УДК 004.056.5

# Цифровой иммунитет как стратегический подход к обеспечению кибербезопасности устройств и технологий на всех этапах их жизненного цикла

**Маурина Мария Юрьевна** mashmar2006@mail.ru
**Маслова Татьяна Ивановна**(*) mas.tatiana2009@yandex.ru
SPIN-код: 7110-3851

*МГТУ им. Н.Э. Баумана, Москва, Россия*

***Аннотация.*** *Рассмотрено понятие цифровой иммунной системы и ее сравнение с иммунной системой человека. Показано различие между традиционными методами обеспечения информационной безопасности и стратегиями построения цифрового иммунитета. Определена основная задача цифрового иммунитета и перечислены его составляющие. Прослежены этапы жизненного цикла цифровых устройств и технологий. Отмечены направления деятельности по обеспечению кибербезопасности на всех этапах жизненного цикла устройств и технологий. Указаны ресурсы и условия, необходимые для успешного внедрения цифрового иммунитета на предприятии. Рассмотрен комплексный подход к кибербезопасности, основанный на принципах философии Сунь-Цзы.*

***Ключевые слова:*** *цифровая иммунная система, цифровой иммунитет, кибербезопасность, жизненный цикл устройства, жизненный цикл технологии*

# Digital immunity as a strategic approach to ensuring the cybersecurity of devices and technologies at all stages of their life cycle

**Maurina Maria Yurievna** mashmar2006@mail.ru
**Maslova Tatyana Ivanovna**(*) mas.tatiana2009@yandex.ru
SPIN-code: 7110-3851

*BMSTU, Moscow, Russia*

***Abstract.*** *The concept of the digital immune system and its comparison with the human immune system are considered. The difference between traditional methods of information security and strategies for building digital immunity is shown. The main task of digital immunity is defined and its components are listed. The stages of the life cycle of digital devices and technologies are traced. Areas of activity to ensure cybersecurity at all stages of the life cycle of devices and technologies are noted. The resources and conditions necessary for the successful implementation of digital immunity at the enterprise are indicated. An integrated approach to cybersecurity based on the principles of Sun Tzu's philosophy is considered.*

***Keywords:*** *digital immune system, digital immunity, cybersecurity, device lifecycle, technology lifecycle*

**Введение.** В XXI веке с ростом цифровых технологий увеличилось и количество угроз, направленных на уничтожение, повреждение и кражу данных. Вопрос защиты информации приобретает особую актуальность. Тема цифровой безопасности с каждым годом все шире рассматривается в научном сообществе. Эксперты в этой области делятся своими знаниями и практическими решениями. Однако вопрос обеспечения кибербезопасности цифровых устройств и технологий на всех этапах их жизненного цикла не был рассмотрен учеными. Поэтому целью нашей работы является формирование нового подхода к вопросу кибербезопасности устройств и технологий на всех этапах их жизненного цикла. Для выполнения этой цели поставлены задачи: рассмотреть концепцию цифровой иммунной системы и ее компоненты; отметить направления деятельности по обеспечению кибербезопасности на всех этапах жизненного цикла устройств и технологий.

**Материалы и методы.** В исследовании будем применять метод аналогии. Цифровая иммунная система (DIS) работает по принципу иммунной системы человека [1, 2]. Цифровая иммунная система по аналогии с иммунной системой организма постоянно проверяет цифровую среду организации на наличие новых угроз, анализирует предыдущие атаки и адаптируется для предотвращения будущих взломов. Цифровой иммунитет обеспечивает устойчивость информационных систем, технологий и ресурсов к атакам так же, как иммунная система человека защищает его от болезней.

Мы используем метод аналогии, применяя к современным технологиям тысячелетнее воинское искусство предупреждения атак. Как говорил китайский философ Сунь-Цзы: «Лучший способ выиграть сражение — избежать его». Цифровой иммунитет работает по тому же принципу — он помогает предупредить атаки злоумышленников и нейтрализовать их с минимальными потерями, а значит — победить в битве, не вступив в сражение [3].

**Результаты.** Проведя теоретическое исследование научно-методической литературы, авторы пришли к выводу, что цифровая иммунная система представляет собой совокупность различных методов, процессов, технологий проектирования программного обеспечения, разработки, эксплуатации и аналитики, которые совместно работают для защиты систем и данных от кибератак, сбоев и других вредоносных воздействий [2, 4]. Это не отдельная технология, а комплексный подход, интегрирующий различные практики и технологии на протяжении всего жизненного цикла разработки программного обеспечения, от проектирования до эксплуатации.

