МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2017
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2017
Proceedings of the Forty-sixth Spring Conference
of the Union of Bulgarian Mathematicians
Borovets, April 9–13, 2017

НОВА ОБРАЗОВАТЕЛНА ИНИЦИАТИВА ЗА ИЗГРАЖДАНЕ НА ДИГИТАЛНИ КОМПЕТЕНТНОСТИ ПО КОМПЮТЪРНА И ИНФОРМАЦИОННА СИГУРНОСТ

Димитрина Полимирова

Въпросите и проблемите, свързани със защита и сигурност на информационните и комуникационните системи, е от изключително важно значение. През последните години експерти и политици изразиха нарастваща загриженост за защита на тези системи от кибератаки, за които се очаква да се увеличат не само като честота, но и като тежест по отношение на нанесени щети през следващите години. Основните участници в киберсигурността са правителствени организации, бизнесът и крайните потребители, които предприемат специфични мерки за повишаването ѝ. Обща отговорност обаче и на трите типа участници са действия, свързани с киберосведомеността.

В настоящата статия са представени идеите при проектирането на курс „Компютърна и информационна сигурност“, насочен към изграждане на базови знания за вредителските програми и получаване на компетентности за анализ, почистване и възстановяване на заразени компютърни системи. Споделени са впечатления от пилотния експеримент, проведен в Националната лаборатория по компютърна вирусология при БАН и Института по математика и информатика при БАН, с участници от Софийската профилирана гимназия по електроника „Джон Атанасов“.

1. Въведение. През последните години сме свидетели на бурното развитие на опасностите в киберпространството. Същността на кибератаките се заключава в манипулиране на информационната среда, което включва операционната система, приложенията, мрежовите протоколи, транспортните протоколи, протоколите за процедурите за сигурност и др. по такъв начин, че се променя идентичността на отделния потребител, компютър, система или мрежа, заблуждава се насрещната страна за правомерността на определени действия, извличат се по нерегламентиран начин данни, чието използване носи преки финансови или морални загуби на физически или юридически субекти, преодолявайки регионални, национални или глобални граници [1], [2].

Бурното развитие и нарастване на кибератаките върви успоредно и с развитието на методите и средствата за превенция, защита и възстановяване на компютри, системи и мрежи. Това е постоянен процес на натрупване на знания и опит, тъй като съвременната информационна и комуникационна индустрия се развива непрекъснато. Технологията е повсеместна и все по-неразделна част от почти всеки аспект

на съвременното информационно общество, в което устройствата и компонентите обикновено са взаимосвързани и прекъсването или модифицирането (правомерни или не) на едно, може да се отрази на много други. Затова въпросите и проблемите, свързани със защитата и сигурността на информационните и комуникационните системи, е от изключително важно значение.

Днес злонамереното мислене и злонамерените действия не се фокусират само върху уязвимостите, намерени в софтуера. Много по-опасни и ефективни са човешките уязвимости. За разлика, обаче, от софтуерните уязвимости, човешките не могат просто да бъдат „закърпени“ чрез сваляне на „кръпка“ от интернет. Едно от решенията в тази посока е да се работи по осведомяването и обучението на хората по въпросите за киберсигурността, киберзащитата и киберустойчивостта. Процесите за осведомяване и обучение трябва да бъдат не само на хората, работещи в ИТ индустрията, но и извън нея, независимо от професия, социално положение, образование, възрастова група и т.н.

Най-трайни резултати дава обучението в училищна възраст, когато се формира и интернет профилът на отделния човек, вече наричан *потребител на информационни и комуникационни системи в киберпространството*. За съжаление се наблюдава една небрежност в действията и поведението на някои от тези потребители, но тя идва от недостатъчната им осведоменост по въпросите за киберсигурността.

Повишаването на киберосведомеността на участниците в глобалната мрежа може да доведе (и ще доведе) от една страна до по-сигурни компютри, системи и мрежи, а от друга – до по-успешни атаки. Затова процесът на обучение трябва да бъде добре подготвен, подходящо представен на обучаваните и проведен в специализирана, обезопасена среда. Целта е след обучението да се произведат грамотни и добронамерено мислещи потребители.

