DOI 10.15276/imms.v10.no1-2.84
УДК 004. 681.3

Informatics and Mathematical Methods in Simulation
Vol. 10 (2020), No. 1-2, pp. 84-89

ЖИВУЧЕСТЬ СИСТЕМЫ КИБЕРБЕЗОПАСНОСТИ ГОСУДАРСТВА

В.А. Хорошко, Ю.Е. Хохлачева, А. Аясрах, А. Аль-Далваш

Национальный авиационный университет,
пр. Любомир Гузар, 1, Киев, 03058, Украина; e-mail: post@nau.edu.ua

В настоящее время стремительно развивающиеся информационные технологии, динамично растущие объемы информации и увеличение ее значимости в жизни современного общества и государства в целом ставит вопрос информационной и кибербезопасности в ряд наиболее актуальных, а проблемам защиты информации и киберзащиты уделяется все большее внимание, что обуславливает растущее количество публикаций по данной тематике во всем мире. Практически все авторы так или иначе считают проблему надежной и живучей системы защиты информации наиболее острой, при этом сама проблема защиты информации и киберзащиты трактуется в широком смысле – как проблема предупреждения ее искажения или уничтожения, несанкционированной модификации, злоумышленного получения и использования информации и т.п. Влияние случайных факторов на процессы защиты информации делает практически непригодными методы классической теории систем применительно к решению задач создания, организации и обеспечения функционирования системы защиты. Количество (и виды) воздействий и процессов, связанных с несанкционированным (а возможно и случайным) доступом к информации определить практически невозможно. Одним из важнейших вопросов при проектировании и эксплуатации систем защиты информации является вопрос обеспечения и оценки ее живучести. В работе было проведено исследования, которые показали, что критерии вероятностной оценки качества функционирования средств защиты и оценки надежности (живучести) системы защиты в целом можно использовать. К обобщенному процессу защиты применены критерии теории надежности, позволяющие в ходе проектирования и эксплуатации систем защиты оперативно оценивать ее надежность (живучесть, готовность).

Ключевые слова: кибербезопасность государства, живучесть системы защиты, надежность системы защиты, готовность.

Введение

Динамично растущие объемы информации и увеличение ее значимости в жизни современного общества и государства в целом, ставит вопрос информационной и кибербезопасности в ряд наиболее актуальных в настоящее время.

Сегодня проблемам защиты информации и киберзащиты уделяется все большее внимание, чем обусловлено растущее количество публикаций по данной тематике. Практически все авторы так или иначе считают проблему надежной и живучей защиты информации наиболее острой, при этом сама проблема защиты информации и киберзащиты трактуется в широком смысле – как проблема предупреждения ее искажения или уничтожения, несанкционированной модификации, злоумышленного получения и использования информации и т.п.

Однако, как растущее количество публикаций, ни увеличивающееся число специализированных фирм и организаций, осуществляющих деятельность, так или иначе связанную с кибербезопастностью (которая является составной частью информационной безопасности), не могут не только решить проблему, но и зачастую прийти к согласию по частным вопросам. И объяснить это можно довольно просто – неопределенностью (либо многообразием) исходных для проектирования систем защиты данных: объектов защиты-множество; видов и количества угроз – множество;

пользователей информации (ПИ) и источников информации (ИИ) – множество; возможностей взаимодействий ПИ с ИИ – множество и т.д. Действительно, при проектировании комплексной системы защиты (составной частью, которой является система киберзащиты), связанной с конкретным объектом, можно получить количественную информацию по объектам защиты, ПИ, и ИИ. Но количество (и виды) воздействий и процессов, связанных с несанкционированным (а возможно и случайным) доступом к информации определить практически невозможно. И это неоспоримо, иначе возможным было бы построение абсолютной системы защиты информации, что, как известно, не является возможным.

Основная часть

Таким образом, влияние случайных факторов на процессы защиты информации делает практически непригодными методы классической теории систем применительно к решению задач создания, организации и обеспечения функционирования системы защиты [1, Т.1 С.50, Т.2, С.13].

