Проучени са основни документи и свързани материали за най-опасни заплахи за информационната сигурност:

- 2011 CWE/SANS Top 25 Most Dangerous Software Errors, http://cwe.mitre.org/top25/index.html
- https://www.sans.org/top25-software-errors
- Common Weakness Scoring System (CWSS™), http://cwe.mitre.org/cwss/cwss_v1.0.1.html
- OWASP Top 10 - 2017 The Ten Most Critical Web Application Security Risks, https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf
- National Vulnerability Database, NIST, https://nvd.nist.gov/vuln-metrics/cvss
- CVE Details, The ultimate security vulnerability data source, https://www.cvedetails.com/index.php

Проучени са публикувани актуални анализи за информационната сигурност:

- Global Application & Network Security Report 2017-2018, Radware
- Attack Mitigation Solutions Overview – Radware
- The Global State of Information Security® Survey 2018 – PWC
- Fortinet 2016 Predictions for the Evolving Threat Landscape - Fortinet.

Извършени са следните дейности по внедряване на GDPR:

- проучване и анализ на основни документи и материали за прилагането на GDPR.
- проучване на решения за внедряването на GDPR в Системи за управление на задачи (LMS – Learning Management System) .
- проучване и анализ на събиране, обработка и съответствие на данните според изискванията на EU GDPR в широко използваната система за електронно обучение Moodle в различни учебни институции.

Установено е сътрудничество с Института за публична администрация и ДА е-Управление. Подготвя се общ доклад на тема „Human factor in digitalization and cyber resilience of PA", който ще отрази работата ни последните 2 години в контекста на ННП ИКТ в науката, образованието и сигурността, и в частност задачата за обучение в администрацията по ИКТ и инфо (кибер) сигурност.
Разработва се програма за администрацията за обучение по информационна сигурност, която ще бъде тествана през есента на 2019 г.
Проведени бяха консултации в Скопие с НАТО по изграждане на програма за обучение и институт по кибер сигурност в Северна Македония, 15-17.4.2019 г., в гр. Скопие.
Предвижда се използване на външни изпълнители от ESI-CEE (с контактно лице Георги Шарков) по подготовка на таксономия по информационна сигурност за целите на обучението.

Осъществени са контакти със следните училища:

1. Софийска професионална гимназия „Джон Атанасов". НЛКВ–БАН, гр. София
2. Природо-математическа гимназия – Благоевград, гр. Благоевград;

3. Частна профилирана гимназия “Образователни технологии“, гр. София.

Проведе се пилотно обучение по компютърна и информационна сигурност. Направен бе анализ на нивото на обучение, на интересите на учениците и на учителите и на материала, включен в програмата на трите училища (тук се включват освен задължителните предмети от МОН и профилирани предмети, включени от ръководството на съответното училище). С избрани ученици е проведено обучение по писане на сигурен програмен код (на PHP и MySQL). В обучението участваха ученици и учители.

Изводите, които направихме от проведеното пилотно обучение, са:

- в училищата няма специализирани курсове за обучение по компютърна и информационна сигурност. В най-общ вид някои понятия се дискутират като отделна тема в рамките на 1-2 урока.
- липсва практическо обучение, където най-добре се разбира и запомня материала;
- необходимо е предварително да се наблегне повече на основните понятия като цяло, за да е по-ефективно обучението в дълбочина. Учениците работят добре с клавиатура и мишка, но трудно работят с терминология, която се използва за подобен тип обучение, и която е необходима за постигане на дълбочина на знанията. Затова в учебния материал, който трябва да се предложи, е необходимо да се отдели внимание и на базови понятия.
- необходими са допълнителни усилия и ресурси, за да се изгради тестова среда в изолирана мрежа за подобен тип практическо обучение;
- практическото обучението е пи-ефективно за група от 6-10 човека;
- лекционното обучение е по-добре да бъде направено в голяма група (над 30 човека), тъй като спонтанно се задават много въпроси от ежедневието на обучаваните и естествено се получава контролирана (по отношение на достоверността на информацията) дискусия.

В резултат на направено проучване са идентифицирани няколко учебни рамки (curricula) в областта на обучението по киберсигурност

- CYBERSECURITY CURRICULUM - CSEC 2017 v1.0
- CYBERSECURITY A GENERIC REFERENCE CURRICULUM
- CERT® Resilience Management Model, Version 1.2

Идентифицирани са представителни курсове по информационна сигурност от различни университети:

- Магистърски курс по Информационна сигурност в Лисабонския университет – Португалия, цели да даде на обучаемите и техните компании конкурентни знания и умения по сигурност на критични инфраструктури. Програмата включва от една страна безопасност и надеждност, и информация и инфраструктура – от друга. Програмата дава солидна теоретична база в комбинация с интензивна лабораторна работа.
- Курс по Верификация на протоколи за сигурност в дисциплина “Технологии на информационната сигурност” на ниво бакалавър в Технологичен

университет – Айндховен, Нидерландия, включва моделиране на протоколи за сигурност тип “черна кутия”, моделиране на поведение на нарушител (intruder), изисквания към сигурността, BAN логика и др. логика на протоколи за сигурност, алгебричен подход към верификация на протоколи за сигурност, проверка на моделите.

- Курс по Компютърна сигурност на ниво бакалавър в Технически университет – Прага, се фокусира върху криптографска математика, комплексни Internet технологии, висша криптография, сигурност и технически ресурси.
- Курс по Информационна сигурност на ниво бакалавър в Загребски университет – Хърватия, се фокусира върху основите на информационната сигурност, мрежова сигурност, управление на сигурността и риска, биометрична удостоверяване, приложна криптография, компютърна криминалистика, сигурни архитектури, сигурност на безжичните мрежи, сигурност на електронната търговия, сигурност на базите от данни и софтуера, одит на сигурността, юридически аспекти на компютърната сигурност.
- Магистърски курс по Информационна сигурност във Военно-техническа академия – Букурещ, Румъния, включва компютърна сигурност, въведение в криптографията и механизмите за сигурност, мрежова сигурност, сигурни бизнес технологии, юридически и регулационни аспекти на електронната търговия, сигурност на базите от данни. Фокусира се върху криптографски механизми, услуги и протоколи, електронни подписи, PKI инфраструктури, приложения със смарт карти, електронни разплащания, сигурност на мрежовите протоколи и др.