Метод оценки живучести информационно-технических объектов по отношению к программно-аппаратным воздействиям

В.В.Мухортов[1], *Ю.В.Нефедьев*[2]

[1]*Военная академия войсковой противовоздушной обороны Вооруженных Сил Российской Федерации имени маршала Советского Союза А.М.Василевского,*
[2]*Краснодарское высшее военное училище им. генерала армии С.М.Штеменко*

Аннотация: В статье представлен метод проведения количественной оценки комплексной живучести информационно-технических объектов, по отношению к средствам программно-аппаратного воздействия, в том числе основанные на оценке соотношений разного рода воздействий, соотношении вероятности необратимых последствий для поврежденной и неповрежденной системы. Обоснована необходимость повышения комплексной живучести информационно-технических объектов для обеспечения безопасности в условиях глобального кибернетического пространства.
Ключевые слова: живучесть, информационно-технические объекты, инфосфера, киберживучесть, кибернетическое оружие, программно-аппаратные воздействия, техносфера.

В настоящее время наблюдается применение во всех сферах человеческой деятельности высокоинформатизированных систем (робототехнические комплексы, системы управления объектами критической инфраструктуры, информатизированные образцы техники (автомобили, авиация, бытовая техника и тд.), центры, сбора, обработки и анализа информации, каналы информационного обмена, другие объекты, оснащенные информационно-техническими средствами). Эти системы в полной мере функционируют кроме общепринятого физического пространства (техносферы), в инфосфере (киберпространстве, как глобального домена внутри инфосферы), что позволяет объединить их в один глобальный класс – информационно-технические объекты (ИТО).

При разработке и функционировании ИТО возникает необходимость оценки устойчивости их функционирования, которая определяется такими показателями как живучесть, надежность и помехозащищенность.

Однако в связи с тем, что в ноосфере с ростом технического прогресса, произошло формирование новой сферы, взаимодействующей с другими ее

составляющими – инфосферы, которая включает в себя киберпространство (кибер- (*cyber- с англ., префиксный элемент*) – связанный с компьютерными технологиями), появилась необходимость оценки устойчивости функционирования в ней сложных технических систем, а также комплексной устойчивости сложных технических систем, функционирующих одновременно в техносфере и инфосфере [1].

Если с классической устойчивостью и ее показателями в техносфере все определено, то с инфосферой возникает ряд проблем, характеризуемых виртуальностью этой среды, однако процессы, протекающие в ней могут оказывать воздействия, последствия которых могут проецироваться на техносферу, инфосферу и биосферу, рисунок 1.

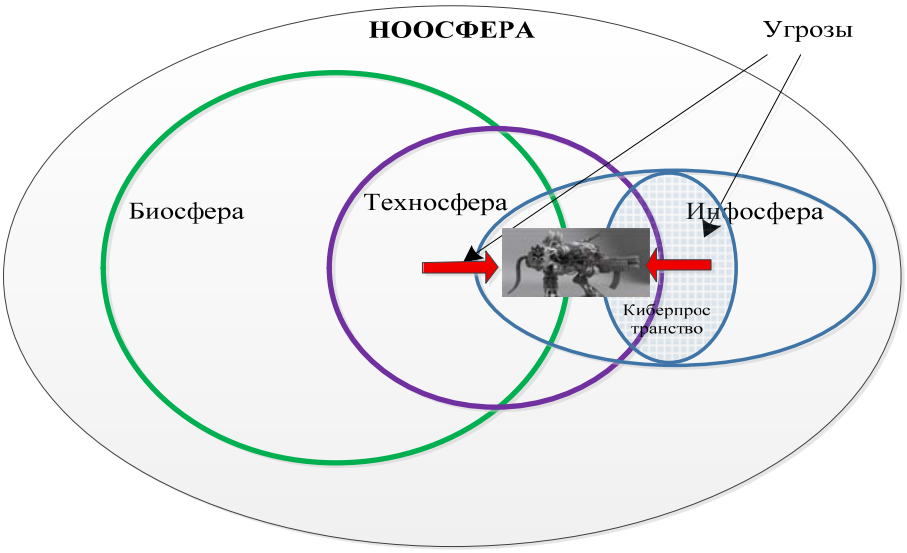

Рисунок 1 – Функционирование сложных технических систем под воздействием угроз в различных «сферах»

Рассмотрим один из показателей комплексной устойчивости комплексная живучесть.