В условиях конкретной задачи можно попытаться применить эмпирический подход. Однако, он не может претендовать на моделирование абсолютно всех возможных ситуаций, а кроме этого, может быть связан со значительными материальными затратами, неадекватными к стоимости самой защищаемой информации. И здесь незаменимыми оказываются методы теории вероятностей [2, С.25] и теории принятия решений. [3, С.201].

В этом плане работа [4, С.192] является базовой, обобщающей и дающей основы вероятностной модели системы защиты. Анализ преимуществ и недостатков такой модели дает работа [4, С.93]. В ней рассматривается модель, которая привлекательна своей простотой. Причем, для определения показателей защищенности информации достаточно знать вероятностные характеристики дестабилизирующих воздействий на информацию и эффективность функционирования системы защиты. Кроме того, можно делать вывод, что такую модель целесообразно использовать при оценке надежности и живучести системы защиты на этапе проектирования и эксплуатации ее, а также при оперативной оценке возможностей проектируемой и эксплуатируемой системы.

Однако, вероятностные методы могут быть эффективными не только при построении модели самой системы защиты, но и при разработке критериев функционирования средств защиты информации, согласно с работой [5, С.187], качество функционирования определяется вероятностной мерой, значение которой соответствует доверию к конкретному средству защиты со стороны потребителя. Такую оценку можно проводить путем оценки двух показателей- целостности средства защиты и непрерывности обслуживания (вероятность живучести средств защиты в произвольный момент времени и безотказной работы с этого момента в течении заданного интервала). Оценка качества по данным критериям позволяет выбрать оптимальные средства защиты в рамках конкретной задачи.

Предлагаемые критерии можно применять к средствам защиты информации, однако применять их к оценке системы защиты не представляется возможным хотя бы потому, что задачу придется рассматривать в общем, абстрагировавшись от этапов построения конкретной системы защиты и выбора конкретных средств защиты информации.

Несмотря на важность количественной оценки качества, можно утверждать, что одним из важнейших вопросов при проектировании и эксплуатации является именно вопрос обеспечения и оценки живучести системы защиты. Применительно к системе защиты от несанкционированного действия живучесть – это свойство системы защиты обеспечивать защиту от несанкционированных действий в течение заданного

промежутка времени. Под отказом системы защиты понимается обнаружение злоумышленником канала несанкционированных действий к информации [2].

Подход работы [2, С.221], где аналогично теории надежности вычислительных систем в качестве двух важнейших параметров, характеризующих систему защиты, вводятся интенсивность отказов (среднее число возможных отказов в единицу времени α) и время восстановления системы после отказа ($T_в$), является перспективным в плане применения этих критериев и вероятностной модели [4] и в последствии модели [5], которая не имеет недостатков, присущих вероятностным моделям и является более общей.

Итак, согласно [2, С.23], под интенсивностью отказов системы защиты от несанкционированных действий будем понимать интенсивность обнаружения каналов несанкционированных действий по отношению к информации в единицу времени. При расчете надежности и живучести принимаем, что интенсивность отказов постоянная во времени величина. Если предположить, что угрозы несанкционированных действий взаимно независимы и любая *i*-я $(i = 1, 2, ..., I)$ угроза носит катастрофический характер, то интенсивность отказов системы защиты равна сумме интенсивностей угроз несанкционированных действий к соответствующей системе защиты:

$$\lambda = \sum_{i=1}^{I} \lambda_i .$$

Тогда вероятность непрерывной работы системы защиты в течение произвольного интервала времени определяется следующим образом:

$$p(t) = e^{-\lambda \cdot t} .$$

Соответственно, обратная величина интенсивности отказов системы равна среднему промежутку времени между двумя отказами и называется [2, С.315] временем наработки на отказ:

$$T = 1/\lambda .$$

Интенсивность отказов системы определяется различными параметрами, в том числе сложностью исследования механизмов защиты, реализованных в системе, квалификацией злоумышленника, временным интервалом эксплуатации системы защиты.