2. Визия, цел и резултати на курс „Компютърна и информационна сигурност“. Изхождайки от казаното по-горе, учени от Националната лаборатория по компютърна вирусология при БАН съвместно с Института по математика и информатика при БАН и Съюза на учените в България решиха да организират една нова образователна инициатива за изграждане на дигитални компетенции по компютърна и информационна сигурност. Преценихме, че най-подходящата възрастова група за полагане на основи за информационната и комуникационната сигурност са ученици от 9. до 12. клас. В тази възраст се предполага, че учениците вече притежават елементарна компютърна грамотност и имат базови познания по операционни системи.

Традиционният метод за обучение по компютърна и информационна сигурност на ученици, студенти, служители и крайни потребители, неспециалисти в областта, много често включва съставянето на списък с най-основните 10 проблема по темата, който се представя под формата на компютърна презентация. При така представения материал не може да се разчита, че обучаваните могат да запомнят, разберат и приложат знанията, които им се предоставят. Как ще реагира потребителят, когато е поставен в реална ситуация? Ще бъде ли полезен този писмен материал? Образованието по компютърна и информационна сигурност трябва да включва както теоретична част, така и практическа част, като се поставят казуси от реалния живот.

Екип от учени от Националната лаборатория по компютърна вирусология при БАН, Института по математика и информатика при БАН и Съюза на математиците в България, съчетавайки експертния си опит в областите на киберсигурност, превенция, защита и възстановяване на компютри, системи и мрежи, обучение на ученици, студенти и преподаватели, реши да създаде една нова образователна инициатива. Тя бе продиктувана от събеседвания между учените за проблемите, които възникват в процеса на обучение на младите хора още в най-ранна детска възраст, и за ефекта върху тяхното професионално и кариерно развитие. Стигна се до извода, че промени в средствата и формата на обучение са необходимо условие за изграждане на задълбочени знания чрез разбиране на материала/проблема/задачата. Обучение по компютърна и информационна сигурност, съчетано с теория и практика, ще доведе до правилно насочване на компютърните умения на обучаваните в посока на превенция и защита на компютри, системи и мрежи, а не в посока на атакуването им (не малка част от съществуващия злонамерен код се е породил точно от опити да се покажат/докажат недокрай развити специфични умения).

Курсът „Компютърна и информационна сигурност“, който екипът разработи и проведе с ученици от 9. до 12. клас, обхваща теми, засягащи основни видове вредителски програми и техники за анализ, почистване и възстановяване на засегнати компютърни системи. За по-лесно възприемане на материала от учениците екипът предложи лекционният материал да бъде съчетан с реални примери от професионалния живот и работата на лекторите, които са на постоянна работа в Националната лаборатория по компютърна вирусология при БАН. Комбинацията от теоретични познания и практически умения, които се очаква да бъдат придобити по време на този курс, могат да бъдат полезни не само в ежедневието, но и при евентуална бъдеща работа в областта на киберсигурността.

С курса се цели да се изградят базови знания на участниците за вредителските програми и компетентности за анализ, почистване и възстановяване на заразени компютърни системи.

3. Тематичен план на курса. Описаният в тази точка тематичен план отговаря на целта на курса. Тематичният план на курса е разделен на пет части, обобщени в два модула:

• *Модул I: Компютърни вируси: минало, настояще и бъдеще.* Изцяло теоретичен, който запознава аудиторията с основни понятия в тази област, вредителски програми, принцип на работа на антивирусните програми, текущото състояние на вредителските програми и тенденциите за развитие. Модулът включва следните три части:

Част I:

1. Дефиниции.
2. Видове вредителски програми.
3. История на компютърните вируси:
   3.1. Начални академични разработки. Първите вируси за персонални компютри.
   3.2. Макровируси. Потопът от червеи в началото на века.

Част II:

3.3. Военни вируси, използвани като оръжия.

4. Настояще на вредителските програми.
5. Бъдещи насоки на развитие. Кибероръжия и кибервойни.

Част III:

6. Антивирусни програми: скенери, програми за мониторинг, програми за проверка на интегритета и др. Перфектната антивирусна програма.
7. Защо „добрите“ вируси са лоша идея. Как да направим „добър“ вирус.

