

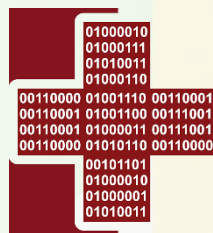


ИНСТИТУТ ПО МАТЕМАТИКА И ИНФОРМАТИКА
БЪЛГАРСКА АКАДЕМИЯ НА НАУКИТЕ



ДИНАМИЧНА МАТЕМАТИКА В ОБРАЗОВАНИЕТО

**ПОВИШАВАНЕ НА ДИГИТАЛНАТА КУЛТУРА И
ОТГОВОРНОСТИТЕ НА УЧЕНИЦИТЕ В
КИБЕР ПРОСТРАНСТВОТО ЧРЕЗ ОСИГУРЯВАНЕ НА
ЗАЩИТЕНА СРЕДА ЗА ОБУЧЕНИЕ**



ДИМИТРИНА ПОЛИМИРОВА

**НАЦИОНАЛНА ЛАБОРАТОРИЯ ПО
КОМПЮТЪРНА ВИРУСОЛОГИЯ ПРИ БАН**

15 февруари 2020 г., София, ИМИ – БАН





1. КРАТКО ПРЕДСТАВЯНЕ НА ЛАБОРАТОРИЯТА

- Кратка информация
- Научно-изследователска дейност
- Експертна дейност
- В помощ на обществото
- Обучение