Второй составляющей надежности системы защиты, как уже отмечалось, является время восстановления. Под этим понятием понимается интервал времени, в течение которого после возникновения отказа системы защиты обнаруженный канал несанкционированных действий на информацию устраняется. Время восстановления характеризуется двумя компонентами: временем установления соответствующего канала несанкционированных действий на информацию разработчиком системы защиты (T_y), и временем внедрения на защищаемый объект исправлений $(T_{ИС})$. Можно принять среднее время восстановления определяющимся средним временем устранения канала несанкционированных действий к информации:

$$T_B = T_y + T_{ИС} .$$

Можно считать в течение всего времени восстановления систему защиты отказавшей, а защищаемый объект – незащищаемым. Однако следует учитывать тот фактор, что живучесть системы защиты не позволяет оставить объект не защищенным. Считается, что выход параметров системы защиты за границы допусков все-таки

обеспечивает какой-то уровень защиты и она противодействует несанкционированным действиям злоумышленников.

С точки зрения теории надежности, эксплуатационные свойства системы защиты могут быть охарактеризованы коэффициентом готовности [2, С.172]:

$$K_r = T / \left(T + T_B\right).$$

Коэффициент готовности характеризует не только долю времени, в течение которого система защиты работоспособна, а вероятность того, что в любой произвольный момент времени система защиты работоспособна.

Для того, чтобы проиллюстрировать смысл такой характеристики, как коэффициент готовности и его связь с временем восстановления, можно рассматривать вопрос следующим образом.

Примем интенсивность обнаружения ошибки, которая может привести к несанкционированным действиям к информации, равной 1 в месяц [5]. В таблице 1 показано изменение коэффициента готовности системы при различных значениях времени восстановления. Полученные результаты наглядно свидетельствуют о том, что, следуя требованиям к надежности системы (определяемым обычно коэффициентом готовности 0,99), время восстановления системы должно определяться часами.

Таблица 1.

Изменение коэффициента готовности системы при различных значениях времени восстановления

Время восстановления	2 недели	1 неделя	3 дня	1 день	12 часов
Коэффициент готовности	0,682	0,811	0,909	0,968	0,984

Теперь рассмотрим два основных критерия оценки надежности (живучести) системы защиты на базе обобщенной модели процесса защиты информации [1,5] и общей модели системы, построенной в [4,5]. Вероятность нейтрализации несанкционированных действий с учетом введенного выше коэффициента готовности системы будет определяться выражением (для системы защиты, обладающей свойствами контроля в обнаружении несанкционированных действий):

$$P_{ЗН} = P_{обн} \cdot K_Г \cdot P_{ФМ} \cdot e^{-\lambda \cdot t} \cdot \left(\left(1 - P_{обх1}\right) \vee \left(1 - P_{обх2}\right) \vee \ldots \vee \left(1 - P_{обхn}\right)\right),$$

где $P_{обн} = 1 - t_{пр} / t_{обн}$ - вероятность обнаружения нарушителя; $t_{пр}$ - время преодоления системы защиты; $t_{обн}$ - время обнаружения злоумышленника; $K_Г$ - коэффициент готовности системы защиты; $P_{ФМ}$ - вероятность отказа системы защиты в результате наступления форс-мажорных обстоятельств; $P_{обхi}$ - вероятность обхода системы защиты по *i*-ому возможному пути ($i = \overline{1,n}$).

Данное соотношение можно использовать и для оценки многозонной или многорубежной системы защиты, тогда по этой формуле будет определяться вероятность предотвращения несанкционированных действий конкретным злоумышленником в конкретном звене или на конкретном рубеже.

Выводы

Проведенные исследования показали, что критерии вероятностной оценки качества функционирования средств защиты и оценки надежности (живучести) системы защиты в целом можно использовать. К обобщенному процессу защиты применены критерии теории надежности, позволяющие в ходе проектирования и эксплуатации систем защиты оперативно оценивать ее надежность (живучесть, готовность).

