

Жантлесов Жангабул Хамитович, к.ф-м.н
Байбусинов Азамат Сансызбаевич, магистрант
Казахский Агротехнический университет им. С. Сейфуллина
г.Астана, Казахстан, e-mail: azamat_b_astana@mail.ru
ORCID 0000-0002-9714-278X

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ КРИМИНАЛИСТИЧЕСКОГО ИССЛЕДОВАНИЯ РЕЕСТРА ОПЕРАЦИОННОЙ СИСТЕМЫ WINDOWS

Zhangabul Zhantlessov, & Azamat Baibussinov
S.Seifullin Kazakh AgroTechnical university
Astana, Kazakhstan
e-mail: azamat_b_astana@mail.ru
ORCID 0000-0002-9714-278X

SOFTWARE DEVELOPMENT FOR CRIMINALISTICS RESEARCH OF REGISTER OF THE OPERATING SYSTEM WINDOWS

Annotation: *The article addresses the issue of extending the range of technical arsenal of forensic divisions by developing a domestic software product in digital forensic field as part of the "Cybershield of Kazakhstan" state program [1].*

Keywords: *digital forensics, computer crimes, Cybershield of Kazakhstan, Cybersecurity concept, Digital Kazakhstan*

Аннотация: *В статье рассматривается вопрос о расширении технического арсенала криминалистических подразделений путем создания отечественного программного продукта в области "цифровой" криминалистики в рамках реализации государственной программы "Киберщит Казахстана" [1].*

Ключевые слова: *"цифровая" криминалистика, компьютерные преступления, Киберщит Казахстана, Концепция кибербезопасности, Цифровой Казахстан*

Повсеместное использование компьютерной техники обусловило увеличение количества принципиально нового вида преступности – киберпреступления, что наблюдается практически во всех развитых странах и наносит значительный ущерб их экономике и безопасности.

По статистическим данным интернет-ресурса Comss.ru (StatCounter, NetMarketShare, AdDuplex и Steam) на долю операционной системы Windows приходится 96,77% пользователей Интернета [2], в связи с чем данная система является основным объектом кибератак и инструментом киберпреступников, которые могут сохранить "цифровые следы" противоправной деятельности.

Одним из объектов исследования "цифровой" криминалистики являются файлы реестра операционной системы Windows, где хранятся различные сведения об учетных записях, загружаемых из сети файлах, подключенных USB-устройствах и прочая криминалистически значимая информация, которая должна быть зафиксирована, изъята и использована в качестве доказательной базы преступной деятельности злоумышленников с использованием средств компьютерных технологий [3].

В настоящее время, магистрантом 2 курса кафедры "Вычислительная техника и программное обеспечение" факультета "Компьютерных систем и профессионального образования" Казахского агротехнического университета имени Сакена Сейфуллина ведется научно-исследовательская работа по теме "Разработка программного обеспечения для криминалистического исследования реестра операционной системы Windows".

Разрабатываемый программный продукт может стать одним из первых отечественных инструментов, позволяющих быстро, достоверно и безопасно получить криминалистически значимую информацию из реестра операционной системы для дальнейшего документирования преступной деятельности. В дальнейшем программный продукт будет развиваться, расширять свой функционал и может использоваться экспертами Центра судебных экспертиз Министерства юстиции РК, а также специалистами-криминалистами специальных и правоохранительных органов Республики Казахстан в качестве бюджетного аналога дорогостоящих программ.

Ожидаемые результаты:

- простота реализации и быстрое действие отечественного программного продукта позволит сократить общее время проведения экспертно-криминалистических исследований "цифровых" доказательств;
- снижение финансовых затрат бюджетных организаций на приобретение, эксплуатацию и техническую поддержку отечественного программного продукта по сравнению с зарубежными аналогами;
- импортозамещение;
- повышение доверия государственными органами Республики Казахстан к отечественному программному продукту, соответствие всем требованиям информационной безопасности;
- создание условий для эффективной борьбы с киберпреступностью путем расширения арсенала технических средств фиксации и криминалистических исследований "цифровых" доказательств, что отражено в Концепции кибербезопасности (*Киберщит Казахстана*), утвержденной Постановлением Правительства Республики Казахстан от 30 июня 2017 года №407 [1];
- диверсификация национальной экономики путем дальнейшего развития программного продукта, повышения его конкурентоспособности и выхода на международный рынок, в соответствии с Государственной программой "Цифровой Казахстан" на 2017-2020 годы [4].

Список литературы

1. Постановление Правительства Республики Казахстан от 30 июня 2017 года №407 (Киберщит Казахстана).
2. [Электрон.ресурс] – URL(дата обращения 15.10.2018): Статья "Статистика использования операционных систем Windows 10, Windows 7, Windows XP в июле 2018 года. Аналитические данные от StatCounter, NetMarketShare, AdDuplex и Steam", <https://www.comss.ru/page.php?id=5244>.
3. [Электрон.ресурс] – URL(дата обращения 15.10.2018): Статья "Некоторые особенности судебно-экспертного исследования реестра Windows", Гортинский А.В., Мордвинкин М.М., <https://cyberleninka.ru/article/n/nekotorye-osobennosti-sudebno-ekspertnogo-issledovaniya-reestra-windows>.
4. Постановление Правительства Республики Казахстан от 12 декабря 2017 года №827 (Цифровой Казахстан).