

УПРАВЛЕНИЕ НА ИНФОРМАЦИОННА СИГУРНОСТ В ОБРАЗОВАТЕЛНИТЕ ИНСТИТУЦИИ: ПОЛИТИКИ, ПРОЦЕДУРИ И ДОБРИ ПРАКТИКИ

Деан Василев

Икономически университет, Варна, България, e-mail: dean.vasilev@ue-varna.bg

РЕЗЮМЕ

Настоящият доклад разглежда основните принципи и стъпки при разработването и прилагането на политики за управление на информационната сигурност в образователните институции, със специален фокус върху Професионалната гимназия по икономика "Д-р Иван Богоров" – Варна. Изследва се процесът на създаване на политика за информационна сигурност в контекста на нормативната уредба и международните стандарти. Докладът включва анализ на основните стъпки за внедряване на политики за информационна сигурност в образователните среди и конкретно прилагане на тези политики в рамките на ПГИ "Д-р Иван Богоров".

КЛЮЧОВИ ДУМИ: безопасно училище, киберсигурност, информационна сигурност

INFORMATION SECURITY MANAGEMENT IN EDUCATIONAL INSTITUTIONS: POLICIES, PROCEDURES AND GOOD PRACTICES

Dean Vasilev

University of Economics, Varna, Bulgaria, e-mail: dean.vasilev@ue-varna.bg

ABSTRACT

This report examines the main principles and steps in the development and implementation of information security management policies in educational institutions, with a special focus on the Vocational High School of Economics "Dr. Ivan Bogorov" - Varna. The process of creating an information security policy in the context of regulations and international standards is explored. The report includes an analysis of the main steps for the implementation of information security policies in educational environments and the specific implementation of these policies within the Vocational High School of Economics "Dr. Ivan Bogorov".

KEYWORDS: Safe school, Cybersecurity, Information security

ВЪВЕДЕНИЕ

Информационната сигурност е критично важна за образователните институции, които обработват чувствителна информация, свързана с ученици, преподаватели и административен персонал. С разрастването на дигиталните технологии, училищата и университетите все повече разчитат на информационни системи за управлението на учебния процес и административните дейности. За да се гарантира защитата на тези данни и предотвратяването на инциденти, е необходимо разработването и прилагането на адекватни политики за информационна сигурност (ИС). Цел на настоящия доклад е да се анализират процедурите за разработване на такива политики, разглеждайки общите принципи и прилагането на мерки за защита на данните в ПГИ "Д-р Иван Богоров".

1. ЗАКОНОВА И НОРМАТИВНА РАМКА

Политиките за управление на информационната сигурност в образователните институции са основният механизъм за осигуряване на защитата на данните и информационните системи. Те задават рамките за управление на достъпа до информационни ресурси, защита от киберзаплахи, управление на инциденти и възстановяване след инциденти. Целта на тези политики е да гарантират, че информацията ще бъде защитена от неототоризиран достъп, ще остане достъпна само за ототоризирани потребители и ще бъде съхранена правилно, така че да се предотврати загуба на данни.

Основните принципи на политиките за информационна сигурност са (Каракънева, 2013):

- **Конфиденциалност:** гарантира, че информацията е достъпна само за ототоризирани лица.
- **Цялостност:** информацията остава непокътната и не е променена неразрешено.
- **Наличност:** информацията е на разположение, когато е необходима, без прекъсвания.

В България и Европейския съюз има няколко основни нормативни акта и стандарти, които регулират информационната сигурност в различни институции, включително образователните. Те задават основните изисквания за сигурност и механизми за защита на данните.

Закон за киберсигурност (България) (МС, обн. ДВ бр.94 от 13 Ноември 2018г.): Законът за киберсигурност урежда организацията на мрежовата и информационна сигурност в България. Той определя задълженията на различни институции, включително образователни, за осигуряване на минимални мерки за защита срещу киберзаплахи. Законът също така налага необходимостта от създаване на системи за управление на инциденти и планиране на действия при извънредни ситуации.