Список литературы

1. Ленков С.В., Перегудов Д.А, Хорошко В.А. Методы и средства защиты информации: в 2-х томах. К: Арий, 2008.
2. Креденцер Б.П. Расчет показателей надежности технических систем с избыточностью. К: Феникс, 2019. 520 с.
3. Тарасов В.А., Герасимов Б.М., Левик Н.А., Корнейчук В.А. Интеллектуальные системы поддержки принятия решений: теория, синтез, эффективностью. К: МАКНС, 2007. 336 с.
4. Павлов І.М., Хорошко В.О. Проектування комплексних систем захисту інформації. К: ВІТІ – ДУІКТ, 2011. 245 с.
5. Кобозєва А.А., Мачалін І.О, Хорошко В.О. Аналіз захищеності інформаційних систем. К: ДУІКТ, 2010. 316 с.

ЖИВУЧІСТЬ СИСТЕМИ КІБЕРБЕЗПЕКИ ДЕРЖАВИ

В.О. Хорошко, Ю.Є. Хохлачова, А. Аясрах, А. Аль-Далваш

Національний авіаційний університет,
пр. Любомира Гузара, 1, Київ, 03058, Україна; e-mail: post@nau.edu.ua

В даний час стрімко розвиваються інформаційні технології, динамічно зростаючі обсяги інформації і збільшення її значущості в житті сучасного суспільства і держави в цілому ставить питання інформаційної та кібербезпеки в ряд найбільш актуальних, а проблемам захисту інформації і кіберзахисту приділяється все більша увага, що обумовлює зростаюча кількість публікацій з даної тематики у всьому світі. Практично всі автори так чи інакше вважають проблему надійної і живучої системи захисту інформації найбільш гострою, при цьому сама проблема захисту інформації і кіберзахисту трактується в широкому сенсі - як проблема попередження її спотворення або знищення, несанкціонованої модифікації, зловмисної отримання і використання інформації і т.п . Вплив випадкових факторів на процеси захисту інформації робить практично непридатними методи класичної теорії систем стосовно до вирішення завдань створення, організації та забезпечення функціонування системи захисту. Кількість (і види) впливів і процесів, пов'язаних з несанкціонованим (а можливо і випадковим) доступом до інформації визначити практично неможливо. Одним з найважливіших питань при проектуванні і експлуатації систем захисту інформації є питання забезпечення і оцінки її живучості. У роботі було проведено дослідження, які показали, що критерії ймовірнісної оцінки якості функціонування засобів захисту і оцінки надійності (живучості) системи захисту в цілому можна використовувати. До узагальненому процесу захисту застосовані критерії теорії надійності, що дозволяють в ході проектування і експлуатації систем захисту оперативно оцінювати її надійність (живучість, готовність).

Ключові слова: кібербезпека держави, живучість системи захисту, надійність системи захисту, готовність.

STABILITY OF THE STATE CYBER SECURITY SYSTEM

V.O. Khoroshko, Yu.Ye. Khokhlachova, A. Ayasrah, A. Al-Dalwash

National Aviation University,
1, Lubomyr Guzarv Ave, Kyiv, 03058, Ukraine; e-mail: post@nau.edu.ua

Currently, rapidly developing information technologies, dynamically growing volumes of information and the increase in its importance in the life of modern society and the state as a whole puts the issue of information and cybersecurity among the most urgent, and increasing attention is paid to the problems of information security and cyber protection, which leads to a growing number of publications on this topic all over the world. Almost all authors in one way or another consider the problem of a reliable and tenacious information protection system to be the most acute, while the problem of information protection and cyber protection itself is interpreted in a broad sense - as the problem of preventing its distortion or destruction, unauthorized modification, malicious acquisition and use of information, etc. ... The influence of random factors on information security processes makes the methods of classical systems theory practically unsuitable for solving the problems of creating, organizing and ensuring the functioning of a security system. The number (and types) of impacts and processes associated with unauthorized (and possibly accidental) access to information is almost impossible to determine. One of the most important issues in the design and operation of information security systems is the issue of ensuring and assessing its survivability. In the work, studies were carried out, which showed that the criteria for the probabilistic assessment of the quality of the functioning of protection means and the assessment of the reliability (survivability) of the protection system as a whole can be used. The criteria of the theory of reliability have been applied to the generalized process of protection, which make it possible to quickly assess its reliability (survivability, readiness) during the design and operation of protection systems.

Keywords: state cybersecurity, survivability of the protection system, reliability of the protection system, readiness.