• *Модул II: Анализ, почистване и възстановяване на компютърни системи.* Изцяло практическо занятие, насочено към ключови места в компютърната система за анализ, почистване и възстановяване на модифицирани компютърни системи, работа с инструменти за анализ и възстановяване. Модулът включва следните две части:

Част IV: (Практическо занятие)

8. Ключови места при анализ, почистване и възстановяване. Файлова структура. Регистър на Windows (Windows Registry)

Част V: (Практическо занятие)

9. Инструменти за анализ.
10. Инструменти за възстановяване.

След приключване на курса участниците ще:

- могат да разпознават различните видове вредителски програми;
- могат да разбират опасностите, които се крият в киберпространството, както и отговорностите на крайния потребител;
- 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.

Предвидената **продължителност на курса** е 5 блока по 2 учебни часа от 45 минути. Екипът реши, че това ще бъде напълно достатъчно, за да се дадат основни знания и умения, без да бъде отегчена аудиторията. Освен това натрупването на много знания наведнъж в рамките на един ден не би било напълно ефективно. Особено при практическите занятия е много важно натрупаните знания от Част 1 да бъдат усвоени и изпрактикувани няколкократно, за да могат да бъдат приложени без замисляне във втората част на практическото обучение, когато няма време за търсене на бележки и трябва да се справят със задачата в поставения времеви лимит.

4. Резултати и наблюдения от пилотното провеждане на курса. За пилотно провеждане на курса бе избрана целева аудитория от ученици от 9. до 12. клас. С помощта на екип от преподаватели в училище да бъде предложен на учениците безплатен курс за обучение „Компютърна и информационна сигурност“ и да се направи списък с желаещите да посетят курса.

Условията за провеждане на пилотното обучение са следните:

- времето за провеждане на курса е в рамките на три седмици (два пъти седмично), извън редовните учебни занятия на учениците;
- мястото е сградата на Института по математика и информатика (ИМИ), в която се помещава и Националната лаборатория по компютърна вирусология (НЛКВ). Мултимедийната зала на ИМИ–БАН е 80-местна и в нея се провежда обучението по Модул I. Залата за обучение на НЛКВ–БАН е предвидена за

Модул II, като тя е 10-местна и предлага специализирана за подобен тип работа компютърна мрежа;

- за курса могат да се запишат всички желаещи от посочената таргет група без предварително селектиране;
- курсът е безплатен и няма задължителен характер. Това дава възможност за естествено подбиране на заинтересованите участници;
- тъй като залата за практическо обучение е ограничена, се налага формиране на няколко групи за обучение.

Курсът бе проведен с ученици от 10. и 11. клас на Софийската профилирана гимназия по електроника „Джон Атанасов“ през втория учебен срок на 2015/2016 учебна година. Предварително курсът бе обявен и за 9. клас, но поради големия интерес бе взето решение курсът да се повтори през първия срок на следващата 2016/2017 учебна година[1]. Курсът бе проведен в мултимедийната зала на Институт по математика и информатика при БАН и в залата за обучение на Национална лаборатория по компютърна вирусология при БАН. За съжаление провеждането на подобно обучение не може да стане при всякакви условия (например в компютърните зали на училището). Причината за това е не защото предлаганата в училището техника е слаба и с невисоки хардуерни изисквания, а защото обучението предполага предварително нарушаване на работоспособността на компютърната система. Освен това по време на обучение е естествено да се случват грешки, които при никакъв начин не бива да навредят на нормалния учебен процес по други предмети. За по-голяма сигурност за недопускане на вредителски непредумишлени действия от страна на обучаемите, компютърните системи се поставят в ограничена обезопасена мрежа.

