уничтожение данных»

3.2 Функциональная модель тактики эксфильтрация данных

Техниками, применяемыми нарушителем при использовании тактики эксфильтрация данных в процессе реализации этапа выполнения деструктивных действий вредоносным кодом в операционной среде АСУ СН, являются техника изучения файлов и каталогов, техника передачи инструментов внутри периметра и техника автоматизированного сбора данных. В терминах выражения (2) указанные техники представляются как $\phi_{221}^{(3)}$, $\phi_{222}^{(3)}$ и $\phi_{223}^{(3)}$, соответственно.

Порядок реализации перечисленных функциональных компонент приводится на рис. 6.

3.3 Функциональная модель тактики манипуляции с данными

Техниками, применяемыми нарушителем при использовании тактики манипуляции с данными в процессе реализации этапа выполнения деструктивных действий вредоносным кодом в операционной среде АСУ СН, являются техника манипуляции с хранимыми данными, техника манипуляции с передаваемыми данными, техника манипуляции с обрабатываемыми данными и техника нарушения целостности данных. В терминах выражения (2) указанные техники представляются как $\phi_{231}^{(3)}$, $\phi_{232}^{(3)}$, $\phi_{233}^{(3)}$ и $\phi_{234}^{(3)}$, соответственно.

Порядок реализации перечисленных функциональных компонент приводится на рис. 7.

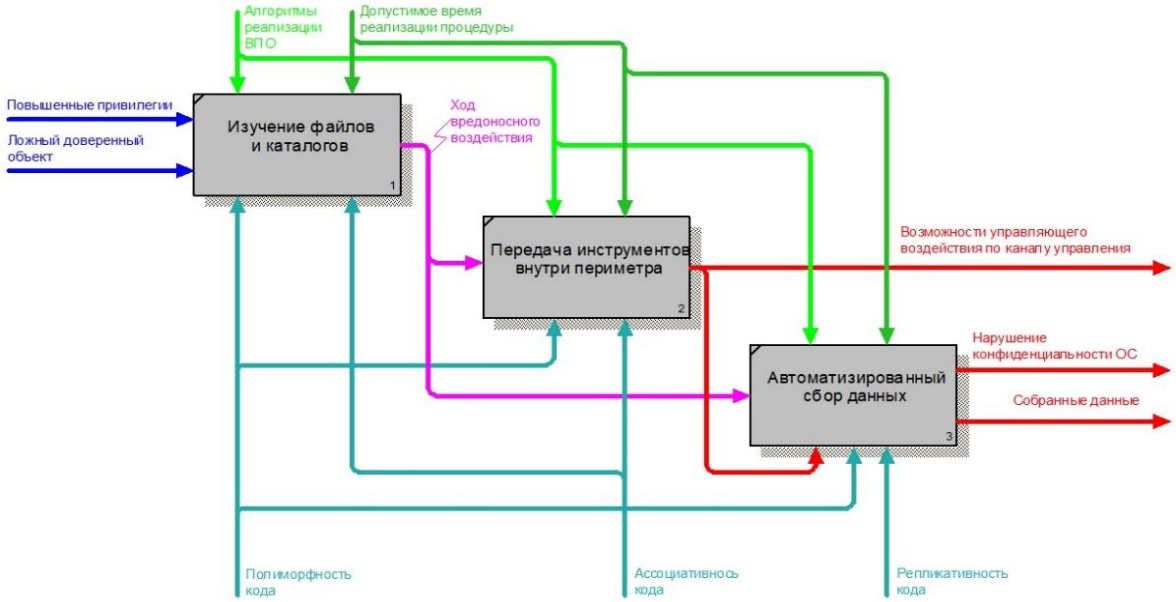

Рис. 6. Декомпозиционное представление тактики «Эксфильтрация данных»