ЗА ЛАБОРАТОРИЯТА



1990

• ГОДИНА НА ОСНОВАВАНЕ



13

• СЛУЖИТЕЛИ



3

• НЕЗАВИСИМИ МРЕЖИ



10

• ТЕСТОВИ РАБОТНИ МЕСТА



98%

• СОБСТВЕНИ ПРИХОДИ



60+

• ВЪЗЛОЖЕНИ ПОРЪЧКИ



300+

• ИЗНЕСЕНИ ЛЕКЦИИ



200+

• БЕЗПЛАТНИ УСЛУГИ

НАУЧНО-ИЗСЛЕДОВАТЕЛСКА ДЕЙНОСТ

Методи и средства за анализ и оценка на малуеър

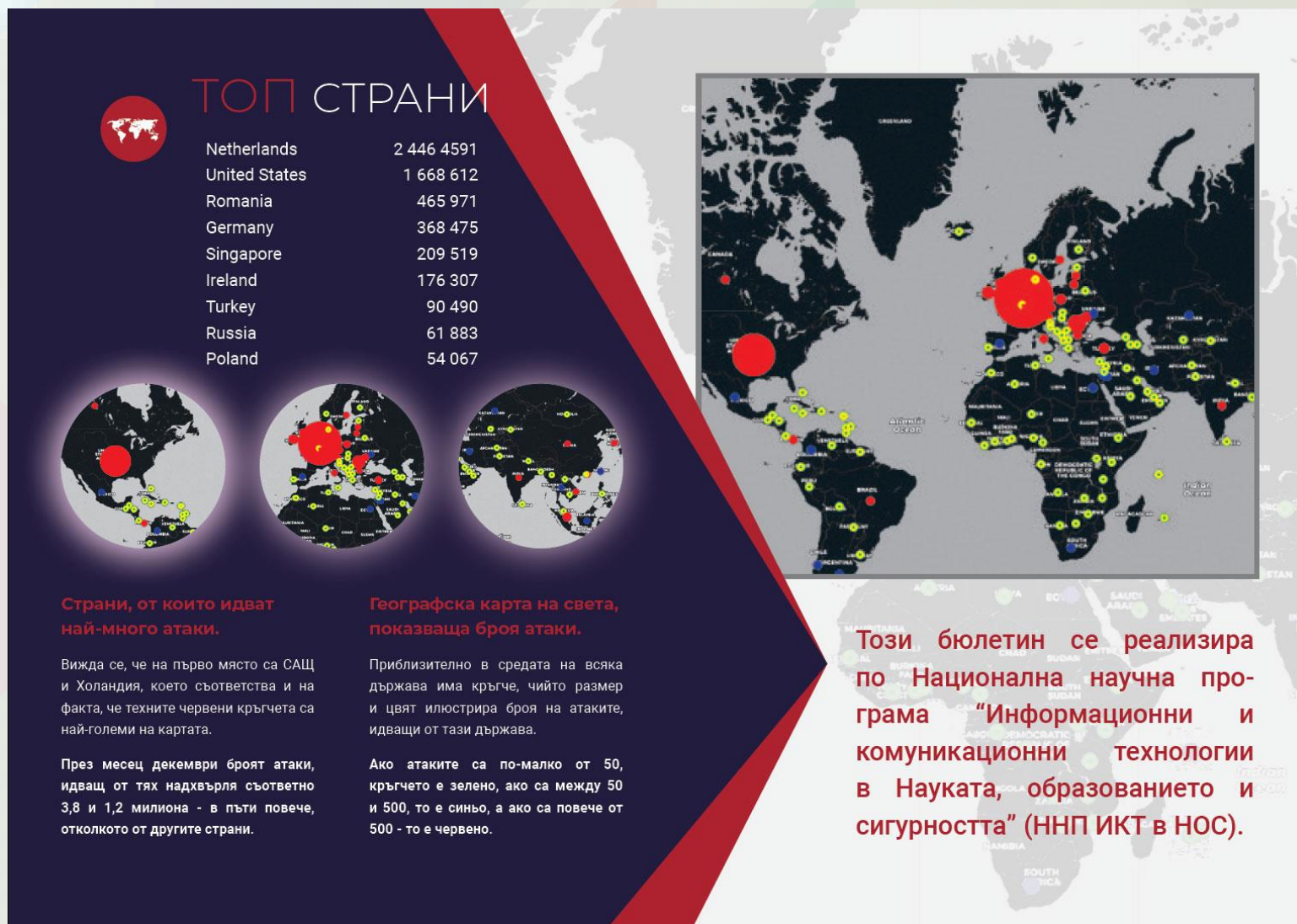
Създаване и актуализиране на вече съществуващи бази от данни за малуеър

Създаване и изследване на методи за компютърна сигурност и АВ защита

Изследване и класификация на нови компютърни вредителски програми

Методи и средства за откриване и отстраняване на малуеър

Методи и средства за възстановяване на данни



АНАЛИЗ И ОЦЕНКА НА:

- компютърна сигурност в мрежова среда;
