5. *Kozlov A., Noga N.* Applying the Methods of Regression Analysis and Fuzzy Logic for Assessing the Information Security Risk of Complex Systems / Proceedings of the 14th International Conference "Management of Large-Scale System Development" (MLSD). – M.: IEEE, 2021. – URL: https://ieeexplore.ieee.org/document/9600245 (дата обращения 10.10.2022).

DOI: 10.25728/iccss.2022.48.34.023

Абдулова Е.А.

Оценка критической информационной инфраструктуры: киберцели и оценка критичности

Аннотация: В работе рассмотрены кибер-цели и их характеристики, приведено сопоставление целей в физическом и кибер-пространствах и принципы их преобразования, рассмотрены уровни кибер-целей, показана разница в методологических подходах к оценке критичности и риска.

Ключевые слова: критическая информационная инфраструктура, киберсистема, кибер-цели, оценка риска, оценка критичности

Современное общество – это общество, основанное на знаниях, которое в значительной степени полагается на технологии для выполнения или поддержки выполнения задач или функций. В результате современное общество гораздо более уязвимо даже по сравнению с началом века.

Масштабы уязвимости обусловлены тем, что очень много выполняемых операций в какой-то момент поддерживается вводом, хранением и поиском данных и информации во взаимосвязанной сети жестких дисков и серверов данных. Более того, в каждом из этих моментов существует возможность кражи информации, обхода защит, манипулирования или диверсии. При этом не учитывается риск, связанный с непреднамеренными инцидентами, связанными с человеческим фактором, системными сбоями, несовместимостью или другими неожиданными проблемами, а также «стихийными бедствиями». Все больше и больше экспертов по безопасности

заявляют, что защита киберсистем и данных является более серьезной проблемой, чем терроризм, учитывая масштаб угрозы (относительно кибератак) и фактический ущерб, который ежегодно наносится (а также возможные последствия в случае компрометации определенных систем и структур) [1].

Приоритетной целью на сегодняшний день является обеспечение информационной безопасности объектов критической информационной инфраструктуры (КИИ), так и КИИ в целом [2]. Для успешной реализации мероприятий по обеспечению безопасности объектов КИИ и КИИ в целом необходимо решение целого ряда сложных научно-технических задач, из которых задача оценки текущего уровня безопасности объектов КИИ и КИИ в целом и прогнозирования его изменения является одной из ключевых [3].

Оценка критичности, наряду с оценками рисков, критической инфраструктуры, в том числе и КИИ, является важной задачей в комплексе задач по обеспечению защиты критической инфраструктуры. В 2014 году в США была разработана национальная система кибербезопасности, а в основу которой заложен подход, базирующийся на оценке риска, который помогает при столкновении с угрозами кибербезопасности, систематически рассматривать, что они собой представляют (люди, информация, объекты и т. д.), и каковы возможные последствия этих угроз, что можно сделать для устранения этих угроз, как отреагировать на угрозы, и что можно сделать, чтобы обеспечить быстрое восстановление [1].

Кибер-цели в критической инфраструктуре можно оценивать и классифицировать по целевым характеристикам. Каждая цель имеет определенные характеристики, которые составляют основу для обнаружения, определения местоположения, идентификации и классификации цели для последующего наблюдения, анализа, нападения и оценки. Можно выделить четыре категории характеристик, на основе которых можно определить обычные цели: физические, функциональные, когнитивные, экологические [4].

Основными характеристиками цели являются физические особенности: форма, внешний вид, количество и природа элементов, отражательная способность, структурный состав, степень упрочнения, электромагнитное излучение, местоположение, размер и дисперсия. Примером характеристик окружающей среды являются

особенности местности. К когнитивным функциям относятся, например, способ обработки информации целью, информация, которая требуется цели для функционирования, также сюда относятся процессы, которые выполняет цель, количество информации, которую может обрабатывать цель и как цель или система хранит информацию. Функциональные особенности – к ним относятся, например, какие материалы или ресурсы требуются цели для функционирования.

