Биологическая метафора кибер-иммунитета

Н. М. Григорьева[1], С. А. Петренко[2]
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
[1]Nataliegrigoreva.8@gmail.com, [2]S.Petrenko@rambler.ru

***Аннотация*. Иммунная система человека состоит из специфических слоев защиты организма, существенной особенностью которых является распознавание всех входящих объектов как «собственный» или «чужеродный» и уничтожение последних. Все биологические клетки, принадлежащие нашему организму, сохраняются в «памяти» иммунной системы как «собственные» сущности и помечаются как «занесенные в белый список». Этот тип объектов предоставляет специальные белковые маркеры в качестве инструмента их идентификации. Другие объекты, которые не могут предоставить свой белковый маркер, помечаются как «чужеродные» и будут уничтожены иммунной системой в дальнейшем. Принцип работы иммунитета помог определить биологическую метафору, которая может быть применена к сфере кибербезопасности путем присвоения «иммунной памяти» реакций на как известные, так и неизвестные ранее кибератаки.**

Ключевые слова: биологическая метафора; кибер-иммунитет; кибербезопасность

I. Вступление

В этом разделе кратко рассматриваются основные предпосылки для создания необходимых аппаратно-программных систем иммунной защиты грядущей Индустрии 4.0. Исключительная важность иммунитета живого организма объясняется его уникальной способностью справляться со вспышками новых или возвращающихся инфекций. Изучение «врожденного» и «приобретенного» иммунитета живого организма помогло определить и обосновать соответствующую биологическую метафору киберуязвимости для адекватной защиты критической информационной инфраструктуры Индустрии 4.0 перед лицом растущих угроз информационной безопасности. Понимание ключевых принципов и механизмов иммунной защиты привело к разработке соответствующей концепции киберуязвимости Индустрии 4.0.

II. Биологический аспект

Ф. Бернет разработал теорию клонального размножения классической и математической иммунологии, результаты которой были дополнены Н. Джерном, Дж. Ледербергом и Д. Талмедж [1–3]. Они определили, что иммунная система на молекулярном уровне распознает и пытается уничтожить клетки под названием антиген, которые опасны для организма. Проще говоря, он распознает генетически чужеродный или измененный материал (например, раковые опухоли). Реализация этой функции достигается путем создания клонов иммунных клеток, «настроенных» на обнаружение специфического антигена. В организме существуют группы различных клонов, которые помогают распознавать большинство возможных антигенов, исключая свои собственные (иначе организм попытается атаковать сам себя).

Основные принципы иммунной системы включают в себя состав двух тесно взаимодействующих систем – врожденного и адаптивного иммунитета. Врожденная иммунная система – это неотъемлемая существующая система, которая быстро уничтожает микробы. Макрофаги, гранулоциты, естественные клетки-киллеры и дендритные клетки являются первичными клетками врожденной иммунной системы, которые обеспечивают так называемые рецепторы распознавания образов (PRRs) на поверхности специализированных иммунных клеток врожденного иммунитета, описанных выше, а также почти во всех клетках организма. После того, как патоген идентифицирован, врожденные иммунные клетки пытаются уничтожить его. Этот процесс можно назвать первым уровнем защиты, если же он не справляется со своей работой, то уже начинает действовать адаптивная система [4–5].

Адаптивный иммунитет часто опирается в своем развитии на базовые основы врожденного иммунитета, поскольку клетки врожденного иммунитета действуют как носители информации для клеток адаптивного иммунитета. Адаптивный иммунитет далее можно разделить на гуморальные и клеточные реакции. Гуморальный ответ может быть описан активацией В-лимфоцитов с последующим созреванием в плазматических клетках и выработкой антител, тогда как клеточный иммунный ответ характеризуется трансформацией Т-лимфоцитов в Т-киллеры – клетки, способные убивать инфицированные вирусом клетки [6–8].

Рис. 1. Виды иммунитета живого организма [8]

III. Применимость процесса иммунной защиты в области кибербезопасности

Количество и серьезность угроз кибербезопасности возрастают с каждым годом, и критическая информационная инфраструктура требует надежной

защиты [9–10]. Критическая информационная инфраструктура требует обеспечения высокого уровня ее защиты. Таким образом, возникла необходимость определить концепцию систем кибер-иммунитета, которая имеет некоторые общие моменты с теорией биологического иммунитета, и обогатилась результатами научных и прикладных разделов биологической и кибернетической иммунологии.