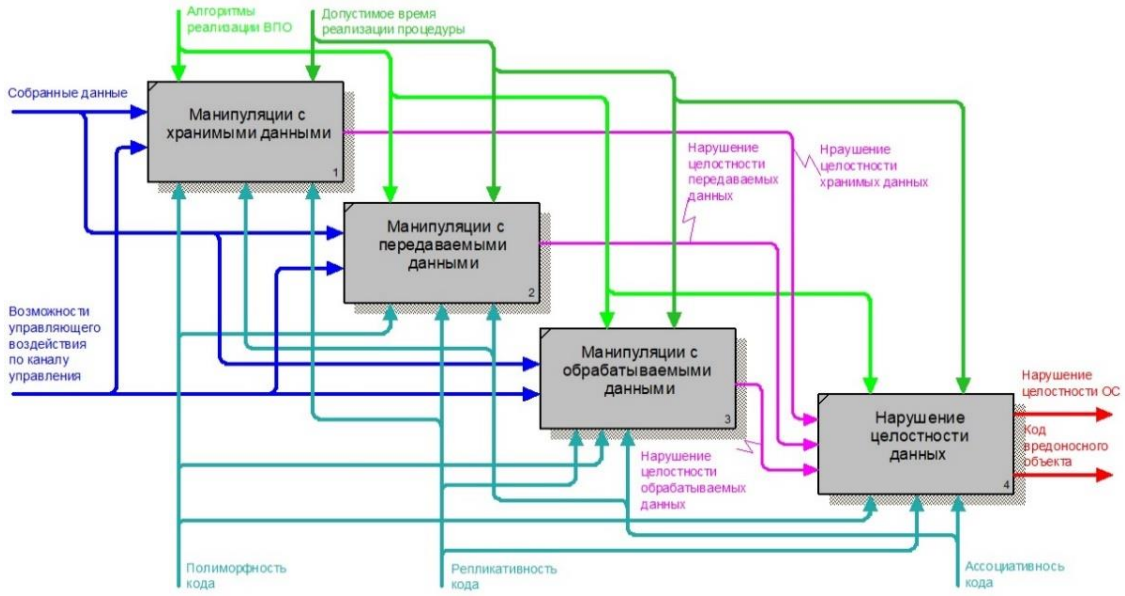

Рис. 7. Декомпозиционное представление тактики «Манипуляция с данными»

4. Функциональная модель этапа сокрытия следов воздействия вредоносного кода на операционную среду АСУ СН

Тактиками, используемыми нарушителем при реализации этапа сокрытия следов воздействия вредоносного кода на ОС АСУ СН, являются тактика предотвращения обнаружения и тактика самоуничтожения вредоносного кода. В терминах выражения (1) указанные тактики представляются как $\phi_{31}^{(2)}$ и $\phi_{32}^{(2)}$, соответственно.

Порядок реализации перечисленных функциональных компонент приводится на рис. 8.