- source code (в уеб страници, бази от данни);
- системни регистри;

ОПРЕДЕЛЯНЕ НА ПРОЦЕДУРИ ЗА КОМУНИКАЦИОННА СИГУРНОСТ НА КОМУНИКАЦИОННО ОБОРУДВАНЕ

ОЦЕНКА НА:

- заплахите в SQL базирани приложения;
- възможностите за проникване в защитени мрежи;

АНАЛИЗ НА ЗЛОНАМЕРЕН СОФТУЕР И ЗЛОНАМЕРЕНИ АТАКИ В УЕБ ПРИЛОЖЕНИЯ.

СКАНИРАНЕ ЗА УЯЗВИМОСТИ

СИСТЕМНИ ПОЛИТИКИ ЗА СИГУРНОСТ

ОТКРИВАНЕ НА АНОМАЛИИ

ЕЖЕДНЕВНИ НУЖДИ

- Проектиране, изграждане и конфигуриране на мрежи, сървъри, защитни стени

ПРОЕКТИРАНЕ, ИЗГРАЖДАНЕ И ВНЕДРЯВАНЕ НА УЕБ-БАЗИРАНИ СИСТЕМИ ЗА:

- управление на йерархично структурирани данни
- отдалечено управление на машини и инсталации
- мониторинг и анализ на движещи се обекти и др.

