Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники
Кафедра инженерной психологии и эргономики

На правах рукописи

УДК 004.415

Шевченко
Антон Олегович

ОБЕСПЕЧЕНИЕ НАДЕЖНОСТИ ЗАЩИТЫ ПОЛЬЗОВАТЕЛЬСКОЙ ИНФОРМАЦИИ: ИНЖЕНЕРНО-ПСИХОЛОГИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

Автореферат на соискание академической степени
магистра технических наук

1-23 80 08 – Психология труда, инженерная психология, эргономика

Магистрант А.О. Шевченко

Научный руководитель
В.М. Бондарик, кандидат
технических наук, доцент

Заведующий кафедрой ИПиЭ
К.Д. Яшин, кандидат
технических наук, доцент

Минск 2019

КРАТКОЕ ВВЕДЕНИЕ

Прогресс подарил человечеству великое множество достижений, но тот же прогресс породил и массу проблем. Человеческий разум, разрешая одни проблемы, непременно сталкивается при этом с другими, новыми, и этот процесс обречен на бесконечность в своей последовательности. Хотя, если уж быть точным, новые проблемы - это всего лишь обновленная форма старых. Вечная проблема - защита информации. На различных этапах своего развития человечество решало эту проблему с присущей для данной эпохи характерностью. Изобретение компьютера и дальнейшее бурное развитие информационных технологий во второй половине 20 века сделали проблему защиты информации настолько актуальной и острой, насколько актуальна сегодня информатизация для всего общества.

Главная тенденция, характеризующая развитие современных информационных технологий - рост числа компьютерных преступлений и связанных с ними хищений конфиденциальной и иной информации, а также материальных потерь. По результатам одного исследования, посвященного вопросам компьютерных преступлений, около 58% опрошенных пострадали от компьютерных взломов за последние 12 месяцев. Примерно 18 % опрошенных из этого числа заявляют, что потеряли более миллиона долларов в ходе нападений, более 66 процентов потерпели убытки в размере 50 тыс. долларов. Свыше 22% атак были нацелены на промышленные секреты или документы, представляющие интерес прежде всего для конкурентов.

Сегодня, наверное, никто не сможет с уверенностью назвать точную цифру суммарных потерь от компьютерных преступлений, связанных с несанкционированным доступом к информации. Это объясняется, прежде всего, нежеланием пострадавших компаний обнародовать информацию о своих потерях, а также тем, что не всегда потери от хищения информации можно точно оценить в денежном эквиваленте. Однако по данным, опубликованным в сети Internet, общие потери от несанкционированного доступа к информации в компьютерных системах в 1997 году оценивались в 20 миллионов долларов, а уже в 1998 года в 53,6 миллионов долларов.

Причин активизации компьютерных преступлений и связанных с ними финансовых потерь достаточно много, существенными из них являются:

– переход от традиционной "бумажной" технологии хранения и передачи сведений на электронную и недостаточное при этом развитие технологии защиты информации в таких технологиях;

– объединение вычислительных систем, создание глобальных сетей и расширение доступа к информационным ресурсам;

– увеличение сложности программных средств и связанное с этим уменьшение их надежности и увеличением числа уязвимостей.

Современные методы обработки, передачи и накопления информации способствовали появлению угроз, связанных с возможностью потери, искажения и раскрытия данных, адресованных или принадлежащих конечным пользователям. Поэтому обеспечение информационной безопасности компьютерных систем и сетей является одним из ведущих направлений развития ИТ.

Защита информации — это деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Объект защиты — информация, носитель информации или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации.

Цель защиты информации — это желаемый результат защиты информации. Целью защиты информации может быть предотвращение ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации и/или несанкционированного и непреднамеренного воздействия на информацию.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Объектом исследования данной научной работы является защита пользовательских данных на локальных и сетевых системах.

Предметом исследования выступают инженерно-психологические методы защиты пользовательской информации.

Цель данной работы: разработка программного средства защиты пользовательских данных с использованием современных инженерно-психологических средств разработки.