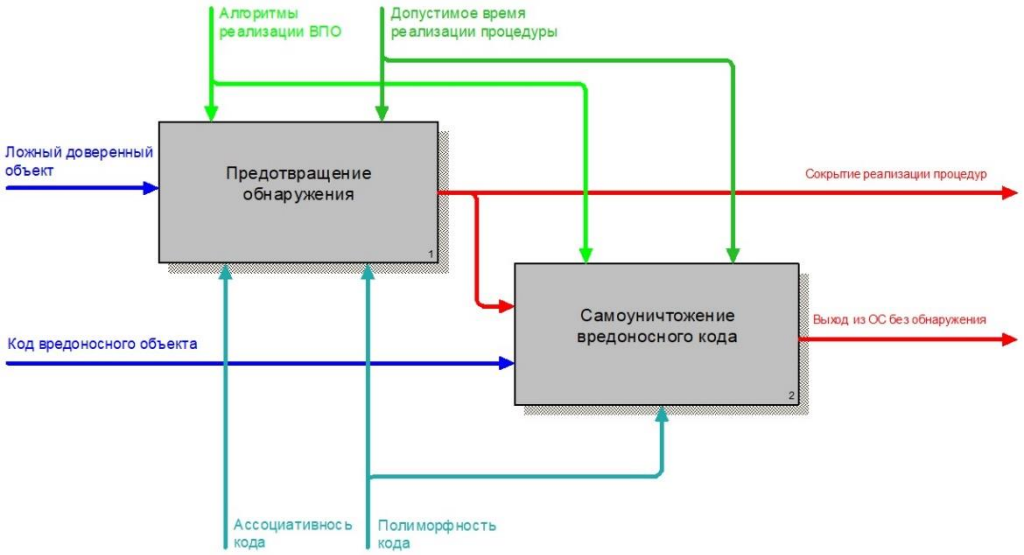

Рис. 8. Декомпозиционное представление этапа «Сокрытие следов воздействия вредоносного кода на ОС АСУ СН»

4.1 Функциональная модель тактики предотвращения обнаружения

Техниками, применяемыми нарушителем при использовании тактики предотвращения обнаружения, являются использование техники «Руткит» и использование техники «Маскировка». В терминах выражения (2) указанные техники представляются как $\phi_{311}^{(3)}$ и $\phi_{312}^{(3)}$, соответственно.

Порядок реализации перечисленных функциональных компонент приводится на рис. 9.

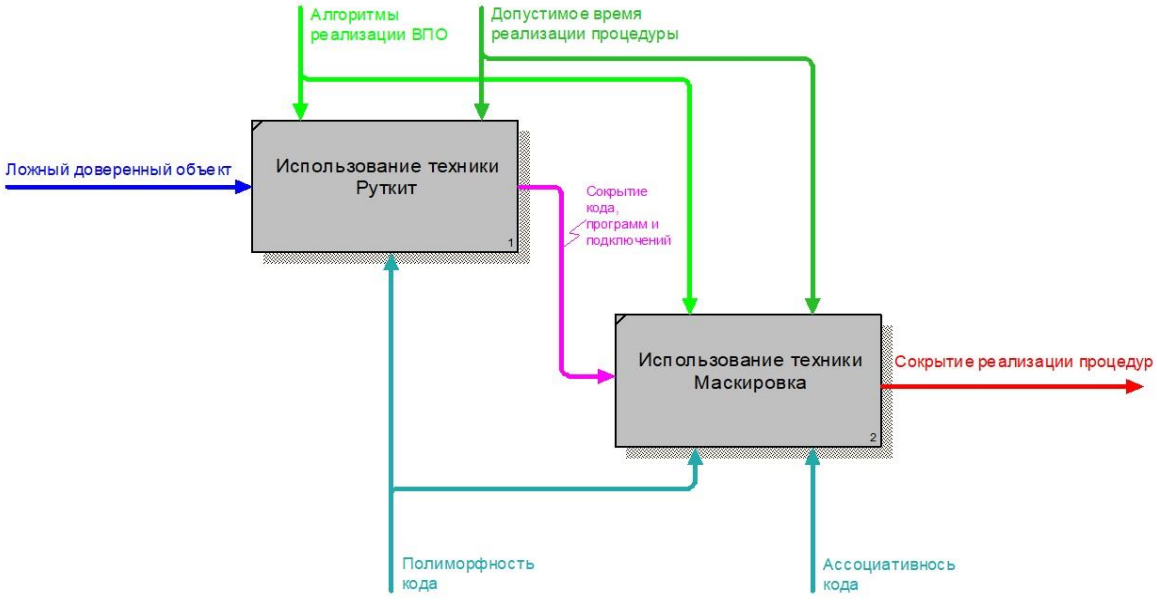

Рис. 9. Декомпозиционное представление тактики «Предотвращение обнаружения»

4.2 Функциональная модель тактики самоуничтожения вредоносного кода

Техниками, применяемыми нарушителем при использовании тактики самоуничтожения вредоносного кода, являются техника установки «тайм-бомбы» вредоносным объектом и техника уничтожения вредоносного кода при обнаружении САВЗ или завершения алгоритма процедуры. В терминах выражения (2) указанные техники представляются как $\phi_{321}^{(3)}$ и $\phi_{322}^{(3)}$, соответственно.