Наредба за минималните изисквания за мрежова и информационна сигурност (МИС) (МС, Обн. ДВ бр. 59 от 26 Юли 2019г.): Тази наредба определя минималните мерки за защита, които трябва да бъдат приложени от всички институции, включително образователни. Тя регламентира процесите по управление на сигурността на информационните системи, процедурите за управление на инциденти и правилата за съхранение и защита на данни. Наредбата е базирана на международните стандарти за информационна сигурност, като ISO/IEC 27001.

Регламент (ЕС) 2016/679 – Общ регламент относно защитата на данните (GDPR) : Един от най-важните документи за защита на личните данни в рамките на Европейския съюз, който обхваща и образователните институции. GDPR налага изисквания за събиране, обработка и съхранение на лични данни на ученици, преподаватели и административен персонал. Освен това, GDPR предвижда санкции при нарушения, свързани със защитата на данни, което прави спазването на регламента критично важно за всяка институция.

Закон за защита на личните данни (България) (МС, Обн. ДВ. бр.1 от 4 Януари 2002г.): Този закон допълва GDPR и урежда обработката на лични данни в България. В контекста на образователните институции, законът определя правилата за съхранение на данни на ученици, административен персонал и преподаватели, както и правата на тези лица относно тяхната лична информация. Законът задължава институциите да осигурят съгласие за обработка на данните и да прилагат мерки за сигурност, за да предотвратят неототоризиран достъп или злоупотреба с данните.

ISO/IEC 27001 – Стандарт за системи за управление на информационната сигурност (СУИС): Международен стандарт, който задава насоки за изграждане и поддържане на ефективни системи за управление на информационната сигурност. Стандартът ISO/IEC 27001

изисква образователните институции да идентифицират информационните активи, да оценяват рисковете, свързани с тях, и да внедряват адекватни мерки за защита. Този стандарт също така изисква редовни одити и актуализация на политиките за информационна сигурност.

Закон за електронното управление (МС, Обн. ДВ. бр.46 от 12 Юни 2007г.): Този закон урежда електронното управление на данни в публичния сектор, като изисква от образователните институции да използват цифрови платформи и електронни услуги по сигурен и отговорен начин. Законът въвежда изисквания за сигурност на електронните системи и обмена на информация.

Наредба за критичната инфраструктура и услугите от съществено значение (МС, Обн. ДВ. бр.81 от 23 Октомври 2012г.): Тази наредба регулира как се определят критичните сектори и услуги, включително образователния сектор, и задава изисквания за защита на критичната инфраструктура. В случай на атака или инцидент, образователните институции трябва да следват определени мерки за възстановяване на нормалната дейност и защита на данните.

Тези нормативни документи задават рамките и изискванията, които образователните институции трябва да следват, за да гарантират защитата на информацията и съответствието с регулаторните изисквания. Политиките за информационна сигурност трябва да отразяват тези закони и стандарти, като гарантират, че всички процеси и процедури са съобразени с нормативните изисквания и са насочени към защита на данните.

2. ПРОЦЕДУРА, ПРИ СЪЗДАВАНЕТО НА ПОЛИТИКА ЗА ИНФОРМАЦИОННА СИГУРНОСТ В ОБРАЗОВАТЕЛНА ИНСТИТУЦИЯ

Процесът на разработване и внедряване на ефективна политика за информационна сигурност в образователна институция изисква систематичен и структуриран подход. Той включва няколко основни етапа, които гарантират правилното идентифициране на нуждите, рисковете и мерките за защита на информационните активи. По-долу са представени основните стъпки за създаване на такава политика:

1. Идентификация на информационните активи

1.1. Описание на информационните активи: Първата стъпка в създаването на политика за информационна сигурност е идентифицирането на всички информационни активи, които трябва да бъдат защитени. Това включва лични данни на ученици, преподаватели и персонал, академична информация, учебни материали, административни документи, информационни системи и технологични инфраструктури.

1.2. Класификация на активите: Веднъж идентифицирани, активите трябва да бъдат класифицирани въз основа на тяхната критичност и степен на чувствителност. Това ще помогне за определяне на приоритетите и подходящите мерки за сигурност за всеки актив.

2. Оценка на риска

2.1. Идентифициране на заплахы и уязвимости: На този етап се анализират потенциалните заплахы за сигурността на информацията, като хакерски атаки, неоторизиран достъп, загуба на данни, зловреден софтуер и други. Всяка заплаха се оценява по отношение на вероятността за възникване и потенциалното ѝ въздействие върху образователната институция.