Согласно классическим определениям, живучесть – применительно к военным системам, является одной из характеристик устойчивости и

отражает способность системы сохранять или быстро восстанавливать свое функционирование в условиях воздействия всех видов оружия противника.

В общем же виде – это способность системы выполнять предписанные ей функции после повреждения (разрушения) ее отдельных элементов. Основное отличие живучести от надежности – живучесть характеризует направленное воздействие, а не природное в отличие от надежности.

Таким образом, живучесть конкретной системы должна вычисляться по отношению к конкретным видам воздействий.

Живучесть системы можно рассмотреть через живучесть ее элементов,, а также через степень защищенности элементов. В качестве показателей оценки живучести ИТО и их элементов можно принять вероятность сохранения и/или восстановления системы при воздействии поражающих факторов всех видов оружия. При этом если с живучестью в техносфере всё более-менее ясно и определенно, то применительно к инфосфере имеется ряд вопросов и неопределенностей, связанных с виртуальностью этой сферы, а также ее взаимосвязями с физическим пространством.

В продолжение работ [2,3] введем следующие определения:

программно-аппаратное воздействие (ПАВ) – комплекс мероприятий, проводимых с преодолением систем защиты информационных (локальных, локально-распределенных, распределенных) вычислительных сетей и автономных программных (программно-технических) комплексов с целью нарушения функционирования технических средств обработки информации, а также добывания, разрушения, уничтожения или искажения информации.

кибернетическое оружие (кибероружие) – специальные программно-аппаратные средства, обладающие возможностями разрушения (нарушения штатной работоспособности) систем или их компонентов, входящих в киберпространство;

кибернетическое пространство (киберпространство) – глобальный домен внутри информационной сферы, состоящий из взаимосвязанной сети информационно-технологических инфраструктур, включая Интернет, телекоммуникационные сети, компьютерные системы, встроенные процессоры и контроллеры, а также биокибернетические объекты;

кибернетическая живучесть (киберживучесть) – способность информационного (информационно-технического) объекта сохранять или быстро восстанавливать свое функционирование в условиях воздействия информационного оружия, реализующего программно-аппаратные воздействия (кибероружие);

комплексная живучесть ИТО – способность информационно-технического объекта сохранять или быстро восстанавливать свое функционирование в условиях воздействия всех видов оружия в инфосфере и/или техносфере.

В ряде работ были отражены попытки оценки живучести (киберживучести) по отношению к программно-аппаратным воздействиям [4]. Не учитывалось, что эти системы являются ИТО и взаимодействуют на уровнях, выходящих за границы классической семиуровневой модели OSI.

В работе [5] не указаны виды программных помех, способных повредить интегрированным информационным системам, а также введен интегральный показатель живучести этих систем, выраженный через вероятность нарушения связи между корреспондирующими абонентами, а показатель живучести узла информационной системы – коэффициент доступности, характеризующий его возможности по обеспечению абонентов услугами с требуемым качеством, что не совсем корректно, исходя из классического определения живучести и введенного определения киберживучести и больше относится к теории надежности [6].

К угрозам, реализуемым с помощью кибероружия, можно отнести: вывод из строя, искажение системных программных модулей, перегрузку, переадресацию сообщений и инфицировние, в том числе по каналам связи, и активацию программно-аппаратных закладок, различного рода нарушения в самой системе [7].

Так же можно отметить, что в настоящее время отсутствуют общие подходы к проведению оценки живучести ИТО [8].

Вследствие высокого уровня неопределенности, связанной с типом и интенсивностью возможных ПАВ и вызываемых ими нарушений, а также способностью ИТО адаптироваться к повреждениям, мера живучести должна быть вероятностной, то есть должна определяться вероятность сохранения ИТО заданным показателям функционирования самой системы.