Кибератаки и биологические атаки имеют много общего: в обоих случаях противник усложняет свои средства нападения и постепенно эволюционирует, усложняет и постепенно меняет свои средства нападения. Однако иммунная система способна отличать свои клетки от чужеродных, что делает ее настолько сильной, что мы зачастую даже не осознаем возможную угрозу.

Очевидно, что биологическая иммунная система работает. Так почему бы не расширить данную метафору немного дальше и не создать кибер-иммунную систему для защиты нашего цифрового пространства? [8]

По данным исследователей ИБ компании Kaspersky [9] только в период конца 2021 г по 2022 г. количество успешных хакерских атак на предприятия превысило 500 в месяц. Новая политика хакеров по получению требуемого выкупа изменилась и теперь часто предусматривает выставление украденных данных или раскрытие существующих уязвимостей в системе защиты компании на аукцион, где случаются ситуации, когда итоговая ставка превышает изначально запрашиваемую. Такая тенденция выгодна злоумышленникам, так как если им не заплатит пострадавшая компания, это сделают другие заинтересованные лица, которые получат доступ к конфиденциальной информации. В первой половине 2023 г. рост кибератак на предприятия только продолжился и нет практически никаких шансов, что ситуация изменится в противоположную сторону. Год от года хакеры только совершенствуют свои навыки и инструменты, и часто способны оказываться впереди существующих средств защиты.

Существующие в настоящее время подходы к кибербезопасности, такие как брандмауэры, становятся устаревшими и не могут обеспечить требуемый уровень защиты, особенно от атак нулевого дня, APT-групп и инсайдерских злоумышленников с возможностями доступа к получению высоких привилегий. Но система кибериммунной безопасности может помочь решить эти проблемы путем подготовки и выполнения программ «иммунного ответа», как это происходит с врожденным и адаптивным иммунитетом в биологическом организме. Эта система может быть построена с использованием технологий искусственного интеллекта, поэтому она будет пытаться извлечь конкретные особенности или паттерны в поведении каждого пользователя или устройства, собирая весь поток информации для изучения нормального и ненормального “поведения” пользователя или устройства.

В обозначаемой кибериммунной теории деструктивный программный код играет роль его биологический прототип – антиген, программа нейтрализации этого кода является клетка-антитело из живого организма. Модель иммунной защиты описывает причинно-следственные связи между антителами и антигенами. Система, основанная на описанных принципах, состоит из трех ключевых частей: распознавателя, планировщика и исполнителя. Основная цель распознавателя – обнаруживать вредоносные паттерны по их специфическим признакам (структурным, корреляционным и т. д.). Планировщик предназначен для составления расписания метапрограмм для нейтрализации возможных вредоносных программ. Наконец, исполнитель предназначен для запуска программ из планировщика. Результатом работы этих трех подсистем является достижение требуемой очистки и формирование доверенной среды для вычислений в условиях различных кибератак. Выполнение программ нейтрализации не предполагает физического уничтожения вредоносных программ, как это происходит в биологической среде, в противном же случае это приведет к неприемлемым последствиям, поскольку потеря части функционального программного кода может привести к отказу в обслуживании и невозможности продолжения вычислений. Напротив, система пытается просто восстановить безопасность этого кода, не теряя его функциональности [10].

Подобно тому, как биологическое тело имеет какой-то порог для иммунной реакции, средства защиты, основанные на кибер-иммунитете, имеют ту же конструкцию, чтобы предотвратить большое количество ложноположительных шумовых примеров. Когда степень полученной травмы достигает определенного уровня серьезности, иммунная система активирует каскады молекулярных сигналов, которые привлекают специализированные иммунные клетки – «Т-клетки-киллеры» – к месту повреждения и устраняют любую потенциальную инфекцию. Киберверсия такой системы работает немного по-другому: чтобы узнать, что является нормальным, она отслеживает обычные события, чтобы извлечь шаблоны нормального поведения, прежде чем будет готова обнаружить подозрительное. Другой тип обучения может включать в себя установку «honeypot» для заманивания злоумышленников в ловушку, чтобы также наблюдать за их поведением.

