Идеология кибериммунных решений.

Для чего нужны, базовые принципы, преимущества

Константин РОДИН,
руководитель направления по развитию продуктов, компания «АйТи Бастион»

Современный мир неотделим от технологий и с каждым днем становится все более цифровым. Однако это относится не только к благам, которые они приносят, но и к угрозам, которые могут в себе нести. Кибербезопасность становится здесь особенно актуальной и значимой областью, а новые идеологии и подходы к ней – крайней необходимостью. Одной из таких инновационных концепций является идеология кибериммунных решений – комплексного подхода к защите информационных систем и данных, основанного на принципах иммунной системы организма человека. Порассуждаем на тему кибериммунности вместе с Константином Родиным, руководителем направления по развитию продуктов, экспертом компании «АйТи Бастион».

С непрерывным увеличением количества кибератак и сложностью их технического исполнения хакеры становятся умнее, находчивее и кажется, что всегда идут «на шаг впереди», раз им удается совершать свои нападения, – традиционные методы кибербезопасности начинают терять свою эффективность. Проактивный инновационный подход к защите информации становится жизненно важным. ИБ-специалисты начинают «смотреть по сторонам» и обращаются к новым информационным нишам. В этом контексте их внимание привлекли научные исследования в области иммунологии. Иммунная система человека успешно справляется с обнаружением инфекций и борьбой с ними благодаря сложной системе адаптивных механизмов. Идея использовать этот принцип для защиты информационных систем и данных и привела к концепции кибериммунных решений.

Что такое кибериммунитет?

Для начала разберемся в самом понятии «кибериммунитет», зачем нужны кибериммунные решения и как они работают.

Традиционные методы кибербезопасности часто основаны на сборе и анализе уже обнаруженных, известных угроз и атак с использованием сигнатур и эвристических правил. Однако такие методы могут ограничивать предотвращение новых, ранее неизученных кибернападений, ибо злоумышленники не стоят на месте и постоянно разрабатывают новые способы обхода ИТ-защиты. Это создает необходимость в более инновационных и адаптивных подходах к кибериммунным решениям.

Кибериммунитет – концепция кибербезопасности, основанная на принципах иммунной системы организма и применяемая для защиты информационных систем и данных от киберугроз и хакерских атак. Такой подход предполагает создание адаптивных, самообучающихся и саморегулирующихся систем, которые способны обнаруживать и противостоять не только известным ранее, но и новым атакам и уязвимостям.

Концепция кибериммунитета и ее составляющих – кибериммунных решений – это перспективный подход к одной большой и значимой цели – обеспечению информационной безопасности, снижению ИБ-рисков и повышению уверенности в цифровом мире.

Для чего нужны кибериммунные продукты?

Как уже было сказано, текущая ситуация выглядит в основном как

игра в догонялки, причем догонять приходится «обороняющей» стороне. Соответственно именно эту ситуацию и призван разрешить кибериммунитет.

Базовая защита. Начнем, конечно, с принципов secure by design, когда подход к безопасности пронизывает все этапы проектирования и разработки программных продуктов, тем самым позволяя реализовать базовый иммунитет.

Проактивная защита в обнаружении новых угроз. Традиционные методы кибербезопасности часто ориентированы на обнаружение уже известных угроз с помощью отработанных алгоритмов. Кибериммунные решения, внедренные в ИТ-инфраструктуру, позволяют обнаруживать новые атаки и аномалии на основе анализа поведения системы, в том числе с использованием искусственного интеллекта.

Снижение времени реакции. Кибериммунные продукты обеспечивают более быстрое реагирование на угрозы благодаря специальным автоматизированным механизмам обнаружения, которые помогают системе самостоятельно адаптироваться под нестандартные условия и создавать противодействие.

Снижение ложных срабатываний. Используя анализ поведения и контекста, кибериммунные системы могут снизить количество ложных срабатываний. Это позволяет сократить нагрузку на специалистов и улучшить эффективность ИБ-системы.