Порядок реализации перечисленных функциональных компонент приводится на рис. 10.

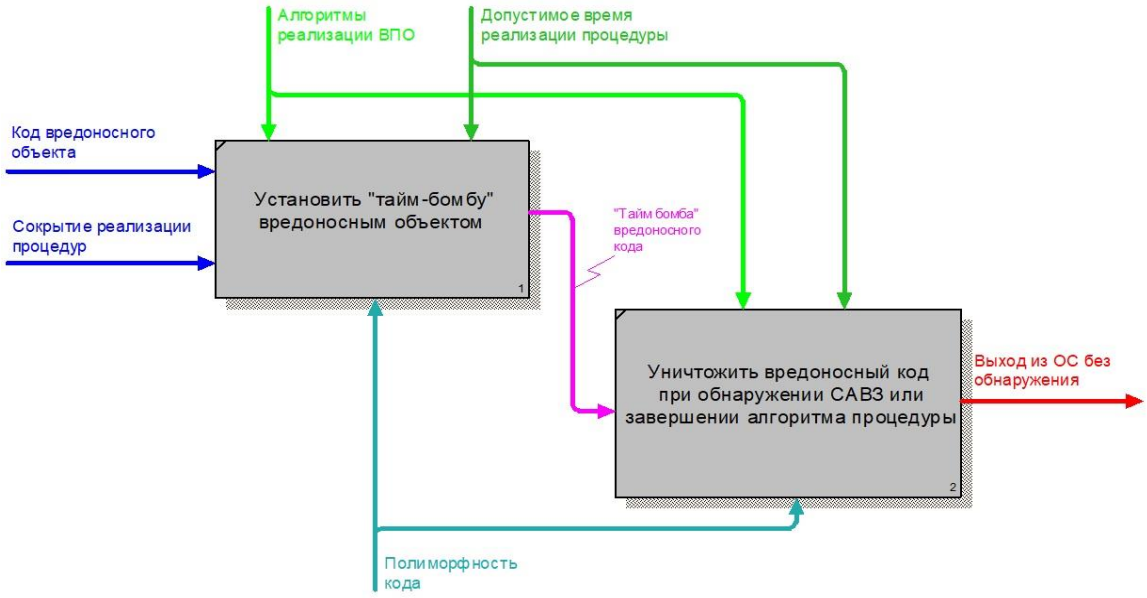

Рис. 10. Декомпозиционное представление тактики «Самоуничтожение вредоносного кода»

Заключение

Полученная ранее двухуровневая структура функционального представления целевой функции – «Воздействие ВПО на ОС АСУ СН» и дополненная в соответствии с материалами данной статьи третьим уровнем, обеспечивает целостное представление функциональной структуры данной целевой функции. Рассмотренные модели являются предпосылкой для разработки в терминах Марковского процесса математических моделей для определения временных характеристик отдельных функциональных компонент и целевой функции в целом. Это позволяет оценить возможности нарушителя по реализации такого рода угроз.

СПИСОК ЛИТЕРАТУРЫ:

1. Кардаш И.Л. Вопросы управления в территориальной системе обеспечения государственной и общественной безопасности. Вестник Академии военных наук: Управление вооруженными силами и их информатизация. 2024, № 1, с. 67–75. URL: https://www.elibrary.ru/item.asp?id=68620707 (дата обращения: 12.10.2024).
2. Устинов И.А., Игумнов В.В. Информационно-управляющие системы в обеспечении информационной безопасности критических инфраструктур. Региональная информатика и информационная безопасность: Информационные технологии в критических инфраструктурах. 2015, т. 1, с. 373–376. – EDN: XVOECF.
3. Жигулин Ю.А., Романов А.В., Сугак В.П. Задачи комплексного исследования устойчивости автоматизированных систем управления специального назначения. Труды военно-космической