2.2. Оценка на вероятността и въздействието: Рисковете се класифицират според степента на вероятност за възникване и въздействието върху институцията. Например, ако рискът от кибератака е висок, а въздействието ѝ може да доведе до загуба на критични данни

или компрометиране на лична информация, този риск се класифицира като висок приоритет за действие.

2.3. Определяне на мерки за минимизиране на риска: След като рисковете са идентифицирани и оценени, се определят конкретни мерки за минимизирането им. Това може да включва внедряване на антивирусен софтуер, подобряване на контрола на достъпа или повишаване на осведомеността на служителите за киберзаплахи.

3. Разработване на политиката

3.1. Изготвяне на документация: Политиката за информационна сигурност трябва да бъде ясно документирана. Тя трябва да включва описание на процедурите за защита на информацията, реда за управление на достъпа, мерките за защита на мрежовата инфраструктура и планове за действие при инциденти. В този етап трябва да се включат и отговорните лица и техните роли в прилагането на политиката.

3.2. Изисквания за контрол на достъпа: Политиката трябва ясно да определя как се осигурява контролът на достъпа до информационните системи. Това включва внедряване на методи за удостоверяване на потребители, като двуфакторна автентикация, уникални пароли и политики за смяна на пароли. Определянето на различни нива на достъп според функциите и правомощията на потребителите е от ключово значение.

3.3. Правила за обработка и съхранение на данни: Политиката трябва да дефинира ясни правила за обработка, съхранение и архивиране на данни. Тези правила включват как се създават резервни копия, как се управляват хардуерните и софтуерните ресурси, както и как се предотвратяват загуби на информация.

4. Внедряване на политиката и обучение

4.1. Обучение на персонала и учениците: Една от най-важните стъпки при внедряването на политика за информационна сигурност е осигуряването на необходимото обучение за персонала и учениците. Това обучение трябва да ги запознае с нововъведените мерки за защита на данните, както и с техните отговорности. Обучението включва идентифициране на киберзаплахи (като фишинг имейли), безопасно използване на пароли и правилно използване на мрежовите ресурси.

4.2. Информираност и съответствие с политиката: След обучението, всички служители трябва да подпишат декларация за спазване на политиката за информационна сигурност. Това гарантира, че те са запознати с правилата и разбират своите задължения. Ръководителите на различните отдели трябва да следят за изпълнението на тези изисквания.

5. Мониторинг, поддръжка и одит

5.1. Редовен мониторинг на системите: Политиката за информационна сигурност трябва да предвижда редовен мониторинг на информационните системи за откриване на възможни заплахи или необичайна активност. Инструментите за мониторинг включват системи за откриване на прониквания (IDS) и инструменти за анализ на трафика, които предупреждават за потенциални проблеми в реално време.

5.2. Одит на политиката: За да се гарантира ефективността на политиките за информационна сигурност, институцията трябва да провежда редовни вътрешни и външни одити. Одитите помагат за оценка на ефективността на прилаганите мерки и за откриване на потенциални пропуски в сигурността. След всеки одит се правят препоръки за подобрение, а установените проблеми трябва да бъдат незабавно коригирани.

5.3. Актуализация на политиката: Политиките трябва да се актуализират редовно, за да отразяват новите заплахи и технологични промени. Прегледите трябва да се провеждат поне

веднъж годишно, като се вземат предвид промените в нормативната уредба, технологиите или организационната структура на институцията.

Тези стъпки осигуряват цялостен процес за създаване и прилагане на политика за информационна сигурност в образователните институции. Ефективното внедряване на подобна политика гарантира защита на чувствителната информация, намалява риска от инциденти и подобрява цялостната сигурност на информационната система в институцията.

3. ПРИЛОЖЕНИЕ НА ПОЛИТИКА ЗА ИНФОРМАЦИОННА СИГУРНОСТ В ПГИ "Д-Р ИВАН БОГОРОВ" – ВАРНА

ПГИ "Д-р Иван Богоров" във Варна е внедрила цялостна система за управление на информационната сигурност, съобразена с нормативните изисквания и добрите практики в сферата на образованието. Това включва контрол на достъпа до информационни системи, управление на инциденти, резервиране на данни и използване на облачни услуги. В този раздел ще се разгледат конкретните мерки и политики, приложени в гимназията.