Тем не менее, система не идеальна. И отчасти это связано с врожденными недостатками биологической иммунной системы, на которой она была основана. Аутоиммунитет очевиден – в некоторых случаях инфекционный агент настолько похож на компоненты нашего собственного организма, что иммунная система теряет способность отличать себя от других. Вместо этого, нанося свои жестокие удары, он непреднамеренно повреждает и наши собственные органы [11].

IV. Принципы развития систем обнаружения вторжений на основе иммунного ответа

На сегодняшний день системы обнаружения вторжений работают обычно на основе одного из следующих методов или в их комбинации: обнаружение сигнатур, корреляций или инвариантов. Подход на основе поиска известных сигнатур представляют собой строгую модель, точно определяющую тип входных данных: корректный или вредоносный, на основе заведомо составленного словаря с сигнатурами известных вирусов. Очевидный недостаток такой системы в том, что все иные варианты воздействий неизвестные на момент создания или обновления модели не анализируются и приводят к ошибкам I-го или II-го

рода (в зависимости, от настройки системы). Корреляционный подход является более продвинутой системой обнаружения атак и выполняет свою работу, анализируя уже не одно событие или файл, а некую последовательность действий, которая может быть отнесена к классам корректного, вредоносного и/или аномального воздействия с некоторой долей вероятности. Такая система, очевидно, более гибкая в вопросе покрытия множества ранее неизвестных воздействий, однако, степень достоверности принятых ею решений может быть невысокой. Наконец, инвариантный подход состоит в поиске всех возможных корректных состояний объекта и минимизации доли зловредных воздействий. Достигается такой подход путем накладывания на все пространство допустимых значений вектора систем ограничений, подобранных соответствующим образом. Данный метод минимизирует возникновение ошибок I-го и II-го рода и способен достаточно качественно выявлять ранее неизвестные типы атак.

В качестве упомянутых ранее основных терминов классической иммунологии: антигена и антитела, в системах обнаружения вторжений могут выступать: деструктивный программный код/нелигитимные системные вызовы и др. подозрительные действия, как антитела, а также база упорядоченных паттернов из структурных, корреляционных и инвариантных признаков, как антигены. Наряду с классическими алгоритмами, реализующими данный подход, существуют методы, учитывающие процедуру мутации, как, например, в работах [12–14]. Программная реализация таких алгоритмов представляет собой обычно наличие модуля генерации обучающей выборки антигенов и выработки на их основе детекторов или сигнатур, а также модуля анализа полученных на вход антигенов и соответствующих детекторов. Входные антигены могут подвергаться различным модификациям или мутациям, которые алгоритм поиска детекторов «учиться» распознавать.

Итак, алгоритмы обнаружения аномалий и вредоносного кода Индустрии 4.0 работают следующим образом:

1. Сперва запускается проверка на обнаружение в критических приложениях вредоносных программных закладок и возможных аномалий работы.
2. При обнаружении известных уязвимостей активируется заранее созданный «врожденный» кибериммунитет.
3. При обнаружении неизвестных заранее деструктивных воздействий запускается подготовка и настройка другого вида иммунитета – «приобретенного», для которого проводится статический и динамический анализ исполняемого кода и постоянно пополняются базы данных новыми наборами различных паттернов.
4. Для уменьшения возможного негативного эффекта переобучения детекторов применяют линеризацию или исключение примеров, встречающихся слишком редко или слишком часто, отчего они не несут важной информации, необходимой для тренировки системы в целом.

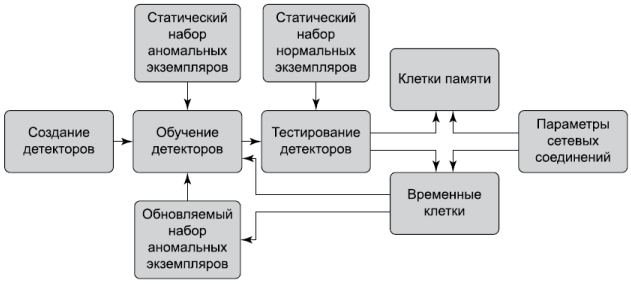

Рис. 2. Жизненный цикл иммунного детектора [7]