В ПОМОЩ НА ОБЩЕСТВОТО



- Консултации



- Обучение



- Диагностика и профилактика



- Възстановяване на данни и системи



- Публични лекции



- Публикуване на описания на текущи вредителски програми

ОБУЧЕНИЕ

В ОБЛАСТА НА КОМПЮТЪРНАТА, ИНФОРМАЦИОННА И
КИБЕР СИГУРНОСТ

НАЦИОНАЛНИ ИНСТИТУЦИИ И ОРГАНИЗАЦИИ

ЛЕКЦИИ В УНИВЕРСИТЕТИ

ПОДГОТОВКА НА ДИПЛОМАНТИ И ДОКТОРАНТИ

ОБУЧЕНИЕ НА УЧЕНИЦИ И УЧИТЕЛИ

2. ОБУЧЕНИЕТО ПО КИБЕРСИГУРНОСТ

- Необходимост или задължение
- Форми на обучение
- Осигуряване на защитена среда за обучение
- Очаквани резултати

Обща отговорност

- Действия, свързани с кибер осведомеността

Защита и сигурност

- Информационни системи
- Комуникационни системи

Основни участници в кибер сигурността:

- Правителствени организации
- Бизнес
- Крайни потребители

Увеличаване на кибер атаките

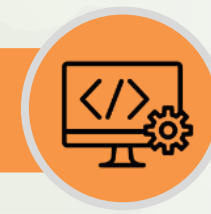
- Като честота
- Като тежест по отношение на нанесени щети



Човешки
уязвимости



Софтуерни
уязвимости



КИБЕР
ЗАЩИТА

КИБЕР
ОСВЕДОМЕНОСТ

КИБЕР
УСТОЙЧИВОСТ

КИБЕР СИГУРНОСТ



ФОРМИ НА ОБУЧЕНИЕ



ОСИГУРЯВАНЕ НА ЗАЩИТЕНА СРЕДА ЗА ОБУЧЕНИЕ

КАК ДА ХАКНЕМ ТЕЛЕФОН?

01

Как да създадем Троянски кон?

- Какво представлява Троянският кон?
- Вектори на атака

02

Съвети за създаване

- Свалете програмата от следния адрес ...
- Използвайте следните опции ...

03

Инсталирайте на мишената

- Техники за инсталиране
- Използвайте незнанието на хората

04

Команди за атака/шпионаж

- Списък команди, които да използвате за слеждане и тяхното значение

КАК ДА ЗАЩИТИМ ТЕЛЕФОН?

01

Как да разпознаем Троянски кон?

- Какво представлява Троянския кон?
- Вектори на разпространение

02

Какво трябва да знаем

- Представя се за добра програма
- Позволени места за достъп на програмата

03

Защита от инсталиране

- Техники за защита от неправомерно инсталиране на програми в телефона

04

Настройки за защита на телефон

- Активирайте следните настройки
- Деактивирайте следните възможности ...

3. ПРЕДЛАГАНИ ТЕМИ ЗА ОБУЧЕНИЕ

- Вредителски програми (malware)
- Въведение в киберсигурността
- Заплахи в киберпространството
- Киберпрестъпления
- Анализ, почистване и възстановяване на компютърни системи

ВРЕДИТЕЛСКИ ПРОГРАМИ (MALWARE)

05

04

03

02

01

Курсът обхваща теми, засягащи основни видове вредителски програми и техники за анализ, почистване и възстановяване на заразени компютърни системи.

След приключване на курса участниците ще:

- разпознават различните видове вредителски програми;
- разбират опасностите, които се крият в кибер пространството както и отговорностите на крайния потребител;

ВРЕДИТЕЛСКИ ПРОГРАМИ (MALWARE)

01

Курсът обхваща теми, засягащи основни видове вредителски програми и техники за анализ, почистване и възстановяване на заразени компютърни системи.

02

03

04

05

ВЪВЕДЕНИЕ В КИБЕРСИГУРНОСТТА

ВРЕДИТЕЛСКИ ПРОГРАМИ (MALWARE)

05

04

03

02

01

Курсът е насочен към овладяване на знания, умения и отношения, свързани с изграждане на начална дигиталната грамотност на учениците по отношение на киберсигурността.

