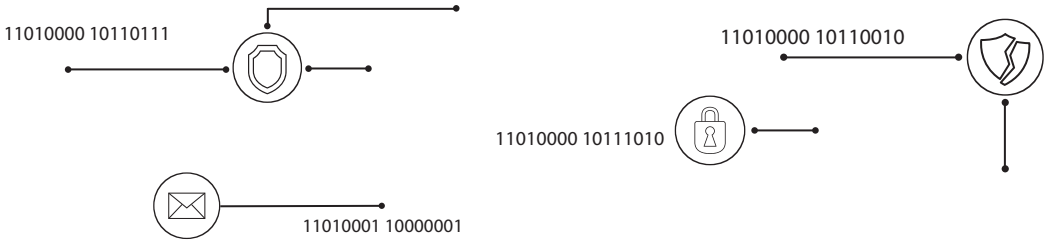
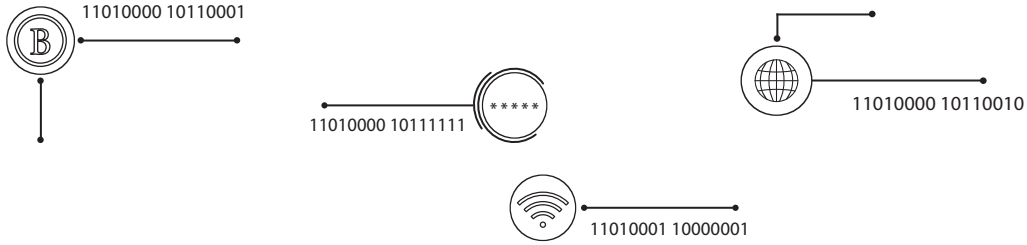


СОДЕРЖАНИЕ

* С ноября 2022 г. на территории Российской Федерации запрещено распространять информацию о VPN-сервисах с целью доступа к запрещенному контенту. Научная, научно-техническая и статистическая информация о VPN-сервисах для обхода блокировок признана запрещенной в России, исключением является информация о VPN для обеспечения защищенного удаленного доступа. — *Прим. ред.*

* В 2022 г. российский суд признал информацию в Tor Browser запрещенной к распространению в стране, запретил приложение Tor Browser, а также ограничил доступ к программе Tor Browser. — *Прим. ред.*

** С ноября 2022 г. на территории Российской Федерации запрещено распространять информацию о VPN-сервисах с целью доступа к запрещенному контенту. Научная, научно-техническая и статистическая информация о VPN-сервисах для обхода блокировок признана запрещенной в России, исключением является информация о VPN для обеспечения защищенного удаленного доступа. — *Прим. ред.*



ПРОЛОГ

ЗДРАВСТВУЙТЕ, ЧИТАТЕЛЬ!

Вы держите в руках руководство, вобравшее в себя разные точки зрения на, казалось бы, привычные уже задачи в области информационной безопасности. В книге собран многолетний, позволяющий по новому взглянуть на будущие вызовы, с которыми сталкиваются предприятия и организации. Ведь не новость, что мы живем в цифровую эпоху, когда информация — будь то личные или корпоративные данные — становится ключевым активом и защита этого актива имеет первостепенное значение.

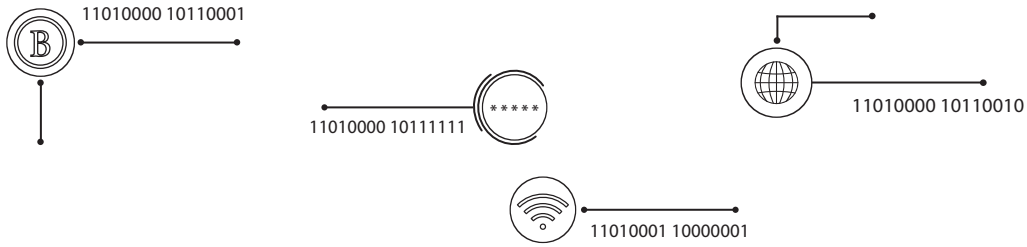
Цель этого труда — ввести понятие «цифровая иммунная система» и сделать его важным не только для промышленных гигантов, но и для куда меньших по размеру организаций, показать, что гигиена информации и цифровой иммунитет необходимы и весьма просты в интеграции. По сути, каждый бизнес-процесс сводится к работе с информацией, а значит, описанные в книге принципы и подходы важны для бизнеса любого масштаба. Более того, многие из нас уже применяют определенные методы защиты в повседневной практике, а значит, обобщение существующего опыта — отличная идея.