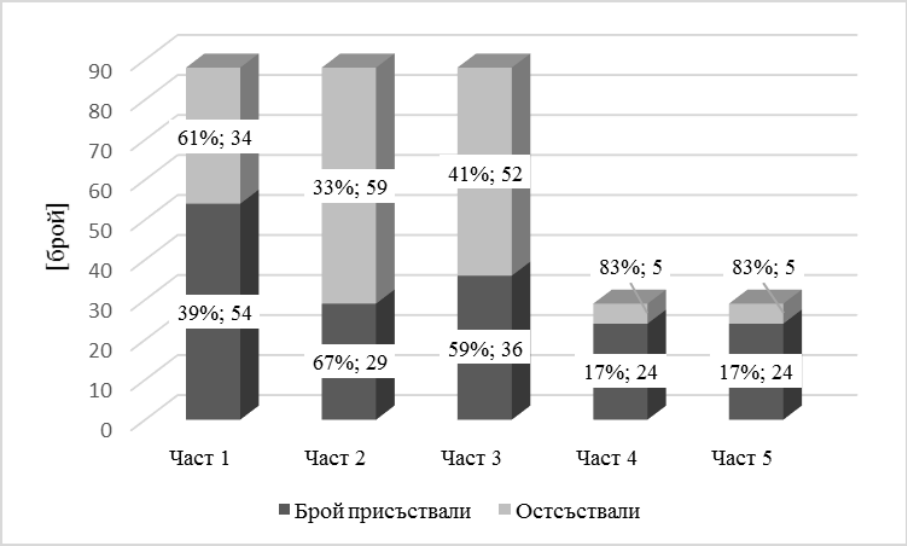
Обучението по Модул I се проведе в лекционна мултимедийна зала. Въпреки лекционния характер на темите, обаче, участниците успяха да предизвикат и участват в беседи, на които се анализираха поведението на потребителите и атакуващите в киберпространството.

До Модул II бяха допуснати само участниците, които са посетили всички части на Модул I. От една страна разчитаме на вече натрупана компетентност от Модул I, а от друга естествено се отделя групата на заинтересованите, които инвестират в това знание.

На фиг. 1 е представено процентното съотношение и броя на присъствалите спрямо регистрираните участници на всичките пет части.

Обучението по Модул II е изцяло приложно и се проведе в зала на Национална лаборатория по компютърна вирусология при БАН, където има специално подготвена тестова среда. На участниците бяха предоставени тестови компютърни системи, оборудвани със стандартен потребителски софтуер (Windows 7, Office 2010, антивирусна програма, Skype, софтуер за принтер и др.). Предварително на компютърните системи бе симулирана ежедневна работа на потребителите като работа с различни външни памети, външни устройства (принтер, скенер), връзка с няколко LAN и WiFi мрежи, посещения на уебадреси и портали и др. подобни. Това бе необходимо за Част 4, в която се изучават начини за анализ и одит на текущото състояние

[1] В доклада са включени резултати само от първото обучение, тъй като към момента на подаване на тази материал обучението на втората група ученици от 9. клас още не е приключило.



Фиг. 1. Съотношение между регистрирани и присъствали ученици

на системата. Такъв тип знания често намират приложение и в разследването на компютърни престъпления.

В Част 5 към Модул II системите предварително бяха модифицирани по такъв начин, че да бъде нарушена тяхната пълна функционалност (което се среща при заразяването на системата с вредителска програма). Целта на участниците бе да възстановят пълната функционалност на системата.

Всички участници бяха разположени в една зала, като имаше възможност за активно събеседване при решаване на отделните проблеми между самите участници.

Направена бе и вътрешна оценка на работата на участниците по следната 5-степенна скала за оценка:

а) отлично – участникът се е справил със задачата в указания времеви лимит от 90 мин., без да търси допълнителна помощ от обучаващия;

б) много добре – участникът изпълнява докрай задача във времевия лимит, но е получавал допълнително насоки в процеса на работа;

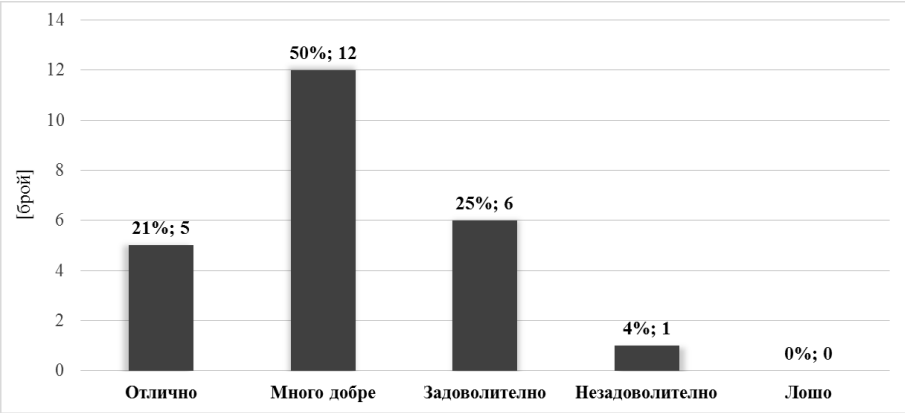
в) задоволително – участникът е изпълнил частично (повече от половината) от поставената задача за даденото време;

г) незадоволително – участникът е изпълнил едва до половината от поставената му задача във времевия лимит;

д) лошо – участникът не се е справил със задачата.