Исторически первым, кто разработал строгий подход к моделированию искусственных иммунных систем, был Н. Ерне, чьи работы положили начало развития математического аппарата математического моделирования в иммунологии, путем описания динамики воспроизведения иммунных клеток и белков иммунной системы с помощью дифференциальных уравнений [15–16]. Далее был предложен метод «отрицательного отбора», при котором генерируются наборы детекторов, не совпадающие ни с одним из антител. Генерация начинается со случайного набора, который в дальнейшем постепенно лишается тех клеток, которые реагируют на свои антитела. Позднее были добавлены операции «клонирования» и «мутации» вредоносных примеров [17]. В работах [18–19] А.О. Тараканов предоставил математический базис такого понятия, как иммунокомпьютинг, который, благодаря реализации вычислений на основе математических абстракций молекул белков и иммунных сетей, позволяет избавиться от недостатков искусственных (нейронных) иммунных сетей. Главным отличием нейрокомпьютинга от других видов вычислений является построение функций базовых элементов на основе их биологических прототипов, например, нейроны или, лучше сказать, формальные пептиды в данных сетях имеют не жестко заданные связи с другими нейронами, а свободные, строящиеся в зависимости от их состояний. Для эффективного выполнения таких вычислений требуется разработка специальных иммуночипов, позволяющих проводить множество исследований одновременно. Такие биочипы меньше по размеру, чем традиционные, и очень чувствительны даже к малому количеству проб.

В настоящее время для решения задачи обнаружения вредоносного кода могут применяться гибридные методы поиска аномалий, такие как, иммунные, генетические, нейронные, нечеткие и пр. подходы [20–22].

V. Заключение

Количество и изощренность атак в киберпространстве растут из года в год, и ожидается, что этот процесс будет продолжаться, в то время как некоторые из существующих средств защиты остаются устаревшими [23–24]. В подавляющем большинстве случаев текущая стратегия заключается в выявлении угроз, а затем в возведении прочных защитных стен, направленных на предотвращение проникновения вредоносного программного обеспечения или агентов [25–27]. Однако эта стратегия неэффективна в ситуациях, когда хакеры получают доступ к внутренней области. Без каких-либо средств отслеживания хакеров, когда они проникают внутрь систем, современные

средства защиты не в состоянии поднять тревогу, пока не станет слишком поздно. Подход, основанный на применении некоторой биологической метафоры для построения системы киберуязвимости, может дать возможность построить другой метод в области киберзащиты.

СПИСОК ЛИТЕРАТУРЫ

[1] Burnet F.M. (1957). A modification of Jerne's theory of antibody production using the concept of clonal selection. Australian Journal Science, 20 (2):67–69. Reprinted in Burnet FM (1976).

[2] Jerne N.K. (1984). Nobel lecture: The Generative Grammar of the Immune System (PDF), Nobelprize.org, retrieved 8 July 2019.

[3] Lederberg J. (1959). "Genes and antibodies". Science, 129 (3364):1649–1653.

[4] Mechnikov I.I. M. Immunity in infectious diseases, 1903; Immunity in Infectious Diseases. M. Mndgiz, 1953. 519 p. – (Academic Collected Works / Edited by N. N. Zhukov-Verezhnikov; Academic Medical Sciences of the USSR; T. 8). (in French, 1901).

[5] Mechnikov I.I. (1913). Studies on the nature of man / 4th ed. M., 1913 (in French, 1903)

[6] Diercks G.F.H., Kluin P.M. (2016). Basic Principles of the Immune System and Autoimmunity. In: Jonkman, M. (eds) Autoimmune Bullous Diseases. Springer, Cham. https://doi.org/10.1007/978-3-319-23754-1_1

[7] Sergei Petrenko "1 Cyber Immunity Concept of the Industry 4.0," in Developing a Cybersecurity Immune System for Industry 4.0, River Publishers, 2020, pp.27-100.] https://doi.org/10.1201/9781003337874]

[8] Immunology Overview: How Does Our Immune System Protect Us? Available at: https://blog.cellsignal.com/immunology-overview-how-does-our-immune-system-protect-us (accessed 4 April 2023)