В связи с тем, что свойства, характеризующие киберживучесть ИТО в условиях осуществления ПАВ, начинают проявляться только после того, как данное воздействие было проведено, то мера комплексной живучести должна определяться через вероятность сохранения работоспособности системы при условии, что система получила некоторое повреждение D от ПАВ.

Исходя из таких определений, под показателем комплексной живучести ИТО - G будем понимать условную вероятность невыхода ИТО за пределы заданной области безопасных состояний S' области S в случае воздействия - Ω в физическом и/или информационном пространстве:

$$G^{тек} = P\left[\left(\left\|S - S_0\right\| < S'\right)\middle|\Omega\right], \quad (1)$$

В качестве критерия оценки комплексной живучести ИТО будем рассматривать выражение:

$$G^{тек}(t) \geq G^{тр}(t), \quad (2)$$

где $G^{тек}(t)$ – уровень комплексной живучести ИТО в настоящее время, а $G^{тр}(t)$ – необходимый уровень комплексной живучести ИТО в условиях осуществления ПАВ.

Для определения общего коэффициента комплексной живучести $k_G(t)$ [9] введем следующие универсальные уровни живучести:

$$k_G(t)=\begin{cases} G^{тек}(t)-G^{тр}(t)>0 & \text{- высокий уровень комплексной живучести;} \\ G^{тек}(t)-G^{тр}(t)=0 & \text{- средний уровень комплексной живучести;} \\ G^{тек}(t)-G^{тр}(t)<0 & \text{- низкий уровень комплексной живучести;} \\ G^{тек}(t)=0 & \text{- «нулевая» комплексная живучесть.} \end{cases} \quad (3)$$

$G^{тр}(t)$ для конкретного ИТО, рассчитывается в зависимости от его класса и предназначения.

В ИТО с высокой комплексной живучестью – определяется прямыми ущербами от локальных повреждений ИТО от ПАВ, в ИТО с низкой комплексной живучестью – вторичным ущербом от повреждений ИТО и косвенными ущербами от невыполнения поставленных задач. Таким образом, основным различием между ИТО с низкой и высокой комплексной живучестью является вид распределения ущерба.

Оценка комплексной живучести ИТО должна складываться из оценки живучести в техносфере и киберживучести в инфосфере, и, исходя из того что комплексная живучесть – это вероятностная величина, она примет вид:

$$G^{тр}(t)=G_T^{тр}(t)+G_K^{тр}(t)-G_T^{тр}(t)*G_K^{тр}(t); \quad (4)$$

$$G^{тек}(t)=G_T^{тек}(t)+G_K^{тек}(t)-G_T^{тек}(t)*G_K^{тек}(t) \quad (5)$$

где $G_T^{тр}(t)$ – требуемая живучесть в техносфере; $G_K^{тр}(t)$ – требуемая киберживучесть; $G_T^{тек}(t)$ – живучесть в техносфере в настоящий момент; $G_K^{тек}(t)$ – текущая киберживучесть.

Причем, при оценки киберживучести требуется производить оценку воздействия через виртуальную среду на физическое пространство. Таким образом, при воздействии кибероружия живучесть в техносфере является производной от киберживучести для ИТО (проекцией на техносферу) [10].

Иначе дело обстоит с объектами, функционирующими в киберпространстве (с программами, базами данных и т.д.), которые не взаимодействуют с физическим пространством – для них оценивается только киберживучесть, которая является для них основной и единственной, и тогда формулы примут вид:

$$G^{тр}(t) = G_K^{тр}(t); \tag{6}$$

$$G^{тек}(t) = G_K^{тек}(t). \tag{7}$$

С помощью индексов комплексной живучести, базирующихся на рисках, можно учесть весь спектр многовариантности сценариев ПАВ и состояний ИТО. При этом должны соблюдаться следующие разграничения:

прямые потери, вызванные ПАВ, $U_{пр\_K}$ и риски $R_{пр\_K}$, которые связаны с локальными повреждениями инфосферной составляющей ИТО в результате кибернетического воздействия[11];

косвенные потери, вызванные ПАВ, $U_{кос\_K}$ и риски $R_{кос\_K}$, возникающие в результате эскалации атакующих воздействий, и обусловленные потерей ИТО в целом.