3.1 Политика за контрол на достъпа

Политиката за контрол на достъпа е насочена към защита на информационните системи и данни от неоторизиран достъп. Основните елементи на тази политика в ПГИ "Д-р Иван Богоров" включват:

- **Уникални потребителски акаунти:** Всеки ученик, учител и служител разполага с уникален потребителски акаунт, като достъпът до системи и данни е ограничен според функциите и ролята на потребителя. По този начин се намалява възможността за неоторизиран достъп до чувствителна информация.
- **Пароли и многофакторна автентикация (MFA):** Институцията прилага правила за силни пароли, които трябва да се сменят периодично. В допълнение към паролите се използва и многофакторна автентикация за достъп до критични системи, което добавя допълнителен слой на сигурност.
- **Ограничен достъп до мрежи и ресурси:** Достъпът до мрежовите ресурси в училището е строго контролиран чрез мрежови правила и системи за управление на достъпа. Само оторизирани потребители имат право да използват мрежовите ресурси.

3.2 Политика за управление на инциденти

Политиката за управление на инциденти осигурява бърза и ефективна реакция при инциденти, свързани с информационната сигурност. Основните елементи на тази политика включват:

- **Идентифициране и докладване на инциденти:** Всички ученици и служители са обучени да разпознават потенциални инциденти, като подозрителна активност, опити за неоторизиран достъп или фишинг атаки. При откриване на инцидент, той трябва да бъде незабавно докладван на отговорното лице.
- **Реагиране и ограничаване на инцидента:** След докладване, екипът по информационна сигурност предприема стъпки за ограничаване на инцидента, като изолира засегнатите системи и анализира проблема, за да се предотврати по-нататъшно разпространение.
- **Документация и анализ:** Всеки инцидент се документира подробно, включително причините, мерките за възстановяване и препоръки за подобрене. Тези доклади помагат за усъвършенстване на процесите и предотвратяване на бъдещи инциденти.

3.3 План за непрекъсваемост на дейността

Политиката за непрекъсваемост на дейността е създадена, за да осигури минимални прекъсвания на учебния процес в случай на сериозен инцидент. Основните елементи на тази политика включват:

- **Редовно създаване на резервни копия:** Всяка седмица се правят автоматични резервни копия на критични данни като академични записи и административна информация. Тези резервни копия се съхраняват както локално, така и в облачни услуги, за да се гарантира, че данните ще бъдат възстановени при загуба.
- **Възстановяване при инциденти:** Училището разполага с план за бързо възстановяване на системите в случай на кибератака, технически срыв или природно бедствие. Планът включва процедури за координация с доставчици и ИТ екипи.
- **Тестове и симулации:** Планът за непрекъсваемост на дейността се тества редовно чрез симулации на различни сценарии, за да се провери готовността на системите и екипите за реагиране при реални инциденти.

3.4 Обучение и осведоменост

Обучението на персонала и учениците е ключова част от политиките за информационна сигурност в ПГИ "Д-р Иван Богоров". Програмата за обучение включва:

- **Обучения за разпознаване на киберзаплахи:** Учениците и персоналят преминават през редовни обучения за разпознаване на фишинг атаки, зловреден софтуер и други киберзаплахи. Обученията обясняват как да реагират при възникване на такива инциденти и как да ги докладват.
- **Обучения по защита на лични данни:** Персоналят е запознат с основните принципи на GDPR и Закона за защита на личните данни, което включва обучение за правилна обработка, съхранение и защита на чувствителни данни.

3.5 Политика за използване на облачни услуги

ПГИ "Д-р Иван Богоров" използва облачни услуги за съхранение и управление на данни, като се гарантира, че тези данни са защитени от неототоризиран достъп и злоупотреби. Основни елементи на политиката включват:

- **Криптиране на данни:** Всички данни, съхранявани в облачните услуги, се криптират както при пренос, така и при съхранение. Това осигурява допълнителен слой на защита дори при неототоризиран достъп.
- **Контрол на достъпа до облачните ресурси:** Само ототоризирани лица имат достъп до облачните ресурси чрез многофакторна автентикация и строги правила за достъп. Това намалява риска от загуба или злоупотреба с данни.
- **Одити на доставчиците на облачни услуги:** Периодичните проверки на доставчиците гарантират, че те спазват изискванията за сигурност и прилагат адекватни мерки за защита на данните.