В этой книге мы рассмотрим актуальные угрозы, методы их предотвращения и пути выстраивания цифровой иммунной системы для защиты данных и их источников. В каждой главе я рассказываю о проверенных временем принципах безопасности и конфиденциальности, которые могут быть внедрены в работу организации, и опираюсь прежде всего на свой личный опыт.

Цифровой мир развивается с невероятной скоростью, и вместе с ним меняются и вызовы. Эта книга помогает разобраться в вопросах цифровой безопасности — принципах и подходах, которые позволят минимизировать риски, связанные с данными и приватностью в интернете. Я стремлюсь донести сложные идеи

простым языком, ориентируясь на специалистов по безопасности, которые хотят осознанно подходить к защите информационной инфраструктуры.

Эта книга будет полезна тем, кто желает распознавать угрозы и грамотно выстраивать защиту, обеспечивая безопасность данных, без изучения лишней теории и путаницы со сложными терминами. Здесь собраны реальные примеры и проверенные решения в формате best practice.



ОБ АВТОРЕ

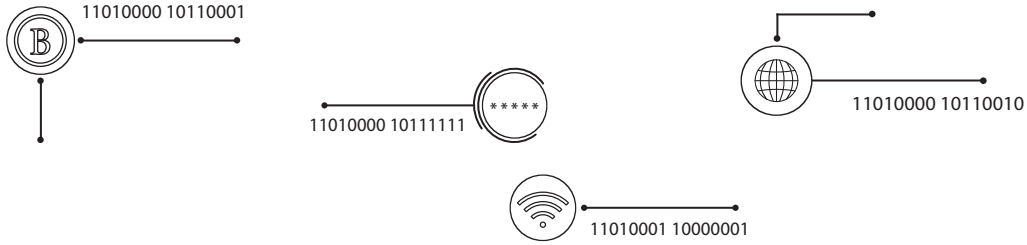
Я, Антон Шустиков, за свою карьеру в области информационной безопасности и ИТ прошел путь от разработчика до управленца на уровне C-level со степенью MBA. Я успел получить опыт как в стартапах, так и в крупных финтехпроектах, например, принимал участие в разработке и внедрении ПО для операторов связи и для осуществления торговли ценными активами. Были шаги и в сторону, вроде разработок для солнечной энергетики и встраиваемых систем. Сегодня у меня за плечами почти 20 лет в информационных технологиях и порядка 10 лет на управленческих позициях. Я специализируюсь на построении защищенных систем и создании продуктов для финтехсектора, на управлении финансами и активами.

Мне посчастливилось поработать над созданием и собственной SIEM-системы, над разработкой решений для анонимного общения лиц, причастных к управлению нашей страной, над решениями для VIP-клиентов, а также участвовать в запуске криптовалютных платформ. Опыт охватывает и аналитическую сторону — от изучения эксплойтов до реагирования на инциденты и расследования киберхищений. В том числе мне довелось основывать и возглавлять разные проекты, что дало глубокое понимание всех аспектов управления информационными технологиями, информационной безопасностью и криптомиром. Опыт работы с высокопоставленными чиновниками и общение с первыми лицами крупных организаций помогли мне сформировать понимание потребностей рынка в целом — от кибергигиены до защиты данных.

Будучи активистом в сфере кибербезопасности, я информирую предприятия и государственные структуры, если обнаруживаю уязвимость или проблему, консультирую по вопросам их устранения. Это также касается частных компаний, где я помогаю выявлять и решать проблемы. Могу назвать себя и сторонником гражданских инициатив: стараюсь поднимать острые вопросы, чтобы

привлечь внимание общественности, делая акцент на важности безопасности в современном цифровом мире.

Основываясь на всем имеющемся опыте, я решил заниматься общественным просвещением в сферах, в которых признан экспертом. Пишу для таких известных изданий, как «Хакер» и Forbes. Недавно запустил проект CakesCats, нацеленный на обеспечение безопасности и упрощение технологий для пользователей. Миссия проекта — снизить технические барьеры и позволить компаниям любого размера пользоваться средствами защиты без сложных настроек или даже использовать преднастроенные конфигурации.



