DOI: 10.58168/CISMP2024_60-64
УДК 004.9

ПРИМЕНЕНИЕ СИСТЕМНОГО АНАЛИЗА В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ

А.О. Карташов, Я.А. Кузнецова

ФГБОУ ВО «Воронежский государственный лесотехнический университет имени Г.Ф. Морозова»

Аннотация. В работе рассматриваются основы такого явления, как системный анализ. Понятие кибербезопасности, значение в современном мире. Методы обеспечения безопасности в информационной сфере. В работе упоминаются основные методы применения системного анализа для выявления угроз кибербезопасности.

Ключевые слова: системный анализ, статистика, кибербезопасность.

APPLICATION OF SYSTEM ANALYSIS IN THE FIELD OF CYBERSECURITY.

A.O. Kartashov, Y.A. Kuznetsova

Voronezh State University of Forestry and Technologies named after G.F. Morozov

Abstract. The paper discusses the basics of such a phenomenon as system analysis. The concept of cybersecurity, its importance in the modern world. Methods of ensuring security in the information sphere. The paper mentions the main methods of applying system analysis to identify cybersecurity threats.

Keywords: system analysis, statistics, cybersecurity.

Введение

В настоящее время желание организаций «идти в ногу со временем», не отставать от своих конкурентов, даже элементарно облегчить себе работу ведёт к использованию развивающихся информационных технологий. Безусловно, развитие IT-сферы и распространение интернета способствует ускорению работы во многих отраслях, однако, влечёт за собой ряд опасностей, о которых пользователь даже не задумывается. Кибербезопасность – неотъемлемая составляющая любого процесса разных областей, от мобильного пользования до бизнес-сферы.

Кибербезопасность – сфера деятельности, занимающаяся защитой компьютерных систем, сетей, программ и данных от киберугроз, включая хакерские атаки, вирусы, вредоносное программное обеспечение и другие цифровые угрозы. Понятие «кибербезопасность» следует отличать от информационной безопасности: часто они используются в качестве синонимов,

но на самом деле под кибербезопасностью понимается защита от атак в киберпространстве. А информационная безопасность занимается защитой данных, то есть информации, от любых форм угроз — цифровых или аналоговых. Год за годом в мире становится все больше угроз и происходит все больше утечек данных. Статистика шокирует: для исследования были взяты данные о совершённых и раскрытых интернет-преступлениях в России, результаты представлены на рис. 1.

Рисунок 1 – Рост интернет-преступности в России

Анализируя эти данные, можно прийти к выводу о том, что с конца десятых годов количество зарегистрированных преступлений неуклонно растет. Пиком является 2020 год, это можно связать с тем, что из-за пандемии многие люди перешли на дистанционный тип работы/учебы, что привело к активизации различных мошенников. Учитывая тот факт, что с 2013 по 2019 год число интернет-преступлений выросло в 25 раз, можно с уверенностью заявить, что в дальнейшем ситуация будет только ухудшаться. Такой вывод можно сделать, исходя из данных о расследованных преступлениях. Несмотря на положительную тенденцию, очевидно, что темпы сильно отстают от общего количества правонарушений.

Не утешают и данные об ущербе кибератак по всему миру, статистика представлена на рис. 2.

Рисунок 2 – Общий ущерб кибератак в мире

Как можно заметить, не только Россия сталкивается с данной проблемой. Например, ущерб от кибератак в США, Китае и Европе выше в 38, 37 и 12 раз соответственно. Данная статистика ярко показывает, что проблема кибербезопасности носит общемировой характер, затрагивая многие сферы человеческой деятельности. А с учетом того, что даже страны “третьего” мира активно интегрируются в “цифровое пространство”, можно предположить, что статистика будет расти на постоянной основе.

Но нельзя однозначно заявить, что подвижек к улучшению ситуации нет. Так в настоящее время специалисты из разных стран активно противостоят данному явлению. Для предотвращения и устранения уже произошедших атак разрабатываются огромное количество приёмов и средств. Также появляются способы анализировать потенциальные мошеннические операции, там самым предотвращать их еще до момента совершения. Далее более подробно рассмотрим один из таких способов.

Системный анализ в области кибербезопасности

Системный анализ представляет собой научную дисциплину, изучающую методы, принципы и средства исследования различных объектов. Список сфер для использования не ограничен, но, если говорить конкретно про кибербезопасность, то здесь системный анализ применяется для выяснения причин существующих неполадок, разработки методов их устранения, выявления потенциальных опасностей и предотвращения таковых.