Преобразование физических и экологических характеристик в киберпространство может быть осуществлено путем преобразования их в виртуальные характеристики и функции информационной инфраструктуры. Физические характеристики будут преобразованы в виртуальные характеристики кибер-цели, такие как операционная система, необходимая эффективность процессора, необходимый объем памяти и форматы файлов или данных. Кибер-цель также может иметь интерфейс к физическому пространству, что позволяет злоумышленнику проникнуть в систему кибер-цели через физическое соединение. Характеристики среды будут учитывать характеристики сети, такие как сетевые протоколы, уровни, серверные операционные системы и базы данных, т.е. характеристики информационной инфраструктуры.

Функциональные характеристики учитывают, что выполняет кибер-цель. Например, такими характеристиками могут быть мобильность цели, способность ее защищаться и восстанавливаться. Эти характеристики у кибер- и обычной целей очень похожи. Когнитивные особенности кибер-цели – это, например, способы обработки информации, обработки ввода и вывода и способы хранения информации.

Общие физические и экологические характеристики должны быть преобразованы в виртуальные характеристики, а функциональные и когнитивные характеристики очень похожи в физическом и киберпространствах. Аналогия между физическими и кибер-характеристиками целей показана на рисунке 1.

Кибер-цель может быть разделена на разные категории в зависимости от уровня цели. Высшим уровнем концепции кибер-цели будет система кибер-цели, которая формируется из подсистем и является основной целью атаки. Это может быть, например, SCADA или система управления объектом критической

инфраструктуры. Кибер-целями будут отдельные функции и подсистемы, необходимые для функционирования всей системы.