След завършването на този курс учениците би следвало да могат:

- да разпознават потенциалните атаки към компютри, системи и мрежи и участниците, които биха могли да ги изпълнят;
- да знаят инструментите и методите за киберзащита и да ги прилагат при подготовка на система за предотвратяване на атаки;
- да предприемат подходящи мерки в случай на пробив в системата;
- да анализират често срещаните грешки в сигурността.

ВЪВЕДЕНИЕ В КИБЕРСИГУРНОСТТА

ВРЕДИТЕЛСКИ ПРОГРАМИ (MALWARE)

05

04

03

02

01

Курсът е насочен към овладяване на знания, умения и отношения, свързани с изграждане на начална дигиталната грамотност на учениците по отношение на киберсигурността.

Курсът обхваща теми, засягащи основни видове вредителски програми и техники за анализ, почистване и възстановяване на заразени компютърни системи.

ЗАПЛАХИ В КИБЕРПРОСТРАНСТВОТО

ВЪВЕДЕНИЕ В КИБЕРСИГУРНОСТТА

ВРЕДИТЕЛСКИ ПРОГРАМИ (MALWARE)

05

04

03

02

01

Целта курса „Заплахи в киберпространството“ е да запознае учениците с видовете заплахи, които могат да присъстват в киберпространството, както и с начините за противодействие.

След завършването на този курс учениците би следвало да могат:

- да идентифицират лошите участници в киберпространството и да сравняват техните ресурси, прилагани техники и мотивация;
- да описват различни видове атаки и техните характеристики;
- да анализират често срещаните грешки в сигурността и да идентифицират конкретни принципи на проектиране, които са нарушени.

ЗАПЛАХИ В КИБЕРПРОСТРАНСТВОТО

ВЪВЕДЕНИЕ В КИБЕРСИГУРНОСТТА

ВРЕДИТЕЛСКИ ПРОГРАМИ (MALWARE)

05

04

03

02

01

Целта курса „Заплахи в киберпространството“ е да запознае учениците с видовете заплахи, които могат да присъстват в киберпространството, както и с начините за противодействие.

Курсът е насочен към овладяване на знания, умения и отношения, свързани с изграждане на начална дигиталната грамотност на учениците по отношение на киберсикурността.

Курсът обхваща теми, засягащи основни видове вредителски програми и техники за анализ, почистване и възстановяване на заразени компютърни системи.

КИБЕРПРЕСТЪПЛЕНИЯ

ЗАПЛАХИ В КИБЕРПРОСТРАНСТВОТО

ВЪВЕДЕНИЕ В КИБЕРСИГУРНОСТТА

ВРЕДИТЕЛСКИ ПРОГРАМИ (MALWARE)

05

04

03

02

01

Целта на курса е да даде на учениците разбиране за киберпрестъпленията и други злоупотреби, възникващи в кибер среда.

След завършването на курса учениците трябва:

- да знаят как интернет се използва за киберпрестъпност, кибер-дебнене и други злоупотреби;
- да могат да оценяват ефективността на приложенията на киберсигурността за предотвратяване на престъпления и злоупотреби.

КИБЕРПРЕСТЪПЛЕНИЯ

ЗАПЛАХИ В КИБЕРПРОСТРАНСТВОТО

ВЪВЕДЕНИЕ В КИБЕРСИГУРНОСТТА

ВРЕДИТЕЛСКИ ПРОГРАМИ (MALWARE)

05

04

03

02

01

Целта на курса е да даде на учениците разбиране за киберпрестъпленията и други злоупотреби, възникващи в кибер среда.

Целта курса „Заплахи в киберпространството“ е да запознае учениците с видовете заплахи, които могат да присъстват в киберпространството, както и с начините за противодействие.

Курсът е насочен към овладяване на знания, умения и отношения, свързани с изграждане на начална дигиталната грамотност на учениците по отношение на киберсигурността.

