**Лабораторная работа №1**

**Цель:** познакомиться с некоторыми аспектами защиты информации и повысить уровень

владения навыками поиска в Интернет.

**Задание 1.**

1. Шифр Атбаш — это метод шифрования, при котором буквы алфавита заменяются на противоположные по порядку. Например, буква "а" заменяется на "я", "б" на "ю" и так далее.

Шифр Цезаря — это метод шифрования, при котором каждая буква сообщения сдвигается на определенное количество позиций по алфавиту. Например, при сдвиге на 3 позиции буква "а" будет заменена на "г", "б" на "д" и так далее.

Шифр Скиталла — это метод шифрования, при котором буквы сообщения записываются в специальном порядке, например по спирали, затем считываются по строкам или столбцам.

1. Основной принцип Керкгоффса заключается в том, что система шифрования должна оставаться безопасной даже в том случае, если информация о способе шифрования становится общеизвестной, за исключением секретного ключа.
2. Первый советский компьютер назывался МЭСМ (Малая электронно-счетная машина) и был создан в 1950 году в Советском Союзе.
3. Перфокарта — это перфорированная бумажная карта, используемая в компьютерах и технике обработки информации. На перфокарте информация записывается в виде отверстий, пробиваемых в определенных позициях на карте. Перфокарты использовались для ввода данных в компьютеры до появления более современных устройств ввода информации, таких как клавиатуры и мыши.
4. Расширением файла называется часть имени файла, которая следует сразу после последней точки в имени файла. Расширение файла обычно указывает на тип или формат файла, позволяя операционной системе и программам определить, как обрабатывать этот файл. Например, у файла "document.docx" расширение файла - "docx", что указывает на то, что это файл в формате Microsoft Word.
5. К безопасному паролю предъявляются следующие требования:

1. Длина: Хороший пароль должен содержать не менее 8 символов.

2. Сложность: Пароль должен содержать комбинацию заглавных и строчных букв, цифр и специальных символов.

3. Непредсказуемость: Пароль не должен быть легко угадываемым на основе личных данных или распространенных шаблонов.

Рекомендации по составлению паролей:

- Используйте уникальные пароли для различных онлайн-сервисов.

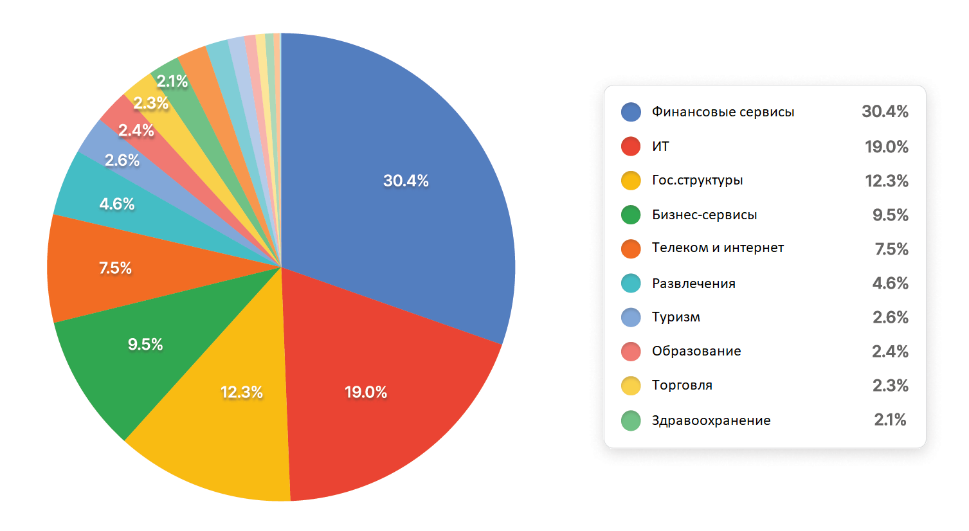
- Не используйте личные данные, такие как даты рождения или имена, в качестве пароля.

