СВЯЗЬ РАБОТЫ СПЕЦИАЛИСТА В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ С БЕЗОПАСНОСТЬЮ ЖИЗНЕДЕЯТЕЛЬНОСТИ

Соколов Александр Владимирович

студент, кафедра экологии, безопасности жизнедеятельности и электропитания, Московский технический университет связи и информатики, РФ, г. Москва

Курбатов Валерий Александрович

научный руководитель, доцент кафедры канд. физ. –мат. наук, Московский технический университет связи и информатики, РФ, г. Москва

Введение

Безопасность жизнедеятельности (БЖД) охватывает защиту не только физической, но и цифровой среды, поскольку современный человек часто взаимодействует с технологиями, которые влияют на его безопасность и конфиденциальность. В условиях цифровизации организаций защита данных и устойчивость систем становятся важными аспектами БЖД. В этой связи DevSecOps, объединяя разработку и безопасность, направлен на обеспечение безопасности всех этапов жизненного цикла программного обеспечения. Это помогает предотвращать утечки данных и кибератаки, которые угрожают как безопасности организаций, так и их пользователей. Настоящий доклад исследует связь DevSecOps и БЖД, подчеркивая его роль в защите пользователей и систем от внешних угроз. Рассматриваются проблемы безопасности, риски уязвимостей и методы DevSecOps для их минимизации. Важной целью является поддержание устойчивой и безопасной работы сервисов, что способствует защите не только данных, но и устойчивости организаций. Внедрение DevSecOps позволяет не только повысить защиту информации, но и минимизировать риски, что особенно важно для компаний, работающих с критически важными данными, такими как финансы или медицина, влияющими на безопасность пользователей.

1. Роль DevSecOps в защите информационных систем и БЖД

DevSecOps интегрирует процессы безопасности и разработки, позволяя обеспечивать защиту данных и инфраструктуры на всех этапах жизненного цикла. Это особенно важно для систем, от которых зависит безопасность пользователей, таких как медицинские устройства, финансовые сервисы или промышленные системы. В традиционном процессе разработки безопасность добавлялась после создания продукта, что увеличивало риск уязвимостей и непредвиденных ошибок. DevSecOps позволяет постоянно отслеживать и устранять угрозы, минимизируя риск утечек данных и атак. Например, уязвимости в системах банковского обслуживания могут привести к кражам средств клиентов, что напрямую угрожает их безопасности. Применение DevSecOps помогает интегрировать механизмы безопасности, такие как шифрование данных и управление доступом, с самого начала, делая системы более устойчивыми к потенциальным угрозам. Постоянное тестирование и мониторинг помогают оперативно выявлять и устранять слабые места, что значительно снижает риски для пользователей и повышает уровень доверия к сервисам.

1. Важность автоматизации процессов безопасности и её влияние на БЖД

Автоматизация процессов безопасности в DevSecOps играет ключевую роль в снижении числа ошибок, ускорении обнаружения уязвимостей и повышении общей устойчивости систем. В рамках цифровой безопасности жизнедеятельности (БЖД) автоматизация позволяет быстро

реагировать на потенциальные угрозы, обеспечивая стабильную и безопасную работу систем, от которых зависят пользователи. Например, автоматизация сканирования уязвимостей помогает находить и исправлять проблемы до их возможного использования злоумышленниками, что минимизирует риск кибератак. Такой подход особенно важен для систем с высокими требованиями к безопасности, например, в здравоохранении, где защита данных пациентов является приоритетом. Автоматизация тестирования безопасности, включая статический и динамический анализ, позволяет выявлять недостатки на каждом этапе разработки, а непрерывная интеграция и доставка (CI/CD) упрощают внедрение обновлений безопасности. Помимо этого, автоматизация процессов безопасности уменьшает влияние человеческого фактора, что делает системы более надежными. Внедрение автоматизированных подходов также позволяет сотрудникам сосредоточиться на стратегических задачах, делая управление безопасностью более эффективным и снижая риски для конечных пользователей. В итоге, автоматизация способствует улучшению уровня безопасности жизнедеятельности в цифровой среде, обеспечивая защиту от потенциальных угроз и способствуя развитию устойчивых систем.

