Построение защищенной АСУТП на базе требований ФСТЭК России, введение дополнительных мер и средств защиты, проведение обучения персонала и т д, то есть провести намеренную работу по снижению риска.

Литература

1. Цапко Г.П., Вериго А.А., Каташев А.С. Анализ рисков безопасности автоматизированных систем управления технологическими процессами // Интернет-журнал «НАУКОВЕДЕНИЕ» Том 8, №5 (2016)

2. Астапчук В.А. Архитектура корпоративных информационных систем / В.А. Астапчук, П.В. Терещенко. – Новосибирск: НГТУ, 2015 - 75 с.

3. Дубинин Е.А. Оценка относительного ущерба безопасности информационной системы: монография / Е.А. Дубинин, Ф.Б. Тебуева, В.В. Копытов. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014 - 192 с.

4. Дятлов С.А. Информационно-сетевая регулирование: Монография / С.А. Дятлов, В.П. Марьяненко, Т.А. Селищева - М.: НИЦ ИНФРА-М, 2016 - 414 с.

5. Комплексная безопасность бизнеса в условиях экономической нестабильности: материалы науч.-практ. конф. / отв. ред. Е.В. Стельмашонок, С.Н. Максимов. – СПб.: Изд-во СПбГЭУ, 2014 – 151 с.

6. Малюк А.А. Теория защиты информации. - М.: Гор. линия-Телеком, 2012 – 184 с.

7. Прокопенко А.В. Синтез систем реального времени с гарантированной доступностью программно-информационных ресурсов: монография / А.В. Прокопенко, М.А. Русаков, Р.Ю. Царев. - Красноярск: Сиб. федер. ун-т, 2013-92 с.

А.А. Батаргалиев, К.Е. Климентьев, В.И. Соловьева

НАУЧНЫЕ И ТЕХНИЧЕСКИЕ АСПЕКТЫ ОРГАНИЗАЦИИ ОБУЧЕНИЯ ВОПРОСАМ ЗАЩИТЫ ИНФОРМАЦИИ

(Самарский университет)

Введение. Преподаватели кафедры ИСТ Самарского университета принимают участие в подготовке бакалавров, магистров и специалистов на разных специальностях ВУЗа, включая, например, 09.03.01 – Информатика и вычислительная техника и 10.05.03 – Информационная безопасность автоматизированных систем. Методическая поддержка курсов, посвященных вопросам защиты информации (см., например, работы [1,2,3,4]), требует проведения ряда предварительных исследований, имеющих самостоятельную научную и техническую ценность. Эти исследования, преимущественно, затрагивают ряд вопросов, связанных с «классической» криптографией, то есть, не актуальной с точки зрения практического применения, но содержащей ряд теоретических положений, знание которых важно при изучении «современной» криптографии.

Методическое обеспечение курсов организовано в виде лабораторного практикума, в рамках которого студентам предлагается выполнить ряд заданий – см. работы [2,3,4]. Подготовка индивидуальных заданий потребовала предварительного выполнения ряда исследовательских работ.

1. Изучение шифра простой замены. Имеется в виду «классический» шифр, основанный на подстановке элементов одного алфавита вместо элементов другого [1,6,8]. Способ дешифрования основан на частотном анализе зашифрованного текста с учетом статистических закономерностей, присущих тому или иному естественному языку. Например, в русском языке наиболее часто встречается буква «О», потом следуют «Е», «А», «И» и т.д (см. [8]). Знание этого обстоятельства позволяет легко автоматизировать процесс дешифрования достаточно длинных текстов (порядка 1500-2000 знаков и более). Однако на «коротких» текстах статистические закономерности практически не проявляются.

1.1. Задача поиска коротких фраз. Отсюда вытекает первая задача исследования: найти короткие текстовые фразы (длиной не более 100 знаков), для которых статистические закономерности выполняются хотя бы частично (например, для нескольких наиболее частых букв – «О», «Е», «А». «И», «Н», «Т»). В ходе решения этой задачи К.Климентьевым было создано соответствующее программное обеспечение и просканированы многочисленные тексты различных авторов с литературных порталов www.samlib.ru и www.proza.ru (всего около 10000 текстов общим объемом порядка 3 млрд. знаков). В результате найдено всего лишь около 300 очень редких фраз, для которых выполняется сформулированное выше условие. Дешифрование именно этих фраз, закодированных случайно выбранными ключевыми подстановками, предлагается в качестве индивидуальных заданий (см. работу [2]). Например, фраза «ТЕПЕРЬ МЫСЛЕННО ПЕРЕДВИГАЙСЯ ОТ КОПЧИКА ДО МАКУШКИ И ОБРАТНО» может быть закодирована как «UNBNWY J6C4N77P BNWNFHL1EXCM PU TPBDLTE FP JETIZTL L PQWEU7P», где 6 раз встречается буква «P» (вероятно, это «О»), 5 раз встречается буква «N» (вероятно, это «Е») и так далее.