Тогда показатель киберживучести может быть представлен в виде (нижележащая формула и ее описание полностью взяты из [9]):

$$G_{R\_K} = \frac{\sum_{i=1}^{m} R_{пр\_K}}{\sum_{i=1}^{m} R_{пр\_K} + \sum_{j=1}^{n} R_{кос\_K}} \tag{8}$$

где m – количество сценариев, в которых имеют место прямые ущербы ($U_{пр\_K}$) и риски ($R_{пр\_K}$) инфосферной составляющей ИТО, обусловленные

локальными повреждениями ИТО (т.е. общее количество сценариев), n – количество сценариев, в которых имеют место косвенные ущербы и риски инфосферной составляющей ИТО, возникающие в результате эскалации атакующих воздействий.

Данные показатели могут быть применены для оценки киберживучести ИТО без атакующих ПАВ противника. Однако они не позволяют показать текущий уровень киберживучести.

Эта величина, как вероятностная характеристика, может быть представлена в интервале [0;1]. Система является киберживучей, в тех случаях, когда косвенные риски имеют незначительный вклад в общесистемный риск $R_{s\_K} = R_{пр\_K} + R_{кос\_K}$, т.е. для киберживучих ИТО $G_{R\_K} \to 1$ – прямые риски значительно превышают косвенные $R_{пр\_K} >> R_{кос\_K}$. Напротив, у ИТО с низкой киберживучестью $G_{R\_K} \to 0$ прямые ущербы и риски незначительны по сравнению с косвенными $R_{пр\_K} << R_{кос\_K}$.

Таким образом, представленный показатель характеризует киберживучесть ИТО, как способность снижать риск разрушения (отказа системы) в случае ее локального повреждения в инфосфрере при ПАВ.

Показатель комплексной живучести ИТО будет сформирован в виде:

$$G_R = \frac{\sum_{i=1}^{m}(R_{пр\_K} + R_{пр\_T})}{\sum_{i=1}^{m}(R_{пр\_K} + R_{пр\_T}) + \sum_{j=1}^{n}(R_{кос\_K} + R_{кос\_T})}, \quad (9)$$

где m – воздействия, в которых присутствуют прямые ущербы ($U_{пр\_K}, U_{пр\_T}$) и риски ($R_{пр\_K}$ и $R_{пр\_K}$) инфосферной и техносферной составляющей ИТО, обусловленные локальными повреждениями ИТО (т.е. общее количество сценариев), n – количество сценариев, в которых имеют место косвенные ущербы и риски инфосферной и техносферной составляющей ИТО, возникающие в результате увеличения атакующих воздействий.

Данный индекс может быть использован для общей оценки комплексной живучести ИТО без ПАВ противника в настоящее время. Однако он не позволяет отслеживать текущий уровень комплексной живучести.

Эта величина, как вероятностный показатель, также варьируется в интервале [0;1]. Будем считать, что система является комплексно живучей, в тех случаях, когда косвенные риски вносят минимальный вклад в общесистемный риск $R_{s\_K} = R_{пр\_K} + R_{пр\_T} + R_{кос\_K} + R_{кос\_T}$, т.е. для комплексно живучих ИТО $G_R \to 1$ – прямые риски в разы превышают косвенные $R_{пр\_K} + R_{пр\_T} >> R_{кос\_K} + R_{кос\_T}$. Напротив, у ИТО с низкой комплексной живучестью $G_R \to 0$ прямые ущербы и риски незначительны по сравнению с косвенными $R_{пр\_K} + R_{пр\_T} << R_{кос\_K} + R_{кос\_T}$.

Таким образом, представленный показатель характеризует комплексную живучесть ИТО, как их способность уменьшать риск деструктивных воздействий в случае ее локального повреждения в инфосфрере и техносфере при ПАВ и иных воздействий.