3.6 Резервни копия и план за възстановяване на данни

ПГИ "Д-р Иван Богоров" е внедрила строга политика за редовно създаване на резервни копия, за да защити критични данни в случай на инциденти. Основните компоненти на тази политика включват:

- **Автоматизирано създаване на резервни копия:** Резервните копия се създават автоматично и се съхраняват както локално, така и в облачни услуги. Това гарантира, че данните могат да бъдат бързо възстановени в случай на загуба.
- **План за възстановяване на данни:** В случай на загуба на данни или срыв на системите, училището има план за възстановяване, който включва използване на резервни копия и координация с ИТ доставчиците за възстановяване на нормалната работа.

ЗАКЛЮЧЕНИЕ

Внедряването на политики за управление на информационната сигурност в образователните институции е от съществено значение за защитата на данните и мрежовите системи. В контекста на нарастващите киберзаплахи и увеличаването на зависимостта от информационни технологии в образованието, институциите трябва да приемат систематичен подход към управлението на риска и сигурността. ПГИ "Д-р Иван Богоров" - Варна служи като добър пример за прилагане на цялостни политики за контрол на достъпа, управление на инциденти и използване на облачни услуги.

Редовното обучение на персонала и учениците, съчетано с постоянен мониторинг на сигурността, е ключово за поддържането на високо ниво на информационна защита. Прилагането на тези мерки не само осигурява съответствие със законовите изисквания, но и повишава ефективността на работата на институцията, като минимизира рисковете от кибератаки и технически проблеми.

На база проведеното проучване и анализ на политиката за информационна сигурност на ПГИ „Д-р Иван Богоров“ могат да се отправят няколко препоръки за подобряване на нейната ефективност. На първо място, е важно да се повиши нивото на обучение и осведоменост на служителите и учениците относно най-новите киберзаплахи и добрите практики за защита на информацията. Това включва редовно организиране на обучения, които обхващат теми като разпознаване на зловреден софтуер, идентифициране на фишинг атаки и използване на силни пароли. Освен това, интеграцията на допълнителни инструменти за мониторинг на сигурността би позволила по-бързо откриване на инциденти и би осигурила реакция в реално време, което е от критично значение за защита на информационната инфраструктура. Препоръчително е също така да се провеждат редовни вътрешни и външни одити на политиките за информационна сигурност, които да идентифицират възможни пропуски и да оптимизират процесите, като резултатите от тези одити се използват за подобряване на мерките за защита. Накрая, с оглед на непрекъснатото развитие на кибератаките, политиките за информационна сигурност трябва да бъдат регулярно актуализирани, за да отразяват новите заплахи и уязвимости, което ще гарантира тяхната адекватност и ефективност в динамичната технологична среда.

REFERENCES / ИЗПОЛЗВАНА ЛИТЕРАТУРА

1. Каракънева, Ю., 2013. Киберсигурност : основни аспекти. София: изд. Авангард прима.
2. МС, Обн. ДВ бр. 59 от 26 Юли 2019г. Наредба за минималните изисквания за мрежова и информационна сигурност. (изм. ДВ бр. 47 от 24 Юни 2022г.)
3. МС, обн. ДВ бр.94 от 13 Ноември 2018г.. Закон за киберсигурност. (изм. ДВ бр.25 от 29 Март 2022г.)
4. МС, Обн. ДВ. бр.1 от 4 Януари 2002г.. Закон за защита на личните данни.(изм. ДВ. бр.70 от 20 Август 2024г.)
5. МС, Обн. ДВ. бр.46 от 12 Юни 2007г. Закон за електронното управление. (изм. и доп. ДВ. бр.80 от 19 Септември 2023г.)
6. МС, Обн. ДВ. бр.81 от 23 Октомври 2012г. Наредба за реда, начина и компетентните органи за установяване на критичните инфраструктури и обектите им и оценката за риска от тях (изм. ДВ. бр.27 от 5 Април 2016г.)