По имеющейся информации, подобная работа никогда и никем ранее не проводилась.

1.2. Задача подбора слов. Тем не менее, знание 5-6 букв фразы не гарантирует ее дешифрования – требуются неформальные эвристические методы, аналогичные описанным в [7]. Частично автоматизировать применение этих методов помогает уникальное программное обеспечение, разработанное В.Соловьевой. Оно позволяет, применяя встроенный словарь, подбирать слова, соответствующие заданной маске, при этом текстовый контекст автоматически модифицируется в соответствии с каждой очередной «гипотезой» – см. рис. 1.

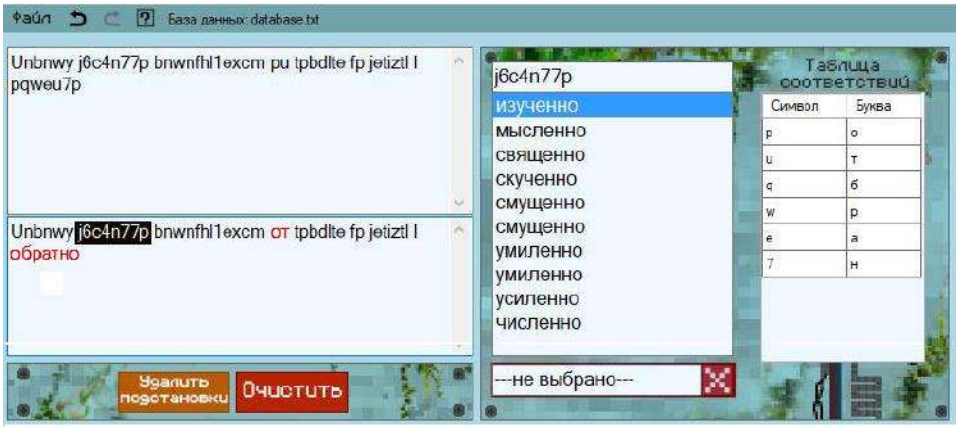

Рис. 1. Утилита подбора слов по маске

Например, маске «$_{3564}E_{77}O$» могут быть сопоставлены слова «ИЗУЧЕННО», «СВЯЩЕННО», «МЫСЛЕННО» и др., из которых «правильное» предлагается выбрать в соответствии с контекстом.

2. Изучение шифров Цезаря и Вижинера. Задача поиска «красивых» примеров. Имеются в виду шифры группы Тритемиуса, основанные на «сложении букв», а фактически – целых чисел в группе вычетов по модулю мощности алфавита [1,8]. Лабораторные работы предполагают как шифрование предложенных слов предложенным ключом, так и их дешифрование, то есть «взлом» без знания ключа [2]. При этом целесообразно использование не произвольных, но тщательно отобранных комбинаций «слово, ключ».

Таблица 1 – Примеры «красивых» сочетаний

Слово	ЗАИКА	БАТАТ	WOMAN	LADY	ДУБЬЁ	ПОМПОНЫ
Ключ	ЗАИКА	СЕЯТЬ	LABEL	WOLF	ММММММ	ДДДДДДД
Сумма	ПАСХА	ТЕСТО	HONEY	HOOD	РАНИТ	УТРУТСЯ

С этой целью К. Климентьевым был проведен поиск подходящих троек «слово, ключ, результат», в которых все три компонента представляли бы собой слова естественного языка. Поиск проведен для двух случаев: 1) нумерация букв 0..32; 2) нумерация букв 1..33. Были использованы словари русского (порядка 93 тыс. слов) и английского языков (порядка 11 тыс. слов) с сайта www.slovari.ru. В результате были получены около тысячи «красивых» сочетаний «слово, ключ, результат» (примеры – см. в табл. 1). Если исследования сочетаний для шифра Цезаря известны (они в лингвистике называются «транспозитами»), то никаких сведений по аналогичным работам для шифра Вижинера не имеется. Найденные «красивые» сочетания использованы в индивидуальных заданиях для лабораторных работ [2].

3. Изучение методов асимметричной криптографии. При изучении математических аспектов шифрования с открытым ключом и электронно-цифровых подписей необходимо использование «длинной арифметики» [5, 6]. А.Батаргалиевым разработан «калькулятор длинных чисел» (составленных из несколько сотен десятичных цифр), который также используется в лабораторном практикуме (см. рис. 2).