Курсът обхваща теми, засягащи основни видове вредителски програми и техники за анализ, почистване и възстановяване на заразени компютърни системи.

АНАЛИЗ, ПОЧИСТВАНЕ И ВЪЗСТА-
НОВЯВАНЕ НА КОМПЮТЪРНИ СИСТЕМИ

КИБЕРПРЕСТЪПЛЕНИЯ

ЗАПЛАХИ В КИБЕРПРОСТРАНСТВОТО

ВЪВЕДЕНИЕ В КИБЕРСИГУРНОСТТА

ВРЕДИТЕЛСКИ ПРОГРАМИ (MALWARE)

05

04

03

02

01

Курсът обхваща теми, засягащи техники за анализ, почистване и възстановяване на заразени компютърни системи.

Основната цел на курса е да се изградят базови компетентности за анализ, почистване и възстановяване на заразени компютърни системи.

След приключване на курса участниците ще:

- могат да анализират състоянието на компютърни системи и да разпознават наличието на вредителска програма в тях;
- знаят основни техники при почистване и възстановяване на заразени компютърни системи.

АНАЛИЗ, ПОЧИСТВАНЕ И ВЪЗСТА-
НОВЯВАНЕ НА КОМПЮТЪРНИ СИСТЕМИ

КИБЕРПРЕСТЪПЛЕНИЯ

ЗАПЛАХИ В КИБЕРПРОСТРАНСТВОТО

ВЪВЕДЕНИЕ В КИБЕРСИГУРНОСТТА

ВРЕДИТЕЛСКИ ПРОГРАМИ (MALWARE)

05

04

03

02

01

Курсът обхваща теми, засягащи техники за анализ, почистване и възстановяване на заразени компютърни системи.
Основната цел на курса е да се изградят базови компетентности за анализ, почистване и възстановяване на заразени компютърни системи.

Целта на курса е да даде на учениците разбиране за киберпрестъпленията и други злоупотреби, възникващи в кибер среда.

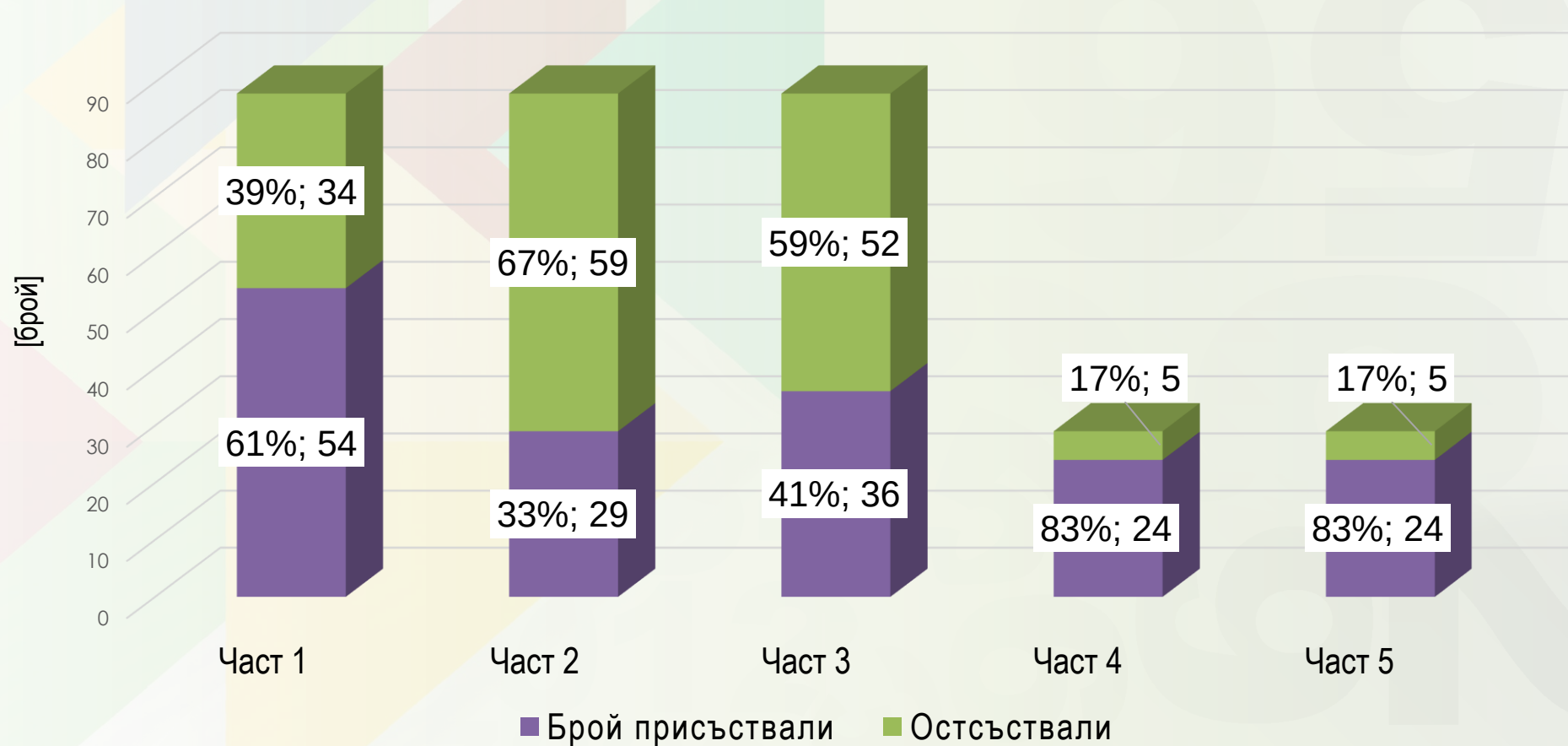
Целта курса „Заплахи в киберпространството“ е да запознае учениците с видовете заплахи, които могат да присъстват в киберпространството, както и с начините за противодействие.