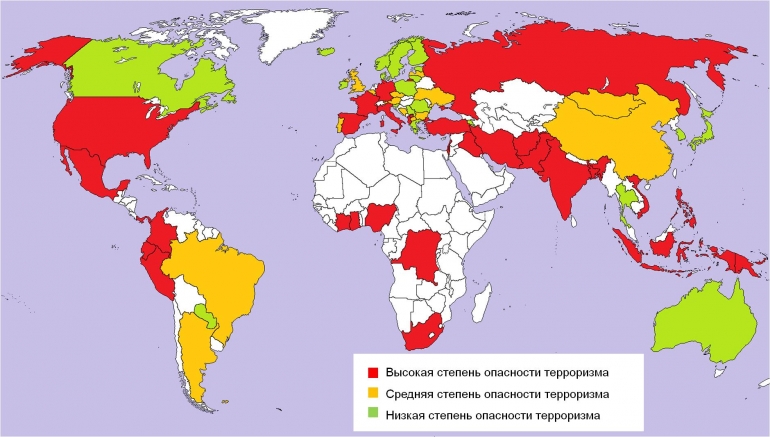
- Используйте фразы, которые легче запомнить, но сложны для угадывания, и добавьте к ним цифры и специальные символы.

- Регулярно меняйте пароли, особенно для важных аккаунтов.

- Используйте двухфакторную аутентификацию там, где это возможно, для дополнительного уровня защиты.

**Задание 2.**





Список “Топ веб-угроз” за последние сутки:

* [нарушение контроля доступа](https://skillbox.ru/media/code/owasp-top-10-samye-rasprostranyennye-uyazvimosti-vebprilozheniy/#stk-1);
* [недочёты криптографии](https://skillbox.ru/media/code/owasp-top-10-samye-rasprostranyennye-uyazvimosti-vebprilozheniy/#stk-2);
* [инъекции](https://skillbox.ru/media/code/owasp-top-10-samye-rasprostranyennye-uyazvimosti-vebprilozheniy/#stk-3);
* [небезопасный дизайн](https://skillbox.ru/media/code/owasp-top-10-samye-rasprostranyennye-uyazvimosti-vebprilozheniy/#stk-4);
* [небезопасная конфигурация](https://skillbox.ru/media/code/owasp-top-10-samye-rasprostranyennye-uyazvimosti-vebprilozheniy/#stk-5);
* [использование уязвимых или устаревших компонентов](https://skillbox.ru/media/code/owasp-top-10-samye-rasprostranyennye-uyazvimosti-vebprilozheniy/#stk-6);
* [ошибки идентификации и аутентификации](https://skillbox.ru/media/code/owasp-top-10-samye-rasprostranyennye-uyazvimosti-vebprilozheniy/#stk-7);
* [нарушения целостности программного обеспечения и данных](https://skillbox.ru/media/code/owasp-top-10-samye-rasprostranyennye-uyazvimosti-vebprilozheniy/#stk-8);
* [ошибки логирования и мониторинга безопасности](https://skillbox.ru/media/code/owasp-top-10-samye-rasprostranyennye-uyazvimosti-vebprilozheniy/#stk-9);
* [подделка запросов на стороне сервера](https://skillbox.ru/media/code/owasp-top-10-samye-rasprostranyennye-uyazvimosti-vebprilozheniy/#stk-10).