Цифровой иммунитет — это «комплексная стратегия, аналогичная подготовке армии, где каждое устройство, компонент и технология становится солдатом, каждое правило — частью тактики, а каждое действие — шагом к победе. «Без подготовки победа невозможна», говорил Сунь-Цзы, и в кибербезопасности это выражается в продуманном выборе технологий и их правильном использовании» [3].

Традиционные методы обеспечения информационной безопасности отличаются от стратегий построения цифрового иммунитета тем, что традици-

онные методы работают в режиме реагирования на киберугрозы. А стратегия построения цифрового иммунитета использует проактивный подход, который предполагает предугадывание действий злоумышленников и защиту от возможных действий еще до их начала [4].

Основная задача цифрового иммунитета заключается в создании устойчивой и адаптивной среды, которая может самостоятельно реагировать на возникающие угрозы и восстанавливаться после инцидентов, при этом поддерживая высокий уровень безопасности и производительности [1]. Ключевая сила цифрового иммунитета — это «способность не только проактивно защищать системы от угроз, но и автоматически восстанавливаться после атак» [4]. Составляющими цифрового иммунитета являются система проактивного управления рисками для их обнаружения, реагирования и устранения вредных последствий, а также стратегия безопасности, предполагающая использование современных средств защиты, повсеместное повышение осведомленности об угрозах и обучение персонала [1].

Успешной реализации цифрового иммунитета на предприятии будут способствовать следующие условия и ресурсы:

– инфраструктурная поддержка (трафик, логи-файлы, камеры наблюдения);

– мощные вычислительные ресурсы для работы алгоритмов машинного обучения в реальном времени;

– специалисты по искусственному интеллекту, машинному обучению и кибербезопасности;

– интеграция с другими системами (SIEM, DLP, IDS) для координации между различными модулями безопасности;

– гибкость и адаптивность для быстрых изменений в жизненном цикле любого бизнеса [1].

**Обсуждение полученных результатов.** Цифровой иммунитет должен распространяться как на отдельные устройства, так и на информационные системы, технологии, где нужна комплексная информационная безопасность. В цифровой экосистеме каждое устройство и технология на всех этапах их жизненного цикла должны быть защищены. Цифровой иммунитет требует постоянной интеграции защитных мер на всех этапах планирования, создания, использования и обновления технологий [3].

Жизненный цикл мобильных устройств включает в себя следующие этапы: приобретение, развертывание, обслуживание и утилизацию. Защита данных на мобильных устройствах является постоянной проблемой в течение их жизненного цикла.

На этапе приобретения необходимо выработать комплексную политику безопасности устройства. В процессе регистрации применяются политики управления устройствами компании. Политики обеспечивают защиту устройств сотрудников и данных компании от несанкционированного доступа. На этапе развертывания обеспечивается готовность устройств к использованию с необходимыми приложениями при сохранении протоколов безопасности.

Техническое обслуживание на протяжении всего срока службы устройства включает в себя обновления программного обеспечения и приложений, удаленные обновления безопасности как для ОС, так и для приложений. Шифрование и возможности удаленного стирания необходимы для предотвращения нарушений. Регулярные проверки и мониторинг безопасности необходимы для обнаружения и устранения потенциальных угроз.

Этап вывода устройства из эксплуатации включает в себя безопасное удаление данных во избежание несанкционированного доступа и экологически ответственную утилизацию. Надлежащая документация и отслеживание утилизированных устройств необходимы для предотвращения утечки данных и юридических проблем [5].

Жизненный цикл технологии представляет собой совокупность последовательно сменяющих друг друга различных этапов инновационного процесса. Этапы жизненного цикла технологий можно сгруппировать в четыре фазы, выражающие логику технологической динамики нововведения:

– первая фаза (зарождение) включает этапы: идеи, воплощения, обоснования;

– вторая фаза (освоение) содержит этапы: сопоставления, испытания и внедрения;

– третья фаза (диффузия) объединяет этапы: адаптации, модификации и распространения;

– четвертая фаза (старение) включает этапы: этапы зрелости, насыщения и замещения [6].

По-иному жизненный цикл технологий можно разделить на этапы исследования и разработки, подъема (развития и распространения), зрелости (массового применения) и заката (упадка и вытеснения новыми технологиями).

Для реализации цифрового иммунитета на первой фазе жизненного цикла технологий необходимо выбрать систему безопасности для интеллектуальной защиты и самовосстановления (Kaspersky Cyber Immunity, Microsoft Azure Sentinel, IBM Resilient (SOAR), IBM Watson for Security Watson) [4, 7, 8].

