ВСТУП

З поширенням комп'ютерної мережі Інтернет в усі сфери людської діяльності особливого значення набуває інформаційна безпека даних, що виставляються користувачами мережі у різного ступеня відкритості доступ. Кіберпростір не має державних кордонів, людина, що здійснює несанкціонований доступ до комп'ютерної інформації, може перебувати на будь-якої території, автор комп'ютерного вірусу може розмістити його на популярному сайті і тим самим забезпечить його проникнення в різні країни.

Так, згідно з даними Cisco в 2015 році кіберзлочинці все активніше впроваджуються в веб-ресурси шляхом крадіжки даних і доступу до серверів АСУ. це створило умови для зростання вразливостей підробки міжсайтових запитів (CSRF), незважаючи на те, що з 2014 по 2015 рік категорія міжсайтового скриптинга (XSS) скоротилася на 47% [1]. Аналіз також показує, що організації досягли певних успіхів в шифруванні інформації при передачі між вузлами, однак збережені дані нерідко залишаються незахищеними. У більшості значущих порушень безпеки за останні кілька років зловмисники скористалися незашифрованими даними, що зберігаються в центрі обробки даних та інших внутрішніх системах, що дозволило хакерам добиратися до цінних відомостей без особливих проблем.

Актуальність проведення досліджень, пов'язаних з розробкою нових методів і способів захисту даних інформаційних систем управління, обумовлена стрімким зростанням впровадження процесів автоматизації в діяльність підприємств і організацій, як державного сектора економіки, так і приватних фірм і компаній.

Серед критеріїв інформаційної безпеки основними є: конфіденційність, цілісність і доступність інформації. Конфіденційність - це збереження в секреті інформації, доступ до якої обмежується вузьким колом користувачів. Цілісність - властивість, згідно з якою інформація зберігає свої початкові або узгоджені з кінцевим користувачем вид і якість, порушенням цілісності є санкціонована зміна змісту інформації. Доступність – це використання інформації за можливостями користувача, що має відповідні повноваження в необхідному для нього вигляді, час і місце, порушення доступності тягне за собою неможливість отримання або обробки інформації.

Метою дипломної роботи є формування методів захисту інформації та впровадження їх у веб-сервіс хмарного зберігання та обміну файлів. На основі поставленої цілі були поставлені задачі:

* проведення дослідження та аналізу існуючих методів захисту інформації та вибір використовуваних методів;
* проведення аналізу і вибір використовуваних технологій;
* розробка веб-сервісу хмарного зберігання файлів;
* впровадження обраних методів захисту в розроблений продукт;
* оцінка ефективності виконаної розробки.

1. Клаверов В.Б. Проблемы противодействия компьютерной преступности / Клаверов В.Б. [Электронный ресурс]. – Режим доступа: http: // www.securitylab.ru / contest / 382194.php [1]