От поставените оценки (фиг. 2) се вижда, че по-голямата част от учениците се справиха много добре с поставената им задача и нямаше ученик, който да не се справи със задачата.

След приключване на обучението може да се каже, че подобно обучение е подходящо за тази възрастова група. Предложеният учебен план, в който е търсен баланс между теория и практика, дава възможност за изграждане и развитие на ключови компетентности на учениците, включващи *дигитална компетентност, умение за*



Фиг. 2. Получени оценки

самостоятелно учене, социални и граждански компетентности, усет за инициатива и предприемачество, подобаващо отношение към изявяването [3].

5. Заключение. Компютърната и информационната сигурност е от изключително важно значение за съвременното общество, което живее зависимо от информационните и комуникационните системи, които са проникнали дълбоко и са се превърнали в основа на всички дейности в икономиката, администрацията, обществото и личния живот на хората. Поради това повишаването на компетентността и осведомеността на обществото по въпросите, свързани със сигурността на тези системи, е от изключително важно значение. Нереално е да си мислим, че можем да обучим всички участници в глобалната мрежа, но можем да фокусираме усилията си в посока на професионално общуване с учениците. Това, обаче, е възможно да стане само с обединените усилия на експерти и преподаватели, които да работят с учениците в стил на творческо общуване и отговорност към това, как трябва да се използват знанията за информационните и комуникационните технологии.

Националната лаборатория по компютърна вирусология при БАН заедно с Института по математика и информатика при БАН и Съюза на математиците в България ще продължат да работят в посока на обучение на ученици и преподаватели по темата за компютърна и информационна сигурност, като ще се стремят да развият, актуализират и доусъвършенстват обучението в тази област.

ЛИТЕРАТУРА

[1] A. Vaseashta, P. Susmann, E. Braman. Cyber Security and Resiliency Policy Framework, IOS Press, 2014, ISBN 1614994463, p. 3.

[2] M. Bishop, N. Miloslavskaya, M. Theocharidou. Information Security Education Across the Curriculum: 9th IFIP WG 11.8 World Conference, WISE 9, Hamburg, Germany, May 26-28, 2015, Proceedings, Springer 2015, ISBN 3319185004, 27–29.

[3] П. Кендеров, Е. Сендова, Т. Чехларова. Развиване на ключови компетентности чрез образованието по математика: Европейският проект KeyCoMath *Математика и математическо образование*, **43** (2014), 99–105.

Димитрина Полимирова
Националната лаборатория по компютърна вирусология
Българска академия на науките
ул. „Акад. Георги Бончев“ бл. 8
1113 София, България
e-mail: dimitrina.polimirova@nlcv.bas.bg

NEW EDUCATIONAL INITIATIVE TO BUILD DIGITAL COMPETENCE IN COMPUTER- AND INFORMATION SECURITY

Dimitrina Lyubomirova Polimirova

The issues and problems related to the protection and security of information and communication systems are extremely important. In recent years, experts and politicians have expressed growing concern about the protection of these systems from cyberattacks, which are expected to increase in the coming years not only in their frequency but also as a burden with respect to the damages. The main actors in cybersecurity are government organizations, businesses and end-users, each of which take various measures to increase it. One of these measures – Cybersecurity awareness, belongs to all three actors.

In this report we present the design and launching of the educational course “Computer- and Information Security”, whose aim is that the participants gain basic knowledge about the malware and competences for analysis, cleaning and recovery of infected computer systems. Impressions of the pilot experiment conducted at the National Laboratory of Computer Virology–BAS and the Institute of Mathematics and Informatics–BAS with participants from the Vocational High School of Electronics “John Atanasov” – Sofia, are shared.