Системный анализ имеет структуру и определённый порядок исполнения задач для достижения результата. Рассмотрим основные шаги, которые

необходимо предпринять при проведении системного анализа угроз кибербезопасности:

1. Определение и анализ проблемы – анализ причин возникновения проблемы, сбор всей информации, которая может быть полезна для установления причинно-следственных связей, в дальнейшем способствующих решению проблемы;
2. Разработка потенциальных решений проблемы – рассмотрение всех возможных выходов из ситуации, оценить плюсы и минусы каждого действия;
3. Оценка источников угроз безопасности информации и возможности реализации способов защиты;
4. Сопоставление возможных угроз и теоретических решений проблемы для выявления недоработок в алгоритме процесса;
5. Реализация сформированного плана решения проблемы, наблюдение его эффективности в течение некоторого времени.

Вывод

Таким образом, можно отметить, что системный анализ в области кибербезопасности является неотъемлемым компонентом. Его инструменты способствуют быстрому обнаружению предпосылок атаки, что в дальнейшем помогает уменьшить масштаб принесённого вреда и ущерба или вовсе предотвратить любые негативные последствия.

Список литературы

1. Русакова О. И., Головань С. А. Анализ кибербезопасности в контексте современных угроз // Управленческий учет. 2022. № 10–2. С. 496–504.
2. Анализ проблем обеспечения информационной безопасности в условиях современного общества / Д. Бразевич [и др.] // Открытый журнал социальных наук. №8, 2020. С. 231-241. DOI: 10.4236/jss.2020.82018.
3. Кокотюха, Э. В. Роль анализа данных в кибербезопасности / Э. В. Кокотюха, Дж. Кларк. // Юный ученый. – 2023. – № 5 (68). – С. 114-117. – URL: https://moluch.ru/young/archive/68/3714/.
4. Полуэктов А.В., Макаренко Ф.В., Ягодкин А.С. Использование сторонних библиотек при написании программ для обработки статистических данных // Моделирование систем и процессов. – 2022. – Т. 15, № 2. – С. 33-41.
5. Модель индивидуально группового назначения доступа к иерархически организованным объектам критических информационных систем с использованием мобильных технологий / Е.А. Рогозин, В.А. Хвостов, В.В. Суханов [и др.] // Моделирование систем и процессов. – 2021. – Т. 14, № 1. – С. 73-79. – DOI: 10.12737/2219-0767-2021-14-1-73-79.
6. Колотушкин, В.В. Моделирование защитных устройств для обеспечения безопасности технологических процессов с использованием взрывоопасных газов / В.В. Колотушкин, С.А. Сазонова, С.Д. Николенко //

Моделирование систем и процессов. – 2021. – Т. 14, № 3. – С. 28-35. – DOI: 10.12737/2219-0767-2021-14-3-28-35.

References

1. Rusakova O. I., Golovan S. A. Analysis of cybersecurity in the context of modern threats // Managerial accounting. 2022. No. 10-2. pp. 496-504.

2. Analysis of the problems of ensuring information security in modern society / D. Brazevich [et al.] // Open Journal of Social Sciences - №8, 2020. - pp.231-241. DOI: 10.4236/jss.2020.82018.

3. Kokotyukha, E. V. The role of data analysis in cybersecurity / E. V. Kokotyukha, Jonathan Clark // Young scientist. – 2023. – № 5 (68). – Pp. 114-117. – URL: https://moluch.ru/young/archive/68/3714/.

4. Poluektov A.V., Makarenko F.V., Yagodkin A.S. The use of third-party libraries when writing programs for processing statistical data // Modeling of systems and processes. – 2022. – Vol. 15, No. 2. – pp. 33-41.

5. Model of individually group assignment of access to hierarchically organized objects of critical information systems using mobile technologies / E.A. Rogozin, V.A. Khvostov, V.V. Sukhanov [et al.]// Modeling of systems and processes. - 2021. – Vol. 14, No. 1. – pp. 73-79. – DOI: 10.12737/2219-0767-2021-14-1-73-79.

6. Kolotushkin, V.V. Modeling of protective devices to ensure the safety of technological processes using explosive gases / V.V. Kolotushkin, S.A. Sazonova, S.D. Nikolenko // Modeling of systems and processes. - 2021. – Vol. 14, No. 3. – pp. 28-35. – DOI: 10.12737/2219-0767-2021-14-3-28-35.