2. **Проблемы и риски, связанные с безопасностью и их влияние на БЖД**

Игнорирование безопасности на этапе разработки ведет к появлению множества уязвимостей, способных нанести ущерб пользователям и бизнесу. Например, утечки данных из-за уязвимости в ПО могут привести к хищению персональной информации, что ставит под угрозу финансовую безопасность людей. Особенно опасными становятся атаки на системы, связанные с критически важной информацией, например, медицинские или промышленные устройства, где риск затрагивает физическое здоровье людей. Отказ в обслуживании, вызванный атакой или технической ошибкой, также создает угрозу для организаций, поскольку приводит к потере данных и снижению производительности. Это напрямую влияет на БЖД пользователей, когда речь идет о сервисах, к которым они привязаны в повседневной жизни. Кибератаки на крупные компании, такие как утечки из Equifax или атак на социальные сети, показывают, что уязвимости ставят под угрозу конфиденциальность миллионов пользователей. DevSecOps стремится минимизировать подобные риски, обеспечивая безопасность данных и процессов.

3. **Влияние уязвимостей на безопасность жизнедеятельности пользователей**

Уязвимости в коде и конфигурации систем могут привести к опасным последствиям для безопасности пользователей. В случае критических данных, таких как медицинские записи или банковская информация, утечки могут повлечь за собой серьезные угрозы для финансовой стабильности и конфиденциальности пользователей. Например, медицинские системы, подвергшиеся атаке, могут оказаться под угрозой отказа в обслуживании, что несет риск для здоровья пациентов. DevSecOps помогает внедрить методы защиты, которые делают системы более устойчивыми к подобным угрозам. Статический анализ кода и автоматическое тестирование позволяют выявлять и устранять ошибки на ранних этапах разработки, значительно снижая риск их использования злоумышленниками. Защита данных и безопасность инфраструктуры становятся приоритетом, что особенно важно для организаций, работающих с личными данными пользователей. Внедрение DevSecOps позволяет не только выявлять уязвимости, но и своевременно предотвращать кибератаки, минимизируя возможные угрозы для пользователей и повышая доверие к предоставляемым сервисам.

4. **Методы DevSecOps для минимизации рисков и защиты цифровой БЖД**

DevSecOps использует ряд методов и инструментов, которые позволяют автоматизировать проверку безопасности, выявляя и устраняя потенциальные угрозы еще до их появления. Среди таких методов — статический и динамический анализ кода, автоматизированное тестирование, управление доступом и регулярное обновление программного обеспечения. Статический анализ помогает выявить ошибки на этапе разработки, а динамическое тестирование позволяет протестировать систему в реальном времени. Постоянный мониторинг системы дает возможность отслеживать возможные инциденты безопасности, оперативно реагировать на них и минимизировать ущерб. Кроме того, DevSecOps подразумевает регулярное обучение сотрудников по вопросам безопасности, что помогает им быть готовыми к современным угрозам. Такие подходы делают системы более устойчивыми и

позволяют обеспечить защиту данных пользователей, что, в свою очередь, улучшает их БЖД. Внедрение этих методов делает инфраструктуру более защищенной, обеспечивая защиту не только бизнес-процессов, но и личных данных клиентов.

Заключение

DevSecOps становится важной составляющей защиты БЖД, так как обеспечивает безопасность информационных систем и данных. Интеграция безопасности на всех этапах жизненного цикла разработки позволяет защитить пользователей и минимизировать риски кибератак и утечек данных. Для повышения уровня безопасности важно регулярно проводить анализ уязвимостей, поддерживать инструменты защиты в актуальном состоянии и обеспечивать автоматизацию процессов безопасности. Кроме того, важно организовывать обучение сотрудников для повышения их осведомленности о киберугрозах и мерах по защите данных.

В заключение, стоит подчеркнуть, что DevSecOps, обеспечивая непрерывное развитие и защиту информационных систем, способствует улучшению безопасности жизнедеятельности в цифровой среде, делая системы более устойчивыми и защищенными. Это также укрепляет доверие пользователей и делает бизнес более надежным, что является важным преимуществом в условиях растущей угрозы кибератак.

Список литературы:

1. Электронный ресурс https://www.jetbrains.com/ru-ru/teamcity/ci-cd-guide/what-is-devsecops/