На второй фазе жизненного цикла технологий необходимо обучить сотрудников новым методам работы с DIS-системами:

– Microsoft Defender for Endpoint использует сценарии имитации угроз для обучения правильным действиям в условиях кибератак. Система может автоматически отправить обучающее уведомление с рекомендациями по безопасным действиям;

– Microsoft Secure Score предоставляет оценку уровня безопасности и предполагает рекомендации и учебные материалы для повышения безопасности;

– KnowBe4 и Cofense. Эти популярные платформы специализируются на обучении сотрудников реагированию на угрозы, включая моделирование сценариев атаки [4].

На третьей фазе жизненного цикла технологий после внедрения DIS необходимо регулярно обновлять механизмы и алгоритмы искусственного

интеллекта и машинного обучения, чтобы они могли адаптироваться к новым видам угроз [4].

На четвертой фазе жизненного цикла технологий, когда предпринимаются попытки принципиально новых усовершенствований технологии, дающих начало новым идеям, по-прежнему необходим постоянный мониторинг, регулярные тренинги для сотрудников и актуализация всех политик безопасности. На этой фазе, когда прежнее нововведение покидает производственный процесс, необходимо безопасно архивировать все данные технологии.

Основными элементами политики безопасности данных на всех этапах жизненного цикла технологий являются:

– четкое общение или ясная коммуникация (регулярные напоминания, информационные бюллетени);

– обучение и осведомленность сотрудников (учебные программы должны охватывать спектр тем от основ гигиены паролей до выявления попыток фишинга и распознавания тактик социальной инженерии);

– определение политики приемлемого использования, описывающей допустимые и недопустимые действия, связанные с обработкой данных, обеспечивая основу для ответственного и безопасного использования ресурсов организации [9].

**Заключение.** Таким образом, по аналогии с иммунной системой человека, цифровая иммунная система призвана обеспечить кибербезопасность различных устройств и технологий на всех этапах их жизненного цикла. Цифровой иммунитет гарантирует устойчивость информационных систем и информационных ресурсов к различным атакам. Ключевая сила цифрового иммунитета — это способность предугадывать действия злоумышленников, защищать системы от угроз еще до их начала, автоматически восстанавливаться после кибератак. В данном исследовании нами прослежены этапы жизненного цикла цифровых устройств и технологий и отмечены направления деятельности по обеспечению кибербезопасности на всех этапах их жизненного цикла.

## Список источников

[1] *Выживут защищенные: как укрепить цифровой иммунитет компании в ИТ.* URL: https://www.computerra.ru/302893/vyzhivut-zashhishhennye-kak-ukrepit-tsifrovoj-immunitet-kompanii-v-it/ (дата обращения 26.08.2025).

[2] *Как укрепить цифровой иммунитет компании в ИТ.* URL: https://tomhunter.ru/press-center/press-releases/kak-ukrepit-czifrovoj-immunitet-kompanii-v-it.html (дата обращения 26.08.2025).

[3] *Кибербезопасность в стиле Сунь-Цзы: защищаемся от угроз по заветам китайского стратега.* URL: https://habr.com/ru/companies/ncloudtech/articles/860302/ (дата обращения 26.08.2025).

[4] Шустиков А.В. *Цифровой иммунитет: защита от киберугроз: практическое руководство по кибергигиене и устойчивости систем для специалистов по ИБ.* Москва, Эксмо, 2025, 320 с.

[5] *Управление жизненным циклом мобильных устройств (MDLM): полное руководство по контролю устройств.* URL: https://blog.scalefusion.com/ru/mobile-device-lifecycle-management/ (дата обращения 26.08.2025).

[6] *Жизненный цикл технологии.* URL: https://bigenc.ru/c/zhiznennyi-tsikl-tekhnologii-ce9387 (дата обращения 26.08.2025).

[7] *От кибербезопасности — к цифровому иммунитету: куда движется отрасль.* URL: https://cipr.ru/news/ot-kiberbezopasnosti-k-czifrovomu-immunitetu-kuda-dvizhetsya-otrasl/ (дата обращения 26.08.2025).

[8] *Understanding the digital immune system in cybersecurity.* URL: https://digitaldigest.com/digital-immune-system/ (дата обращения 26.08.2025).

[9] *Политика безопасности данных для сотрудников: поведенческий разрыв.* URL: https://blog.scalefusion.com/ru/политика-безопасности-данных-для-сотрудников/ (дата обращения 26.08.2025).