ЦИФРОВАЯ ИММУННАЯ СИСТЕМА

В последние десятилетия мир переживает стремительный рост цифровых технологий, которые стали неотъемлемой частью повседневной жизни. Однако наряду с этим ростом возросло и количество угроз, направленных на уничтожение, повреждение или кражу данных. Стремясь защитить свои цифровые активы, организации и компании инвестируют значительные ресурсы в защитные механизмы. Одним из ключевых направлений в области защиты является концепция цифровой иммунной системы (Digital Immune System, DIS), которая постепенно становится фундаментальной стратегией кибербезопасности.

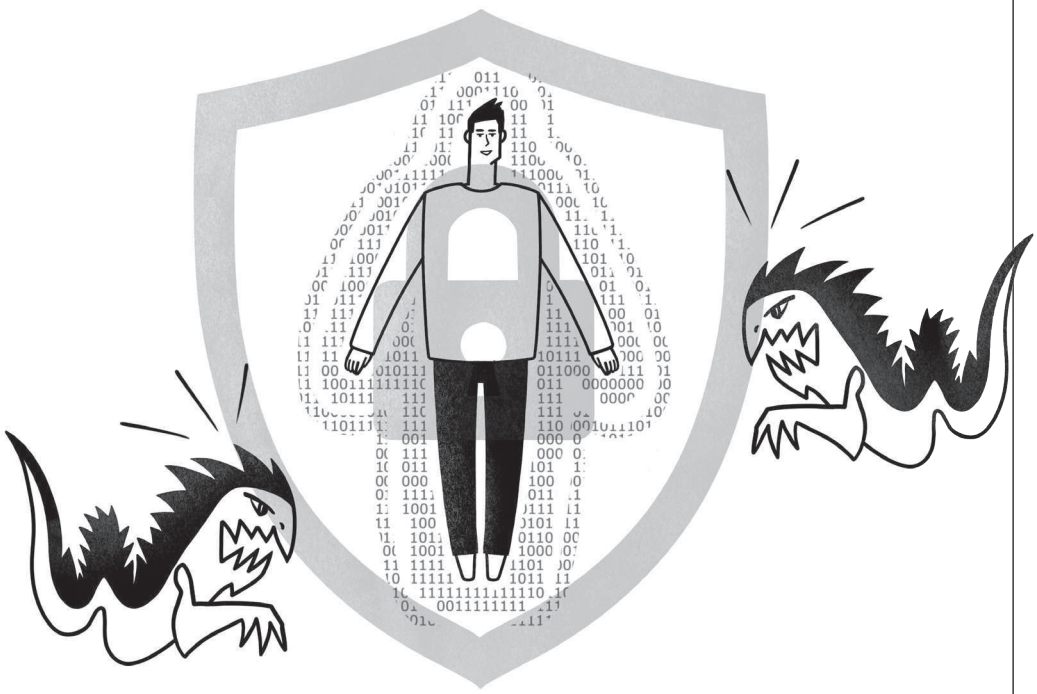
ЧТО ТАКОЕ ЦИФРОВАЯ ИММУННАЯ СИСТЕМА?

Цифровая иммунная система — это инновационная концепция, которая отражает новую эру в кибербезопасности. Мир цифровых технологий продолжает стремительно развиваться, и угроза кибератак растет вместе с этим развитием. В условиях, когда каждую секунду в Сети происходят тысячи атак, создание автоматизированных, адаптивных и проактивных решений безопасности становится критически важным для организаций любого уровня.

Цифровая иммунная система — это не просто технология, это особый подход или, если угодно, гибкая стратегия защиты, позволяющая системе быть готовой к атаке, на которую та еще не ориентирована, быстро восстанавливаться и учиться на опыте, обеспечивая надежную защиту цифровых активов в условиях динамичного и постоянно меняющегося мира киберугроз.

Цифровая иммунная система представляет собой совокупность различных технологий, методов и процессов, которые совместно работают для защиты систем и данных от кибератак, сбоев и других вредоносных воздействий. Как

и биологическая иммунная система, она должна не просто защищать системы от известных угроз, но и адаптироваться к новым, постоянно развивающимся вызовам.