Адаптация к изменяющимся угрозам. Ориентируясь на концепцию иммунной системы человека, кибериммунные продукты способны снизить воздействие успешных хакерских атак и ограничить распространение вредоносного кода, что делает ИТ-систему более надежной и устойчивой.

Какие базовые принципы заложены в работу кибериммунных решений

Изоляция и нулевое доверие. Компоненты системы должны быть изолированы друг от друга, а все их взаимодействия обеспечены через отдельные потоки данных. При этом уровень доступов компонентов должен быть обеспечен на уровне не выше требуемого для решения их задач.

Анализ. Системы обучаются на основе исследования исторических данных о поведении системы, угрозах и атаках. Они используют машинное обучение и анализ больших данных для создания модели «нормального» поведения системы.

Детекция аномалий. Решения постоянно контролируют и мониторят активность ИТ-системы, анализируют ее текущее поведение, сравнивая его с уже изученной моделью. Если в ее работе возникают аномалии, система может считать это потенциальной угрозой информационной безопасности.

Ответ и противодействие. При обнаружении любой подозрительной активности системы кибериммунитета могут самостоятельно предпринимать автоматические действия, направленные на ее пресечение. Это может быть блокировка доступа в ИТ-контур, изоляция уязвимых участков, нейтрализация вредоносных объектов.

Самообучение и адаптация. Кибериммунные решения изменчивы, они постоянно находятся в процессе обучения и адаптируются к новым условиям с течением времени их жизни внутри информационной системы. За счет этого она и сама начинает учиться, подстраивается под новые виды киберугроз и атаки.

Коллективный разум. Некоторые решения кибериммунитета могут обмениваться информацией о новых аномалиях с другими системами, чтобы обеспечить максимально оперативное и эффективное реагирование на вновь появляющиеся угрозы.

Преимущества кибериммунных продуктов

По сути в базовых принципах кибериммунных систем заложены их главные преимущества – создание адаптивных, интеллектуальных и эффективных методов защиты информационных систем от киберугроз.

Помимо анализа угроз и обнаружения атак, непрерывного мониторинга аномалий, быстрого самообучения и адаптивности к изменяющимся условиям, обращения к коллективному киберразуму это еще и системный подход. Ведь кибериммунные решения рассматриваются в первую очередь как комплексный набор инструментов и методов, затрагивающих различные аспекты кибербезопасности:

мониторинг, анализ, предотвращение и реагирование.

Перечисляя преимущества, стоит сказать и о минусах, в первую очередь о необходимости построения единой комплексной системы, которая играет по единым правилам, выстроена с самого первого этапа проектирования и до внедрения. Именно по этой причине текущий этап развития подобных систем отчасти продолжает историю дополнительных наложенных средств защиты существующих ИТ-инфраструктур.

Кибериммунность в России

Кибериммунитет в нашей стране представляет собой динамично развивающуюся область, все усилия направлены на укрепление информационной безопасности и защиту ИТ-систем и данных от разного вида хакерских атак и угроз. Государство, бизнес, представители науки, сферы информационных технологий и ИБ активно работают над внедрением и применением концепции кибериммунности для обеспечения надежной защиты в условиях современной цифровой среды.

Российские ученые и ИБ-эксперты также активно занимаются научными исследованиями в области кибериммунитета. Они разрабатывают новые методы анализа данных, машинного обучения и искусственного интеллекта для создания более эффективных и адаптивных систем защиты. Так, например, специалисты Инновационного института искусственного интеллекта, кибербезопасности и коммуникаций им. В.С. Попова работают над изучением и активным применением искусственного интеллекта в сфере кибербезопасности, а эксперты Хаба кибербезопасности в Сколково – над инновационными подходами к защите информации, включая использование искусственного интеллекта и анализа массивов данных.