Для ИТО специального назначения (в первую очередь военные системы) существует дополнительные требования к боеспособности систем $W_{бое}$ ИТО – способности выполнить непосредственную боевую задачу, которая находится в зависимости от способности после воздействия средств поражения противника выполнять поставленную боевую задачу, т.е. комплексной живучести ИТО специального назначения. $W_{бое}$ ИТО является одной из характеристик комплексной живучести, зависящей от конкретных типов воздействий на всех возможных «полях боя».

Установим следующие значения критерия боеспособности – $W_{бое}$ ИТО специального назначения

$$W_{бое}\begin{cases} G^{тек}(t) \geq N & \text{– ИТО специального назначения боеспособен} \\ G^{тр}(t) \leq G^{тек}(t) < N & \text{– ИТО специального назначения ограниченно боеспособен, при обязательном решении наиболее важной задачи} \\ G^{тек}(t) < G^{тр}(t) & \text{– ИТО специального назначения не боеспособен.} \end{cases}$$

где N – оптимальное значение комплексной живучести, позволяющее выполнить весь спектр задач согласно предназначению ИТО специального назначения в условиях боестолкновения с высокотехнологичным противником.

Для выполнения поставленной задачи для ИТО специального назначения комплексная живучесть является одним из важных показателей, свидетельствующих об их боеспособности и боеготовности после выполнения разовой задачи [12].

Выводы: таким образом, для обеспечения требуемого уровня комплексной живучести ИТО необходима их защита от ПАВ в условиях глобального и постоянно растущего киберпространства.

ИТО, обладающие большой киберживучестью, выходят из строя постепенно, сохраняя при этом ограниченную работоспособность (боеспособность по отношению к специальным системам). Это позволяет принимать защитные действия, тем самым, сводя последствия воздействия главным образом к первичным ущербам от повреждения элементов ИТО. ИТО с малой комплексной живучестью разрушаются мгновенно и катастрофически, что сопровождается значительными вторичными и каскадными разрушениями, которые являются несоразмерными (непропорциональными) инициирующим ПАВ.

Дальнейшие исследования в этой области позволит обеспечить требуемый уровень обнаружения ПАВ, киберживучести по отношению к

ним, комплексной живучести ИТО [13], а для ИТО специального назначения и требуемый уровень боеспособности.

Литература

1. Минаев В.А., Королев И.Д., Мухортов В.В. Комплексная оценка устойчивости функционирования сложных технических систем в техносфере и инфосфере. Вопросы радиоэлектроники. 2018;(5):89-94. URL:doi.org/10.21778/2218-5453-2018-5-89-94.

2. Коцыняк М.А., Кулешов И.А., Кудрявцев А.М., Лаута О.С. Киберустойчивость информационно-телекоммуникационной сети // М.: Бостон-спектр, 2015. 150 с.

3. Голуб Б.В., Кузнецов Е.М., Максимов Р.В. Методика оценки живучести распределенных информационных систем // Вестник ССУ, 2014, URL: vestnik.ssu.samara.ru/tgt/2014_07_221.pdf.

4. Гриценко В.В., Зотов А.И. Надежностная модель частичного отказа в технической системе // Инженерный вестник Дона, 2019, №2 URL: ivdon.ru/ru/magazine/archive/n2y2019/5759.

5. Фиговский О.Л. В интервале пяти лет появятся инновации, которые сегодня кажутся фантастикой // Инженерный вестник Дона, 2011, №4 URL: ivdon.ru/ru/magazine/archive/n4y2011/643.

6. Выговский Л.С. Метод, методика и способы обеспечения надежности интегрированных компьютерных сетей: дис. ... канд. техн. наук. М., 2011. 163 с.

7. Давыдов А.Е., Савицкий О.К., Максимов Р.В. Защита и безопасность ведомственных интегрированных инфокоммуникационных систем // М.: ОАО «Воентелеком», 2015. С 520.

8. Птицын Г.А. Методы оценки и математические модели живучести сетей связи // T-Comm: Телекоммуникации и транспорт, 2016. №4, С. 47-51.