академии имени А.Ф. Можайского. 2019, № 666, с. 18–27. URL: https://elibrary.ru/download/elibrary_38500904_32593057.pdf (дата обращения: 12.10.2024).
4. 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.
5. Храмова А.Р., Петросян Л.Э. Анализ уязвимостей в системах безопасности данных. Инженерный вестник Дона. 2023, № 6, с. 14–23. URL: https://cyberleninka.ru/article/n/analiz-uyazvimostey-v-sistemah-bezopasnosti-dannyh/viewer (дата обращения: 14.10.2024).
6. Добродеев А.Ю. Показатели информационной безопасности как характеристика (мера) соответствия сетей и организаций связи требованиям информационной безопасности. Теория систем. 2023, с. 92–114. – EDN: JPNUXN.
7. Аккаева Х.А. Кибератаки на критическую информационную инфраструктуру. Киберпреступность: Право и управление. 2023, № 9, с. 347–351. URL: https://cyberleninka.ru/article/n/kiberataki-na-kriticheskuyu-informatsionnuyu-infrastrukturu/viewer (дата обращения: 01.09.2024).
8. Стадник А.Н., Скрыль К.С, Купин Д.С. и др. Функциональное представление процедур компрометации в процессе воздействия вредоносного программного обеспечения на информационные ресурсы компьютерной системы. Телекоммуникации. М.: Издательство «Наука и технологии». 2023, № 6, с. 33–39. – EDN: YVIFXQ.
9. 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. DOI: 10.21681/2311-3456-2022-4-52-79.
10. Малахов М.А., Мельников Ю.С. Защита конечных точек: антивирусы. Информационные технологии в науке, бизнесе и образовании. 2020, с. 165–170. URL: https://www.elibrary.ru/item.asp?id=43100568 (дата обращения: 14.10.2024).
11. Харипов Т.К., Палютина Г.Н. Эффективность работы антивирусных программ в современных условиях. Информационные системы, экономика и управление: ученые записки. 2022, № 24, с. 104–107. URL: https://www.elibrary.ru/download/elibrary_50111490_68186013.pdf#page=104 (дата обращения: 01.09.2024).
12. Скрыль С.В., Стадник А.Н., Купин Д.С., Домрачев Д.В., Абачараева Э.Р. Функциональное моделирование как инструмент формализации угроз вирусных атак на информационные ресурсы компьютерных систем. Телекоммуникации. М.: Издательство «Наука и технологии». 2021, № 4, с. 14–19. DOI: 10.31044/1684-2588-2021-0-4-14-19. – EDN: DWOWUP.
13. Кругликов С.В., Касанин С.Н., Кулешов Ю.В. Методицеский подход к комплексному описанию объекта информационной защиты. Вопросы кибербезопасности. 2022, № 4(50), с. 39–51. DOI: 10.21681/2311-3456-2022-4-39-51.
14. 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.
15. Бакшеев А.С., Лившиц И.И. Разработка методики контроля уровня защищенности информации объектов критической информационной инфраструктуры. Вопросы кибербезопасности. 2023, № 2(54), с. 85–98. DOI: 10.21681/2311-3456-2023-2-85-98.

REFERENCES:

[1] Kardash I.L. Issues of management in the territorial system of ensuring state and public security. Bulletin of the Academy of Military Sciences: Management of the Armed Forces and Their Informatization. 2024, no. 1, p. 67–75. URL: https://www.elibrary.ru/item.asp?id=68620707 (accessed: 12.10.2024) (in Russian).
[2] Ustinov I.A., Igumnov V.V. Information Management Systems in Ensuring Information Security of Critical Infrastructures. Regional Informatics and Information Security: Information Technologies in Critical Infrastructures. 2015, v. 1, p. 373–376 (in Russian). – EDN: XVOECF.
[3] Zhigulin Yu.A., Romanov A.V., Sugak V.P. Tasks of a comprehensive study of the stability of automated control systems for special purposes. Proceedings of the Mozhaisky Military Space Academy. 2019, no. 666, p. 18–27. URL: https://elibrary.ru/download/elibrary_38500904_32593057.pdf (accessed: 12.10.2024) (in Russian).