Курсът е насочен към овладяване на знания, умения и отношения, свързани с изграждане на начална дигиталната грамотност на учениците по отношение на киберсигурността.

Курсът обхваща теми, засягащи основни видове вредителски програми и техники за анализ, почистване и възстановяване на заразени компютърни системи.

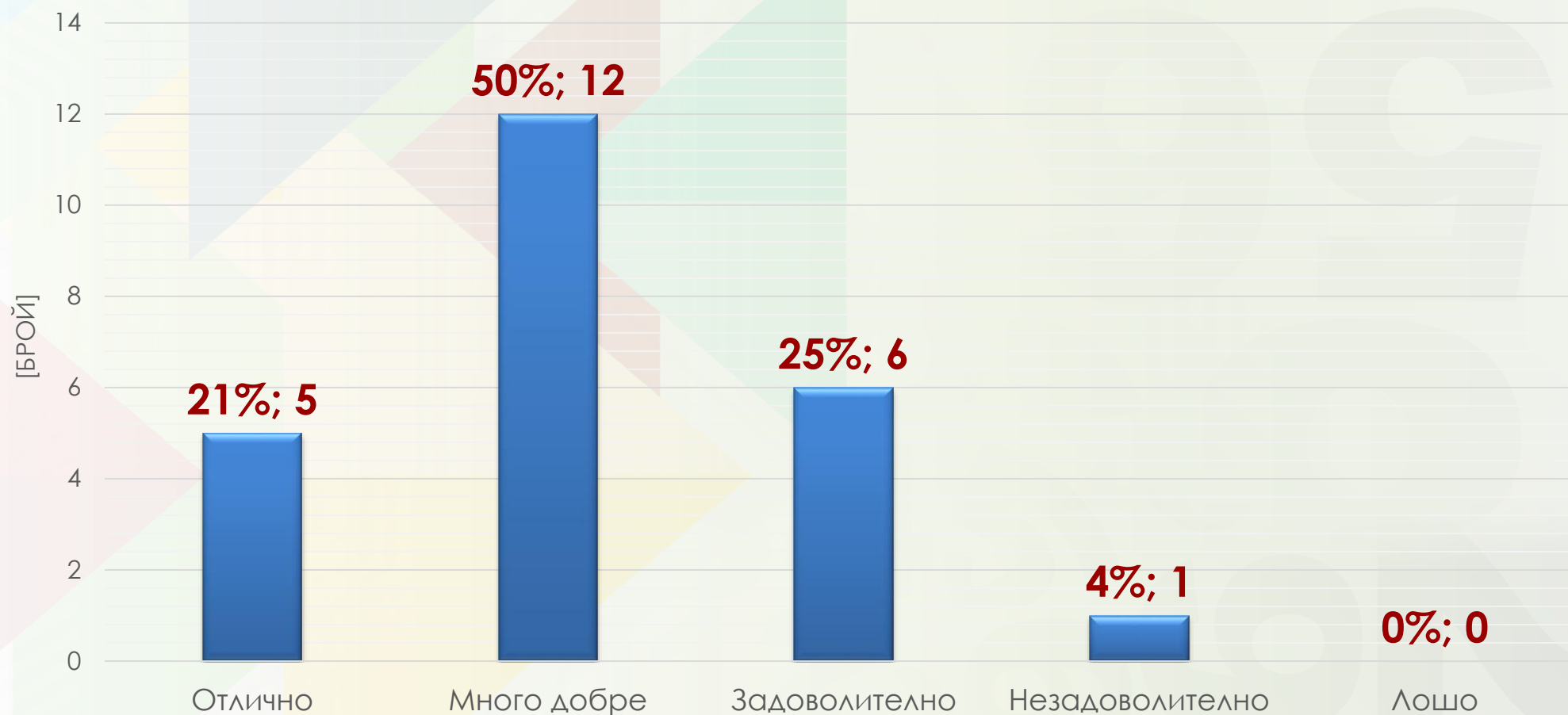
4. РЕЗУЛТАТИ ОТ ПРОВЕДЕНИ ОБУЧЕНИЯ

ПРОЦЕНТНОТО СЪОТНОШЕНИЕ И БРОЙ ПРИСЪСТВАЛИ СПРЯМО РЕГИСТРИРАНИ УЧАСТНИЦИ



30

ПОЛУЧЕНИ ОЦЕНКИ



ОБУЧЕНИЕ, НАСОЧЕНО В ПОСОКА НА ПРЕВЕНЦИЯ И ЗАЩИТА

Правни аспекти



- Универсална стратегия за разрешаване: необходимо е да има доказано причинени щети, да има законен ищец и ответник, който може да бъде посочен.
- Обществото не гледа с необходимата сериозност на този проблем.

Етични аспекти



- Това е високо интелектуална творческа дейност, присъща на определени групи високообразовани потребители в модерното информационно общество.

Социални аспекти



- Конфликтите, които се пораждаат между групата на информационно компетентните, и останалите, които нямат тези информационни умения и имат много по-различна оценка за проблемите.
- Конфликт между поколенията.



БЛАГОДАРЯ ЗА ВНИМАНИЕТО!

ДОЦ. Д-Р ДИМИТРИНА ПОЛИМИРОВА

ДИРЕКТОР НА

НАЦИОНАЛНА ЛАБОРАТОРИЯ ПО
КОМПЮТЪРНА ВИРУСОЛОГИЯ – БАН

НАЦИОНАЛНА ЛАБОРАТОРИЯ ПО КОМПЮТЪРНА ВИРУСОЛОГИЯ – БАН

София 1113, ул. „АКАД. ГЕОРГИ БОНЧЕВ“, БЛОК 8, ОФИС 104

ТЕЛ.: (359 2) 973 33 98

E-MAIL: DIMITRINA.POLIMIROVA@NLCV.BAS.BG

URL: [HTTP://WWW.NLCV.BAS.BG](http://WWW.NLCV.BAS.BG)