УДК 004.056.5

КИБЕРИММУНИТЕТ КАК ИННОВАЦИОННЫЙ ПОДХОД К РАЗРАБОТКЕ БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Корешков Д.С. (АлтГТУ им. И.И. Ползунова), **Прытов М.В.** (АлтГТУ им. И.И. Ползунова), **Стеганцев Д.С.** (АлтГТУ им. И.И. Ползунова)
Научный руководитель – старший преподаватель кафедры ИВТиИБ Теплюк П.А. (АлтГТУ им. И.И. Ползунова)

Введение.

С ростом цифровизации и увеличением числа пользователей в высоконагруженных системах, многие IT-компании нуждаются в быстром масштабировании своего приложения или веб-сервиса, вследствие чего зачастую пренебрегают безопасностью. Ввиду этого, в приложениях появляются уязвимости и возрастает риск кибератаки. Так, согласно отчету компании Positive Technologies за 2 квартал 2023 года, количество компаний, подверженных атакам хакеров, возросло на 17% по сравнению с кварталом прошлого года, количество успешных атак, связанных с эксплуатацией уязвимостей, составляет 35% [1]. Тенденция к подобного рода инцидентам будет продолжаться, особенно в госсекторе Российской Федерации, в связи с чем возникает потребность в создании более безопасных и отказоустойчивых систем.

Основная часть. Основными проблемами безопасности систем являются изначальные ошибки в архитектуре приложения, скорость исправления этих ошибок и стоимость проектирования полноценной системы защиты. Часто бывает так, что вендор, выпускающий свой продукт, может не знать о уязвимостях в приложении – это накладывает большие риски на саму систему и ее конечных пользователей. Неизвестно сколько времени злоумышленник мог эксплуатировать ошибку, а исправление при помощи патчей не всегда помогает, также стоит учитывать время разработки самих патчей, рассылку исправлений всем пользователям, а также саму стоимость дальнейшей поддержки приложения с учетом всех его потенциальных уязвимостей и репутационные риски.

Одним из решений данной проблемы является кибериммунный подход к разработке приложений, представленный Лабораторией Касперского. Данное решение позволяет спроектировать архитектуру приложения с уже «встроенной» защитой от существующих и потенциальных угроз системы [2]. Разработчикам не нужно перегружать систему излишками защитных мер, все внимание сфокусировано на основных, критически важных функциях приложения. Даже если произойдет атака на один из узлов системы, остальное приложение будет исправно работать.

Гибкость подхода позволяет применять его во многих сферах производства и услуг, так как система защиты проектируется параллельно с созданием архитектуры самого приложения, что соответствует идеологии Secure by Design [3]. Защита обеспечивается согласно требованиям международных стандартов безопасности, таких как: Common Criteria, ASPICE, ISO 26262 и других.

Преимуществом кибериммунного подхода является минимизация доверенной кодовой базы, что позволяет обеспечить максимальную защиту без переписывания большого количества кода, даже в уже функционирующих приложениях. Такой подход позволяет уменьшить затраты на дальнейшую поддержку приложения и исправления потенциальных ошибок. Так, при проектировании и разработке кибериммунной системы видеонаблюдения учитывается не только законодательство и международные стандарты, но и политики безопасности со всеми возможными сценариями, применяемыми к конкретному приложению. Примером такого сценария может являться стандартная DDoS-атака на сервер системы, что является серьезной угрозой для системы. Для того, чтобы предотвратить потенциальный инцидент, достаточно на этапе проектирования предусмотреть возможные варианты фильтрации трафика [4].

Выводы. Разработка с применением кибериммунного подхода является одним из перспективных направлений кибербезопасности, соответствует законодательству и стандартам в области обеспечения безопасности и нуждается в популяризации. На примере проектирования кибериммунной системы видеонаблюдения было показано, что решение позволяет минимизировать затраты производства на дальнейшую поддержку приложения в условиях недоверенной среды.

Список использованных источников:

1. Актуальные киберугрозы: II квартал 2023 года // Positive Technologies : [официальный сайт]. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023-q2/.

2. Кибериммунитет // KasperskyOS : [официальный сайт]. – URL: https://os.kaspersky.ru/technologies/.

3. «Врожденная защищенность» Secure by Design // KasperskyOS : [официальный сайт]. – URL: https://os.kaspersky.ru/soczialnye-seti/vrozhdennaya-zashhishhennost-secure-by-design/.

4. Фелисов, Д.А. Архитектура высоконагруженных приложений // Universum: технические науки: электронный научный журнал. – URL: https://7universum.com/ru/tech/archive/item/16138.