Рисунок 1 – Аналогия между характеристиками обычных и кибер-целей

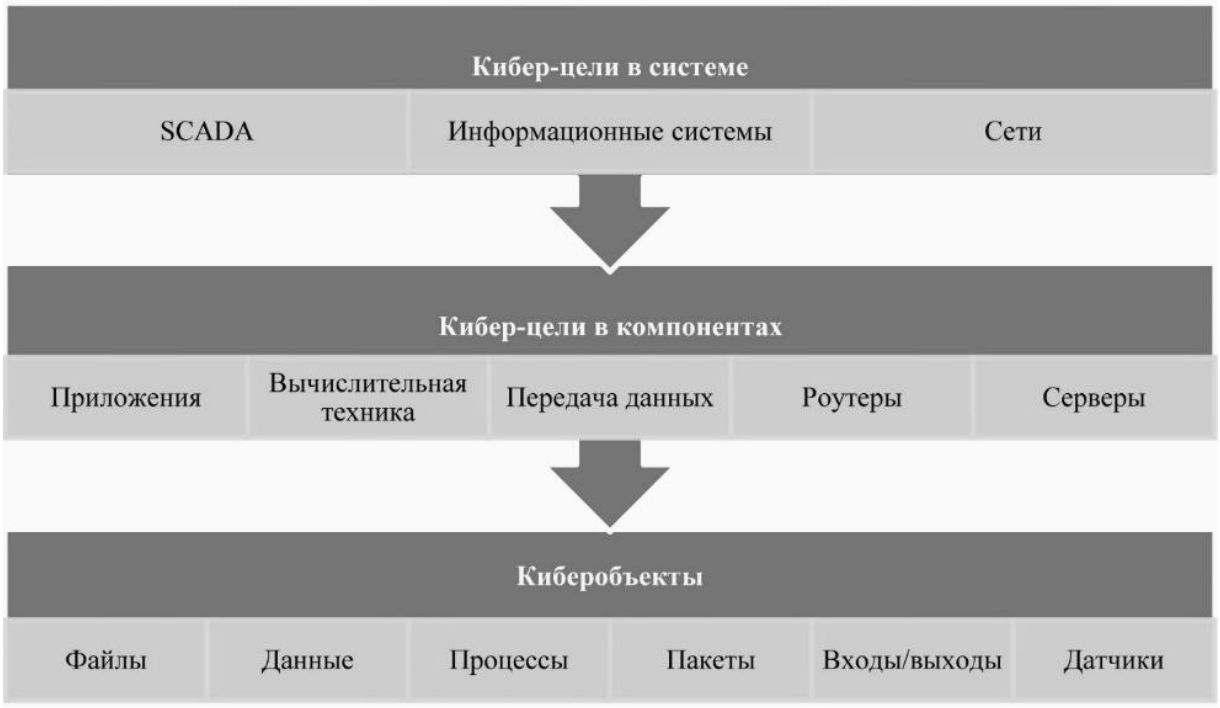

Рисунок 2 – Уровни кибер-целей

Объект кибер-цели — это часть кибер-цели, которая может быть уничтожена по отдельности, но необходима для работы целевой системы. Объектом кибер-цели может быть один процесс, файл, датчик или одна функция. Объекты кибер-цели автономны, соединяются вместе и формируют услугу. Уровни кибер-цели представлены на рисунке 2.

На уровне кибер-целей системы к целям можно отнести SCADA или другие информационные системы, сети и сетевые коммуникации или информационно-телекоммуникационная инфраструктура организаций, содержащая, например, хранилища данных, офисное программное обеспечение и системы обработки сертификатов безопасности. Сложная и распределенная структура этого уровня создает против нее несколько векторов атак.

Кибер-цель в системе также может быть гибридной, существующей как в киберпространстве, так и в физическом пространстве. В такой системе можно оказывать влияние на конечного пользователя через систему, даже если пользователь не существует в киберпространстве или целью может быть физическое устройство.

При оценке критичности критической инфраструктуры, включая КИИ, важно понимать разницу в методологических подходах к оценке критичности и риска (или рискового потенциала [5]). При оценке критичности объекта инфраструктуры в первую очередь учитывают оценку негативного воздействия инфраструктуры на население, общество, окружающую среду, экономику государства, национальную безопасность и т.д. То есть важно оценить ущерб, который был бы вызван, если бы объект перестал функционировать или был бы уничтожен. Вероятность инцидента считается равной единице. При анализе рисков сначала анализируют угрозу активам объекта и оценивают ущерб, который будет нанесен самому объекту. В этом принципиальное различие между подходами к оценке критичности и оценке риска.

Основными критериями, возникающими при оценке критичности объекта критической инфраструктуры, являются: воздействие на общество; экономический эффект; воздействие на окружающую среду; политическое влияние; влияние на национальную безопасность; оценка взаимозависимости, т.е. влияния на функционирование другой критической

инфраструктуры. При оценке также учитываются: масштаб воздействия (каскадные эффекты, географический масштаб и др.), временные характеристики – скорость проявления негативного воздействия, продолжительность воздействия, время восстановления безопасного состояния. Общий уровень критичности оценивается на основе анализа обобщенной нормативной оценки (сумма всех баллов по всем критериям) с последующим применением универсальной шкалы Харингтона [6].

Литература:

1. *Bullock J.A., Haddow G.D., Coppola D.P.* Cybersecurity and critical infrastructure protection (in book Introduction to Homeland Security Principles of All-Hazards Risk Management). – Elsevier, 2021. – P. 425-497

2. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

3. *Калашников А.О.* Управление информационными рисками организационных систем: механизмы комплексного оценивания // Информация и безопасность. – 2016. – Т. 19. № 3. – С. 315-322.

4. Air Force Doctrine Publication 3-60, Targeting, U.S. Air Force, 2021. – URL: https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-60/3-60-AFDP-TARGETING.pdf (дата обращения 25.10.2022).

5. *Абдулова Е.А., Калашников А.О.* К вопросу управления рисками критической информационной инфраструктуры / Труды 14-й Международной конференции «Управление развитием крупномасштабных систем» (MLSD-2021). – М.: ИПУ РАН, 2021. – С. 1275-1282.

6. *Harrington E.C.* The Desirability Function // Industrial Quality Control. – 1965. – Vol. 21. № 10. – P. 494-498.