[9] Enterprise threats in 2023: media blackmail, fake data leaks, and more attacks via clouds. Available at: https://www.kaspersky.com/about/press-releases/2023_enterprise-threats-in-2023-media-blackmail-fake-data-leaks-and-more-attacks-via-clouds (accessed 1 April 2023)

[10] ATT&CK Matrix for Enterprise. Available at https://attack.mitre.org/ (accessed 3 April 2023)

[11] Artificial Immune Systems May Be the Future of Cybersecurity. Available at: https://medium.com/singularityu/artificial-immune-systems-may-be-the-future-of-cybersecurity-493403f54013 (accessed 4 April 2023)

[12] Petrenko S.A., Petrenko A.S. Super-productive monitoring centers for security threats, Part 1, Protection of information. Inside, No. 2 (74), pp. 29м36, Russia, 2017.

[13] Grossman E. What did mathematical models contribute to AIDS research? (book review) // Trends in Ecology & Evolution. 2001. V. 16, № 8. P. 466–467

[14] Nowak M,, May R., Anderson R. The evolutionary dynamics of HIV-1 quasispecies and the development of immunodeficiency disease// AIDS. 1990. no. 4. P. 1095–1103.

[15] Vorobiev, E. G., Petrenko, S. A., Kovaleva, I. V., Abrosimov, I. K. Organization of the entrusted calculations in crucial objects of informatization under uncertainty, In Proceedings of the 20th IEEE International Conference on Soft Computing and Measurements (24–26 May 2017). SCM, pp 299–300. DOI: 10.1109/SCM.2017.7970566, St. Petersburg, Russia, 2017.],

[16] [Кузнецов С.Р. Математическая модель иммунного ответа. Вестник СПбГУ. Сер. 10. 2015. Вып. 4. 16 с.

[17] Barabanov A.V., Markov A.S., Tsirlov V.L. Information Security Controls Against Cross-Site Request Forgery Attacks On Software Application of Automated Systems. Journal of Physics: Conference Series. 2018. V. 1015. P. 042034.

[18] Dasgupta D., Nino L. F. Immunological Computation: Theory and Applications. Boca Ration: CRC Press, 2008. 298 p.

[19] Тараканов А.О. Формальные иммунные сети: математическая теория и технология искусственного интеллекта // Теоретические основы и прикладные задачи интеллектульных информационных технологий.

[20] Tarakanov A.O. Information security with formal immune networks // Information Assurance in Computer Networks (eds. Gorodetsky V.I., Skormin V.A., Popyack L.J.). Berlin: Springer-Verlag, 2001. pp. 115–126.

[21] Ostaszewski M., Seredynski F. et al, Coevolutionary-based mechanisms for network anomaly detection. Journal of Mathematical Modelling and Algorithms. 2007. Vol. 6, pp. 411–431.

[22] Aziz A. S.A., Salama M.A. et al, Genetic algorithm with different feature selection techniques for anomaly detectors generation. // Proceedings of the 2013 Federated Conference on Computer Science and Information Systems. 2013. pp. 769–774.

[23] Федорченко А.В., Чечулин А.А., Котенко И.В. Исследование открытых баз уязвимостей и оценка возможности их применения в системах анализа защищенности компьютерных сетей. // «Информационно-управляющие системы», 2014, no. 5, с. 72–79.

[24] Dorofeev A.V., Markov A.S. Conducting Cyber Exercises Based on the Information Security Threat Model. CEUR Workshop Proceedings, 2021, vol. 3057, pp. 1–10.

[25] Petrenko A., Petrenko S. Basic Algorithms Quantum Cryptanalysis. // Вопросы кибербезопасности. 2022. № 1(53), pp. 100-115. DOI: 10.21681/2311-3456-2023-1-100-115

[26] Petrenko S. Cyber Resilient Platform for Internet of Things (IIoT/IoT)ed Systems: Survey of Architecture Patterns. // Вопросы кибербезопасности. 2021, no. 2 (42), pp. 81-91. DOI: 10.21681/2311-3456-2021-2-81-91.

[27] Petrenko S. Self-Healing Cloud Computing. // Вопросы кибербезопасности. 2021, no. 1 (41), pp. 80-89. DOI: 10.21681/2311-3456-2021-1-80-89.