|  |  |
| --- | --- |
| Дата | Атака и средство атаки |
| 1982 год | Группа хакеров смогла установить троян в SCADA-систему, которая контролировала работу сибирского нефтепровода, что привело к мощному взрыву. |
| 1992 год | Рабочий нефтяной компании Chevron, который взломал компьютеры в офисах компании в Нью-Йорке и Сан-Хосе, отвечавшие за системы предупреждений, перенастроив их на аварию после запуска системы. |
| Август 1994 года | Лейн Джаррет Дэвис сумел взломать сеть Salt River Project, получив доступ к информации и удалив файлы из системы, отвечающей за мониторинг и подачу воды и электричества. |
| 10 марта 1997 года | Хакер проник в систему управления, используемую для коммуникаций системы контроля воздушного движения в Вустере (США, штат Массачусетс), вызвав сбой системы, которая отключила телефонную связь на шесть часов. |
| 1999 год | Хакеры нарушили работу систем безопасности российского энергетического гиганта — компании «Газпром». С помощью инсайдера они использовали троян, чтобы иметь возможность управлять SCADA- системой, контролирующей подачу газа. |
| 2000 год | Бывший сотрудник Maroochy Water System (Австралия) взломал системы управления водоснабжением, в результате чего миллионы литров сточных вод попали в ближайшую реку, что привело также к затоплению местной гостиницы. |
| Декабрь 2002 года | Нефтяная компания PDVSA из Венесуэлы подверглась атаке, в результате которой добыча нефти сократилась с 3 млн. до 370 тыс. баррелей в сутки. Во время атаки было взломано несколько корпоративных компьютеров. |
| 2006 год | Два инженера по организации дорожного движения в Лос-Анджелесе взломали городские светофоры в знак протеста. Им удалось изменить программу работы некоторых светофоров, размещенных на важных участках, после чего они стали гореть красным цветом, что привело к серьезным пробкам. |
| 2008 год | 14-летний студент взломал системы трамвайной сети в польском городе Лодзь, в результате чего 4 трамвая сошли с путей, а 12 человек получили травмы. Студент создал инфракрасный пульт дистанционного управления, как у телевизоров, с помощью которого он смог контролировать трамвайные перекрестки. |

**Задание 4.**



Клод Шеннон (1916-2001) — американский математик, инженер и ученый в области теории информации. Он известен своими работами в области цифровой коммуникации и криптографии.

Пять основных событий в биографии Клода Шеннона:

1. 1937 — Получил степень бакалавра по математике в Мичиганском университете.

2. 1940 — Закончил аспирантуру в Массачусетском технологическом институте, защитил докторскую диссертацию "Математическая теория связи", считается основоположником теории информации.

3. 1948 — Опубликовал статью "A Mathematical Theory of Communication" ("Математическая теория коммуникации"), в которой он описал основы цифровой коммуникации и криптографии.

4. 1949 — Стал профессором Массачусетского технологического института.

5. 1956 — Опубликовал работу "The Bandwagon", в которой представил идею "аналогового компьютера".

Работа, посвященная секретной передаче информации: "Математическая теория коммуникации" (A Mathematical Theory of Communication).

**Задание 5.**

Хорст Фейстель (1915–1990) – немецкий криптограф и инженер, известный своими работами в области криптографии и разработкой симметричного шифрования.

Пять основных событий в биографии Хорста Фейстеля:

1. Родился 30 января 1915 года в Дуйсбурге, Германия.

2. Во время Второй мировой войны работал в Германском институте шифрования, где участвовал в разработке криптографических систем.

3. После войны переехал в Соединенные Штаты Америки, где начал работать в компании IBM.

4. В 1971 году разработал структуру заменяющих сетей, которая стала основой для создания шифра DES (Data Encryption Standard) – одного из самых известных алгоритмов шифрования.

5. Ушел на пенсию в 1986 году, но оставался активным в области криптографии до своей смерти в 1990 году.

В области криптографии основным его вкладом стала разработка структуры заменяющих сетей, которая стала одним из основных компонентов шифра DES и оказала значительное влияние на развитие современных криптографических систем.

**Задание 6.**

"Кодирование" — это процесс преобразования данных из одной формы представления в другую, более удобную для передачи, обработки или хранения. Кодирование может быть использовано для сжатия данных, обеспечения целостности или защиты информации.

"Шифрование" — это процесс преобразования данных с использованием алгоритма шифрования, с целью сделать их непонятными для неавторизованных лиц. Шифрование обычно используется для обеспечения конфиденциальности и безопасности информации.

Отличие между этими понятиями заключается в целях и методах их применения. Кодирование направлено на преобразование данных с целью улучшения их представления, в то время как шифрование используется для обеспечения конфиденциальности и защиты информации от несанкционированного доступа.