В последнее время все чаще используется Service Cloud для оптимизации информационной поддержки предприятия. Платформа обеспечивает пользователей автоматизированными особенностями, чтобы пойти через запросы на обслуживание клиентов, рабочие процессы направления потока, позволяет построить основу для реального разрешения проблем клиента. Преимуществом Service Cloud над любой другой платформой оптимизации информационной поддержки является то, что она позволяет вам получать заказы клиентов быстрее. Сервисная платформа Service Cloud позволяет использовать различные сервисные приложения, чтобы отслеживать требования обслуживания клиентов, технологический процесс обновляется и клиенты работают через процессы самообслуживания. В отличии от CRM, интеграция с Service Cloud предоставит вам возможность улучшить ваши отношения с клиентами тем самым увеличить прибыль компании.

Список использованной литературы

1. Sukhraj R. The 10 Very Best CMS Platforms for Digital Marketing / R.Sukhraj [Електронний ресурс].– Режим доступу: https://www.impactbnd.com/blog/top-10-cms-platforms-for-digital-marketing. – Назва з екрану.
2. Sharma A. Why Service Cloud over any other support optimization platform? / A. Sharma [Електронний ресурс]. – Режим доступу: http://www.signitysolutions.com/blog/salesforce/why-service-cloud-over-any-other-support-optimization-platform. – Назва з екрану.

V.A. Shutenko
I-st year stud. of magister level
specialty «Economisc»,
specialisation «Economic Cybernetics»
Research adviser: Senior lecturer A.S.Maksimov

INFORMATION SECURITY ASSESSMENT

Application security testing and examination help an organization determine whether its custom application software – for example, Web applications –containsvulner abilitie sthatcan be exploited, and whether the software behaves and interacts securely with its users, other applications (such as databases), and its execution environment. Application security can be assessed in a number of ways, ranging from source code review to penetration testing of the implemented application. Many application security tests subject the application to known attack patternstypical for that application's type. These patterns may directly

target the application itself, or may attempt to attack indirectly by targeting the execution environment or security infrastructure. Examples of attack patternsare information leakage (e.g., reconnaissance, exposure of sensitive information), authentication exploits, session management exploits, subversion (e.g., spoofing, impersonation, command injections), anddenial of service attacks [1, p.205].

Application security assessment should be integrated into the software development life cycle of the application to ensure that it is performed throughout the life cycle. For example, code reviews can be performed as code is being implemented, ratherthanwaiting until the entire application is ready for testing. Tests should also be performed periodically once anapplicationhas gone into production; when significant patches, up dates, or other modification saremade; or when significant changes occur in the threat environment where the applicationoperates [2, p.20].

Manyapplication security testing and examination techniques are available. They can be divided into white box techniques, which involve direct analysis of the application's source code, and black box techniques, which are performed against the application's binary executable without source code knowledge. Most assessments of custom application sare performed with white box techniques, since source code is usually available—however, these techniques cannot detect security defects in interfaces between components, nor can they identify security problems caused during compilation, linking, or installation-time configuration of the application. White box techniques still tend to be more efficient and cost-effective for finding security defects in custom applications than black box techniques. Black box techniques should be used primarily to assess the security of individual high-risk compiled components; interactions between components; and interactions between the entire application or application system with its users, other systems, and the external environment. Black box techniques should also be used to determine how effectively anapplication or application system can handlethreats. Many tests use both white box and black box techniques—this combination is known as gray box testing [3, p.22].

Application security continues to grow in importanceasattacke rsincreasingly focus on application-laye rattacks. Because application security assessment is a complex topic with dozens of commonly used techniques, it is outside the scope of this publication to provide specific information on techniques or recommendations for their use.

References:

1. Bayuk J. nformation Security Metrics – An Audit-Based Approach, Computer System Security and Privacy Advisory Board (CSSPAB) workshop on security metrics / J. Bayuk. – Texas: W. W. Norton & Company, 2002. – 785 c.
2. Moore A. Attack Modeling for Information Security and Survivability / A. Moore, R. Ellison, R. Linger. – Regensburg: Carnegie Mellon Technical Note, 2013. – 274 c.
3. Singh S. Probabilistic Validation of an Intrusion-Tolerant Replication System / S. Singh, M. Cukier, W. Sanders. // Master's thesis, University of Illinois at Urbana-Champaign. – 2003. – C. 7–23.