Кроме систем безопасности стоит отметить и работы со стороны ИТ-компаний в части создания непосредственно ИБ-продуктов, которые основываются на базовых принципах кибериммунности и позволяют снизить или полностью исключить часть угроз при их эксплуатации. В частности, специалисты из «Лаборатории Касперского» внедряют собственную операционную систему Kaspersky OS, предназначенную для создания ИТ-решений для отраслей с повышенными требованиями к кибербезопасности, надежности и предсказуемости работы. А эксперты из «Ростелеком-Солар» реализуют комплексный подход по внедрению целой линейки продуктов, которая

включает в себя анализ угроз, предотвращение вторжений, построение и эксплуатацию систем кибербезопасности.

Промышленные предприятия тоже разрабатывают и внедряют продукты, которые основываются на принципах кибериммунности. Такие решения помогают бизнесу выявлять новые угрозы, быстро реагировать на атаки и снижать риски, обеспечивая непрерывную работу и предотвращая возможные потери (финансовые, репутационные и др.).

На уровне государства вопросам кибериммунитета в России также уделяется много внимания. Специалисты занимаются реализацией систем мониторинга и защиты, способных выявлять и анализировать новые угрозы. Это необходимо для обеспечения кибербезопасности государственных органов, критической инфраструктуры и других важных и чувствительных с точки зрения информационной безопасности объектов как внутри страны, так и за ее пределами, если речь идет о международных инициативах и сотрудничестве в области ИБ.

Стоит отметить, что в этом процессе на контроле остается и вопрос подготовки специалистов в области кибербезопасности с учетом принципов кибериммунности: разрабатываются специальные образовательные программы и курсы, в том числе узкой направленности. Такая работа помогает обеспечить наличие квалифицированных специалистов, которые могут создавать и поддерживать системы ИБ-защиты на основе этой концепции.

В целом значимость ситуации в области кибериммунитета в нашей стране растет, интерес к этой области укрепляется. Но ее развитие зависит от множества факторов, включая технологический прогресс, потребности бизнеса и государства, возможности сферы ИТ, ИБ и компетенции специалистов, а также общие, в том числе международные, тренды в области кибербезопасности.

В любом случае, вопрос кибериммунизации – комплексный. Это синергия идей и усилий целой отрасли и множества компаний, когда требуется не только выработка единого подхода, но и слаженность совместных действий. Если говорить о подходе к синергии, то здесь стоит отметить определенные подвижки и выход различных производителей на конструктивный диалог не только со стороны финансового результата, но и с точки зрения повышения безопасности на уровне комплексных систем ИБ в целом. Например, компания «АйТи Бастион» в рамках развития и обеспечения комплексной информационной безопасности доступа к инфраструктуре – экосистемной PAM-платформы безопасного удаленного доступа «СКДПУ НТ» (как для крупного промышленного и государственного сектора, так и для небольших компаний с элементом экосистемы – коробочным продуктом «СКДПУ НТ Компакт») – активно взаимодействует с лидерами рынка ИТ- и ИБ-решений для построения *единой взаимодополняемой и обогащаемой системы безопасности*, которая способна не только узконаправленно обнаруживать потенциальные инциденты, но и обмениваться собранными данными между компонентами, доводя первое срабатывание детекторов до автоматического реагирования.

Новые правила игры в ИБ

В современном цифровом мире, где технологии продолжают стремительно развиваться, информационная безопасность становится все более важной и сложной задачей. Традиционные методы защиты ИТ-систем сталкиваются с новыми вызовами, такими как атаки «нулевого дня», сложные международные киберугрозы и масштабные сетевые атаки. Логично, что в ответ на них в мире кибербезопасности начали развиваться новые концепция и идеология – концепция кибериммунитета и идеология кибериммунных решений.

Подходы к их реализации могут быть разными, но главное, что все усилия в их разработке и внедрении направлены на создание более эффективных, интеллектуальных и адаптивных методов борьбы с современными киберугрозами, основываясь на принципах анализа аномалий, контекстного анализа, адаптивности, самообучения и имея в своей базе ядра, не подверженные основным типам классических атак. По сути на то, чтобы переписывать правила игры в ИБ и обеспечивать надежную защиту информационных ресурсов с момента их создания. ■