В качестве задач исследования можно выделить:

– аналитический обзор литературы на выбранную тематику;

– изучение мировых практик и наработок в области защиты информации;

– анализ существующих методов для защиты информации;

– выделение и изучение основных теоретических сведений по выбранной тематике;

– разработка программного обеспечения, способного значительно повысить криптозащиту личной информации.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Магистерская диссертация состоит из трех основных разделов (глав):

– обзор литературы;
– теоретический раздел;
– экспериментальный раздел.

В первом разделе (глава 1) проводится анализ предметной области, изучается и анализируется тема в различных источниках информации.

При анализе литературы важное значение отводится классификации угроз, связанными с использованием современных технологий и технических средств манипулирования данными, пользовательской информацией. Кроме того, приводятся возможные способы защиты информации и непосредственно необходимое нам программное шифрование данных. Приводится краткое содержание литературных и интернет-источников, проводится их анализ.

В конце раздела мы выделили пару наиболее популярных аналогов разрабатываемого программного средства. Рассмотрели достоинства и недостатки представленных программ. Сделали анализ и выявили положительные аспекты разрабатываемого программного средства в сравнении с аналогами.

Во втором разделе (глава 2) производится теоретическая подготовка, необходимая для реализации всех требований, поставленных в качестве целей написания магистерской диссертации.

В начале раздела проводится анализ требований к программному средству. Мною был составлен список наиболее важных требований, предъявляемых к разрабатываемому программному средству. При составлении этого списка я учитывал анализ литературы, проведенный в предыдущем разделе и в частности анализ аналогов программы.

Далее в разделе описывается выбор технических средств для реализации поставленных целей и задач, а именно среда разработки, язык и прочее. Мною была разработана информационная модель системы, где были описаны основные алгоритмы шифрования, используемые в данной программе.

В конце раздела описывается архитектура разрабатываемого программного средства.

В третьем разделе (глава 3) приводится практическая реализация поставленных целей и задач.

В начале подробно описываются алгоритмы шифрования, необходимые для реализации программного средства. Приводится схематическое описание

алгоритмов шифрования AES, DES, RSA. Приводится упрощенная схема работы приложения, описываются разработанные классы.

В следующем подразделе приводится таблица тестирования. Мною были составлены действия пользователя, необходимые для проверки. По результатам тестирования программное средство было отлажено и готово к использованию.

В конце раздела описывается руководство пользователя. Пользователю описывается алгоритм использования программы с подробным описанием и скриншотами работы приложения.

ЗАКЛЮЧЕНИЕ

Во время работы над магистерской диссертацией мною были освоены мировые практики в области защиты информации, исследованы аналоги программных средств данной тематики, разобраны и проанализированы наиболее распространенные алгоритмы шифрования и дешифрования данных, детально проработана концепция моделируемого программного средства, составлена его структура и описана информационная модель.

Конечный программный продукт выполняет все поставленные цели. Программное средство выполняет шифрование и дешифрирование файлов, папок, дисков на локально компьютере и в сетевом хранилище современными проверенными алгоритмами шифрования. Данные алгоритмы и без особых доработок обладают высоким уровнем криптостойкости. В программном средстве реализованы несколько уровней использования данных алгоритмов в зависимости от необходимостей и возможностей технических средств пользователя.

Структура программы наиболее благоприятным образом упрощает взаимодействие с интерфейсом программы. Даже самым, далеким от программирования пользователям, будет в ней просто разобраться и использовать.

Программное средство соответствует всем современным наработкам и тенденциям в области создания программных продуктов и комплексов.

При проектировании программного средства я ориентировался на мировые передовые практики в области защиты информации. Использовал методы и способы реализации с соблюдением мировых инженерно-психологических критериев.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

[1-А] Шевченко А.О. Обеспечение надежности защиты пользовательской информации: инженерно-психологическое обеспечение // Материалы 55-й научной конференции студентов, магистрантов, аспирантов, УО «Белоруский государственный университет информатики и радиоэлектроники» Минск, БГУИР, 2019. С. 76.