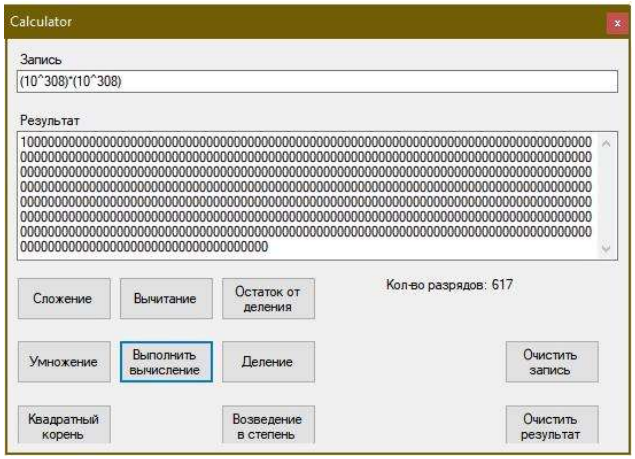

Рис. 2. Калькулятор длинных чисел

Развитием данной работы может служить расширение функционала калькулятора за счет операций «определение НОД двух длинных целых чисел», «определение мультипликативно-обратного в кольце вычетов по длинному модулю», «определение порядка элемента в кольце вычетов по длинному модулю», «поиск примитивных элементов в кольце вычетов по длинному модулю», «генерация длинных простых чисел», «доказательство или опровержение простоты длинного числа», «факторизация длинных чисел» и др. После указанной доработки «калькулятор длинных чисел» превратится в программное обеспечение, не имеющее аналогов.

Заключение. Таким образом, в процессе подготовки индивидуальных заданий для лабораторного практикума по курсу «Защита информации» создано уникальное программное обеспечение и получен ряд уникальных исследовательских результатов.

Литература

1. Климентьев К.Е. Введение в защиту компьютерной информации. – Самара: Изд–во Самар. ун-та, 2020.

2. Алгоритмы и методы классической криптографии / М–во образования и науки Рос. Федерации, Самар. нац. исслед. ун-т им. С. П. Королева (Самар. ун-т); сост. О.А. Заякин, К. Е. Климентьев. – Самара: Изд–во Самар. ун-та, 2017.

3. Практическое применение средств асимметричной криптографии / М–во образования и науки Рос. Федерации, Самар. нац. исслед. ун-т им. С. П. Королева (Самар. ун-т); сост. К. Е. Климентьев. – Самара: Изд–во Самар. ун-та, 2017.

4. Исследование разрушающих программных воздействий / М–во образования и науки Рос. Федерации, Самар. нац. исслед. ун-т им. С. П. Королева (Самар. ун-т); сост. К.Е. Климентьев. – Самара: Изд–во Самар. ун-та, 2017.

5. Домашев А.В., Грунтович М.М., Попов В.О. и др. Программирование алгоритмов защиты информации. – М.: Нолидж, 2002. – 416 с.

6. Введение в криптографию / Под ред. В.В.Ященко. – СПб.: Питер, 2001. – 288 с.

7. По Э. Золотой жук // В кн.: Американская новелла, М.: ГИХЛ. 1958. – С. 54-83.

8. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах. – М.: Горячая Линия-Телеком, 2001. – 148 с.

В.А. Белов, Д.В. Бобров, З.Ф. Камальдинова, А.А. Каштанов, В.С. Милов

КОНЦЕПЦИЯ СИСТЕМЫ ГАРАНТИРОВАННОЙ ИДЕНТИФИКАЦИИ ЛИЧНОСТИ ПОЛЬЗОВАТЕЛЯ В СЕТИ

(Самарский государственный технический университет)

Мы живём в том веке, когда новыми информационными технологиями никого не удивишь. Люди из разных уголков планеты свободно общаются между собой, при этом обмениваясь фотографиями или видеофайлами. Сейчас сложно представить, как мы будем жить без Интернета, ведь именно с его помощью все люди получают нужную для себя информацию.

Но чем больше мы полагаемся на Интернет, тем острее стоит вопрос защиты данных, которые мы туда вносим. Пароль для хакеров уже давно считается самым слабым местом. Такие простые методы как полный перебор (Брутфорс), перехват через открытую точку Wi-fi и банальное подглядывание дают злоумышленнику возможность с легкостью получить доступ к вашей конфиденциальной информации.

И именно поэтому следует разработать другие, более надежные, способы идентификации в сети.

Актуальность исследования. В эпоху бурно развивающихся информационных технологий и масштабности распространённости использования различных сервисов и служб, крайне важно развивать и совершенствовать системы защиты информации. Одной из важнейших задач теории защиты информации является идентификация пользователя в сети.

Данная проблема затрагивает каждого пользователя, так как каждый человек не хочет утечки собственных данных и для их защиты требуется выбрать наиболее рациональный и безопасный способ распознавания пользователя в сети. С каждым днем актуальность данной проблемы будет расти прямо пропорционально развитию информационных технологий.

Цель работы: провести исследования существующих способов идентификации пользователей в сети. Выбрать самый быстрый, эффективный и безопасный способ путем сравнения достоинств и недостатков каждого из метода.

Задачи, поставленные для достижения цели:

– изучить виды идентификации пользователей в сети;