9. Махутов Н.А., Резников Д.О., Петров П.В. Оценка живучести сложных технических систем // Проблемы безопасности и чрезвычайных ситуаций. 2009. № 3. С. 47–66.

10. Report to the Committee on Armed Services, U.S. Senate. Weapon systems cybersecurity DOD. Just Beginning to Grapple with Scale of Vulnerabilities, October 2018.

11. The infosphere of social sciences: Structure, boundaries, and functions // link.springer URL: link.springer.com/article/10.3103%2FS0147688217020022 (дата обращения: 20.05.2019).

12. Мухортов В.В., Минаев В.А., Королев И.Д. Марковские модели защиты информационных систем беспилотных робототехнических объектов // Электронный журнал «Технологии техносферной безопасности». Академия ГПС МЧС РФ, 2016. №6, URL: ipb.mos.ru/ttb/2016-6.html.

13. Анг Чжо Мьо, Анисимов А.А., Портнов Е.М., Гагарина Л.Г. Методика повышения эффективности управления ресурсоемкими задачами в распределенных вычислительных системах // Инженерный вестник Дона, 2020, №2 URL: ivdon.ru/ru/magazine/archive/N2y2020/6294 .

References

1. Minaev V.A., Korolev I.D., Mukhortov V.V. Kompleksnaya ocenka ustoychivosti funkcionirovania slojnyh tehnicheskih system v tehnosfere i infosfere [Integrated assessment of stability functioning complex technical systems in the techno and info sphere]. Issues of radio electronics. 2018 ;(5):89-94. (In Russ.) URL: doi.org/10.21778/2218-5453-2018-5-89-94.

2. Kocinyak M.A., Kuleshov I.A., Kudryavcev A.M., Lauta O.S. Kiberustoychivost informacyonnoy-telecommunikacionnoy sety [Cyber resilience of the telecommunications network]. M: Boston-spectr, 2015. 150 p.

3. Golub B.V., Kuznecov E.M., Maksimov R.V. Vestnyk SSU, 2014, URL: vestnik.ssu.samara.ru/tgt/2014_07_221.pdf.

4. Gricenko V.V., Zotov A.I. Inzenernyj vestnik Dona, 2019, №2. URL: ivdon.ru/ru/magazine/archive/n2y2019/5759.

5. Figovsky O.L. Inzenernyj vestnik Dona, 2011, №4. URL: ivdon.ru/ru/magazine/archive/n4y2011/643.

6. Vigovskiy L.S. Metod, metodika i sposoby obespechenya nadegnosty integrirovannyh komputernyh setey [Method, methodology and methods for ensuring the reliability of integrated computer networks]: dis. ... kand. tehn. nauk. M., 2011. 163 p.

7. Davydov A.E., Savickiy O.K., Maksimov R.V. Zashita i bezopasnost vedomstvennyh integrirovannyh infokommunikacionyh system [Protection and security of departmental integrated information and communication systems]. M.: OAO “Voentelekom”, 2015. 520 p.

8. Ptycin G.A. T-Comm: Telekommunicacii i transport, 2016. №4, pp. 47-51.

9. Mahutov N.A., Reznikov D.O., Petrov P.V. 2009. № 3. pp. 47–66.

10. Report to the Committee on Armed Services, U.S. Senate. Weapon systems cybersecurity DOD. Just Beginning to Grapple with Scale of Vulnerabilities, October 2018.

11. The infosphere of social sciences: Structure, boundaries, and functions //link.springer URL: link.springer.com/article/10.3103%2FS0147688217020022 (data obrashenya: 20.05.2019).

12. Muhortov V.V., Minaev A.V. Korolev I.D. Elektronny gurnal “Tehnologii tehnosphernoy bezopasnosty”. Academya GPC MCHS RF, 2016. №6, URL: ipb.mos.ru/ttb/2016-6.html.

13. Анг Чжо Мьо, Anisimov A.A., Portnov E.M., Gagarina Л.Г. Inzenernyj vestnik Dona, 2020, №2. URL: ivdon.ru/ru/magazine/archive/N2y2020/6294.