Концепция цифровой иммунной системы основана на нескольких ключевых аспектах.

- **Автоматическое реагирование:** способность автоматически выявлять аномалии и отвечать на них без необходимости человеческого вмешательства, что позволяет оперативно реагировать на инциденты.
- **Адаптация и обучение:** подобно тому как биологическая иммунная система учится на предыдущих атаках, цифровая иммунная система собирает данные и использует машинное обучение для постоянного улучшения своих защитных механизмов.
- **Проактивность:** вместо пассивного ожидания атаки цифровая иммунная система предполагает активный мониторинг систем и происходящего вокруг с целью выявления потенциальных угроз до того, как они нанесут значительный ущерб.

ЭВОЛЮЦИЯ КИБЕРУГРОЗ И НЕОБХОДИМОСТЬ НОВОЙ ПАРАДИГМЫ

Современные киберугрозы кардинально отличаются от тех, с которыми столкнулись первые пользователи интернета. Примитивные вирусы и «черви» 90-х годов уступили место сложным целевым атакам (APT), программам-вымогателям (ransomware) и уязвимостям «нулевого дня». Эти атаки становятся все более изощренными, полагаются на социальную инженерию, искусственный интеллект и автоматизированные средства взлома.

Традиционные методы защиты, такие как антивирусы, системы обнаружения вторжений и файрволы, больше не справляются с постоянно развивающимися угрозами. Эти средства, как правило, основаны на сигнатурах, или заранее известных уязвимостях. Однако в мире, где злоумышленники используют искусственный интеллект для создания уникальных атак, старые подходы становятся менее эффективными.

Цифровая иммунная система предлагает более динамичный, адаптивный и интеллектуальный подход к защите персональных данных и систем, который может полностью предотвращать новые и неизвестные угрозы благодаря внедрению несложных правил личной цифровой гигиены.

ОСНОВНЫЕ КОМПОНЕНТЫ ЦИФРОВОЙ ИММУННОЙ СИСТЕМЫ

Цифровая иммунная система состоит из нескольких ключевых компонентов, которые работают вместе, чтобы обеспечить комплексную защиту.

1. **Мониторинг** — постоянный анализ сетевого трафика, активности пользователей и других данных для выявления аномалий и подозрительных действий. Это такие вещи, как менеджмент уязвимостей, Security Operations Center (SOC) или HoneyPot, и для личного применения они мало подходят, однако для «больших данных» необходимы. Сегодня все важнее становится использование машинного обучения и искусственного интеллекта для анализа данных, выявления необычных паттернов и прогнозирования потенциальных угроз. Для физического пользователя сегодняшние приоритеты — это в большой степени

осведомленность о том, какие атаки актуальны, изучение новых угроз и личная гигиена данных.

2. **Проактивность.** Системы, в профиль которых заложена способность предпринимать действия по защите и минимизации последствий, меры, нацеленные на минимизацию атак, такие как изоляция скомпрометированных устройств и аккаунтов, ограничения инструментария и доступа к данным в зависимости от типа используемого аккаунта (вроде «личный» или «рабочий»), использование иных мер вроде «горячих» или «холодных» кошельков с целью минимизации утраты контроля над финансами и благами.
3. **Быстрое восстановление.** В первую очередь это регламенты и планы на случай сбоев и атак, способность быстро восстанавливаться благодаря созданию резервных копий, использованию дублирующих серверов и другим методам обеспечения отказоустойчивости.
4. **Саморегенерация системы** — в случае применения интеллектуальных систем речь может идти даже о такой фантастической вещи. Это кажется невозможным, но на деле все проще — можно вспомнить, как миллионы раз нам по телефону из службы поддержки провайдера говорят одно и то же: «Перезагрузите роутер». Это действие не во всех случаях может помочь, но только после него либо подключаются другие протоколы, либо нас переключают на другого специалиста. Так и тут: некоторые вещи можно поручить как автоматике (перегрузка электросети, например), так и ИИ-помощнику (проверка списка запущенных служб или анализ логов с дальнейшим автоматическим решением).