[4] 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. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2021.1.07 (in Russian).
[5] Khramova A.R. Analysis of vulnerabilities in data security systems. A.R. Khramova, L.E. Petrosyan. Engineering Bulletin of Don. 2023, no. 6, 10 p. URL: https://cyberleninka.ru/article/n/analiz-uyazvimostey-v-sistemah-bezopasnosti-dannyh/viewer (accessed: 01.09.2024) (in Russian).
[6] Dobrodeev, A.Yu. Information security indicators as a characteristic (measure) of compliance of networks and communication organizations with information security requirements. Theory of systems. 2023, p. 92–114 (in Russian). – EDN: JPNUXN.
[7] Akkaeva Kh. A. Cyberattacks on the critical information infrastructure. Cybercrime: Law and Management. 2023, no. 9, p. 347–351. URL: https://cyberleninka.ru/article/n/kiberataki-na-kriticheskuyu-informatsionnuyu-infrastrukturu/viewer (accessed: 01.09.2024) (in Russian).
[8] Stadnik A.N., Skryl K.S., Kupin D.S. et al. Functional representation of compromise procedures in the process of malicious software impact on information resources of a computer system. Telecommunications. M.: Publishing house “Science and Technology”. 2023, no. 6, p. 33–39 (in Russian). – EDN: YVIFXQ.
[9] Kotenko I.V., Khmyrov S.S. Analysis of Models and Methods Used for Attribution of Cybersecurity Violators in the Implementation of Targeted Attacks. Cybersecurity issues. 2022, No. 4 (50), p. 52–79. DOI:10.21681/2311-3456-2022-4-52-79 (in Russian).
[10] Malakhov M.A., Melnikov Yu.S. Endpoint Protection: Antiviruses. Information Technologies in Science, Business and Education. 2020, p. 165–170. URL: https://www.elibrary.ru/item.asp?id=43100568 (accessed: 14.10.2024) (in Russian).
[11] Kharipov T.K., Palutina G.N. Efficiency of antivirus programs in modern conditions. Information systems, economics and management: scientific notes. 2022, no. 24, p. 104–107. URL: https://www.elibrary.ru/download/elibrary_50111490_68186013.pdf#page=104 (accessed: 01.09.2024) (in Russian).
[12] Skryl S.V., Stadnik A.N., Kupin D.S., Domrachev D.V., Abacharaeva E.R. Functional modeling as a tool for formalizing threats of viral attacks on information resources of computer systems. Moscow: Science and Technology Publishing House. 2021, no. 4, p. 14–19. DOI: 10.31044/1684-2588-2021-0-4-14-19 (in Russian). – EDN: DWOWUP.
[13] Kruglikov S.V., Kasanin S.N., Kuleshov Yu.V. Methodological Approach to the Complex Description of the Information Protection Object. Cybersecurity issues. 2022, no. 4(50), p. 39–51. DOI: 10.21681/2311-3456-2022-4-39-51 (in Russian).
[14] 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 (in Russian).
[15] Baksheev A.S., Livshits I.I. Development of a Methodology for Monitoring the Information Security Level of Critical Information Infrastructure Facilities. Cybersecurity issues. 2023, no. 2(54), p. 85–98. DOI: 10.21681/2311-3456-2023-2-85-98 (in Russian).

Поступила в редакцию – 03 сентября 2024 г. Окончательный вариант – 19 октября 2024 г.
Received – September 03, 2024. The final version – October 19, 2024.