ПРЕИМУЩЕСТВА ЦИФРОВОЙ ИММУННОЙ СИСТЕМЫ

Одним из ключевых преимуществ цифровой иммунной системы является ее способность к самовосстановлению и активной защите. В отличие от традиционных систем, которые реагируют только на завершившиеся атаки, цифровая иммунная система стремится предотвратить инциденты на ранних стадиях, минимизируя ущерб. Кроме того, такая система активно учится на прецедентах, улучшая защитные механизмы.

- **Масштабируемость.** Цифровая иммунная система может адаптироваться под потребности различных компаний, от индивидуальных клиентов до крупных корпораций (сам термин берет начало из гигантов отрасли).
- **Быстрое реагирование на угрозы и готовность к атакам.** Способность быстро обнаруживать угрозы и реагировать на них значительно снижает риск, например, при проникновении злоумышленников в сеть.
- **Интеграция с существующими системами.** Цифровая иммунная система легко встраивается в уже существующую инфраструктуру безопасности, дополняя и расширяя возможности традиционных решений. Для физического пользователя это вопрос некоторого порядка в делах.

АВТОМАТИЧЕСКОЕ ОБНАРУЖЕНИЕ И РЕАГИРОВАНИЕ НА УГРОЗЫ: ЦИФРОВАЯ ИММУННАЯ СИСТЕМА В ДЕЙСТВИИ

В условиях постоянно возрастающих цифровых угроз и атак традиционные методы защиты, такие как антивирусы и межсетевые экраны, уже не всегда способны обеспечить полную безопасность. Современные вызовы требуют использования новых технологий и подходов, и здесь на помощь приходит автоматизация обнаружения и реагирования на угрозы. В этом контексте можно провести аналогию с иммунной системой человека — точно так же, как иммунитет распознает возбудителей и борется с инфекциями, системы и меры проактивной безопасности могут выявить и нейтрализовать цифровые угрозы в режиме реального времени.

Автоматизация обнаружения с быстрым реагированием на угрозы — важнейший элемент современной цифровой иммунной системы, которая обеспечивает безопасность данных и инфраструктуры. Такие системы не только позволяют оперативно реагировать на угрозы, но и снижают полученный ущерб и урон, предоставляя возможность сосредоточиться на более сложных задачах. Однако для их успешного внедрения в корпоративном сегменте необходимо учитывать потенциальные риски, связанные с ложными срабатываниями и зависимостью от искусственного интеллекта, ведь, даже синтетическому, ему доверять нельзя

и следует разрабатывать эффективные регламенты безопасности, отталкиваясь от реалий. Какому пользователю необходим файрвол за несколько сотен тысяч долларов? А крупная компания уже не может без него обходиться. В результате в обоих случаях подход будет в корне разный.

Автоматизация в области информационной безопасности охватывает несколько ключевых направлений.

1. **Мониторинг событий.** Системы мониторинга собирают данные о сети и активности на устройствах, выявляя аномальные действия, которые могут свидетельствовать о вторжении или вредоносной активности. Это напоминает работу иммунных клеток, которые «сканируют» организм в поисках угроз.
2. **Машинное обучение и искусственный интеллект.** Многие современные системы безопасности используют искусственный интеллект и машинное обучение для анализа данных. Эти алгоритмы способны выявлять новые типы атак, анализируя поведение системы и предсказывая потенциальные угрозы. Примером могут служить платформы, которые обучаются на основе исторических данных и могут предсказать, когда и как может произойти атака.
3. **Автоматическое реагирование.** После обнаружения угрозы система может немедленно предпринять действия для ее нейтрализации: отключить зараженное устройство, заблокировать подозрительную активность, уведомить администратора. Этот процесс аналогичен работе антител, которые нейтрализуют вирусы и бактерии в организме.
4. **Закалка (Hardening) системы** — это процесс усиления безопасности устройства путем устранения потенциальных уязвимостей, минимизации и ограничения «свободы действий» системы или программ через контроль поведения. Иначе говоря, выключать программу, если она делает что-то странное.

Автоматизация безопасности предоставляет целый ряд преимуществ.

- **Скорость реагирования.** Время — критически важный фактор в любой атаке. Автоматические системы реагируют мгновенно, что минимизирует ущерб и предотвращает дальнейшее распространение угрозы.