Наташа АНГЕЛОСКА-ГАЛЕВСКА
Оливер БАКРЕСКИ

УДК: 342.738:378.4(497.7)
Изворен научен труд

ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ ВО АКАДЕМСКАТА СРЕДИНА: РЕГУЛАТИВИ, ПРЕДИЗВИЦИ И ПРАКТИКИ

Кратка содржина:

Обезбедувањето заштита на личните податоци во рамките на универзитетите е од суштинско значење за одржување на приватноста и безбедноста на студентите, вработените и факултетот како целина. Универзитетите треба да имплементираат технички и организациски мерки како што се контрола на пристап, шифрирање, редовна обука на вработените и планови за превенција и одговор на инциденти за заштита на податоците.

Целта на овој труд е да се анализираат мерките и механизмите што ги применува Филозофскиот факултет во Скопје за обезбедување заштита на личните податоци. За прибирање на валидни и длабински сознанија беше спроведено квалитативно истражување преку полуструктурирани интервјуа со клучни службени лица, како и анализа на содржината на релевантни документи. За зголемување на научната релијабилност беше реализирано и квантитативно истражување со останатите засегнати страни (наставен кадар, административно-технички кадар и студенти). Во овој труд се презентирани главно резултатите и заклучоците изведени од примарните податоци добиени преку интервјуата и од секундарните податоци од прегледот на литературата и анализата на документи.

Добиените резултати покажуваат дека на Филозофскиот факултет се воспоставени соодветни политики и практики за заштита на личните податоци на сите засегнати страни. Во последниве години, донесени се 19 регулаторни акти за обезбедување различни видови информации. Воведени се значајни безбедносни мерки, особено во однос на личните податоци на студентите и вработените, резултатите од испитите и други критични информации поврзани со факултетот. Сепак, потребни се понатамошни подобрувања поради тековните закани за безбедноста на податоците.

Клучни зборови: *Лични податоци, безбедносни мерки, заштита на податоци, универзитет*

1. Вовед

Обезбедувањето на заштитата на личните податоци во рамките на универзитетите е клучно за одржување на приватноста и безбедноста на студентите и на наставниот и административно-техничкиот кадар. Во Република Македонија, Законот за заштита на личните податоци (2020), усогласен со Општата регулатива за заштита на податоците (GDPR) на ЕУ, ја поставува рамката за овие механизми за заштита. Клучните принципи вклучуваат транспарентност, законитост, ограничување на целта, минимизирање на податоците, точност и безбедност. Универзитетите се должни да имплементираат технички и организациски мерки како што се контрола на пристап, енкрипција, редовна обука на вработените и планови за подготвеност и одговор на инциденти за заштита на податоците. Покрај тоа, поединците имаат права, вклучувајќи пристап, исправка, бришење, ограничување на обработката и преносливост на податоците. Овие мерки обезбедуваат услови личните податоци да се обработуваат одговорно, намалувајќи го ризикот од неовластен пристап и прекршувања.Редовните ревизии и строгото почитување на законските стандарди се од суштинско значење за одржување на довербата и интегритетот во академската средина.

Во натамошниот текст се презентираат резултатите од сеопфатна анализа на мерките и механизмите кои се применуваат на Филозофскиот факултет во Скопје за обезбедување заштита на личните податоци во академската средина што треба да овозможи подлабоко разбирање на институционалните практики, процедури и предизвици на овој план.

2. Стратегии за зајакнување на протоколите за заштита на податоци на Универзитетот

Во денешното дигитално доба, универзитетите располагаат со огромни количини чувствителни податоци, вклучувајќи евиденции и лични информации на студентите, вработените и факултетот, финансиски податоци, како и доверливи истражувачки податоци и интелектуална сопственост. Заштитата на безбедноста на овие податоци е од клучно значење за одржување на довербата, почитување на законските барања и заштита на академскиот интегритет. Нарушувањето на безбедноста на податоците не само што ја загрозува приватноста на студентите, вработените и факултетот, туку има и далекусежни правни, финансиски и репутациски импликации за институцијата како целина.

Образовните институции сè повеќе се потпираат на софтверски решенија за поедноставување на административните задачи, за подобрување на методологиите на наставата и подобрување на комуникацијата меѓу наставниците и учениците. Неодамнешните кибернапади врз организациите, вклучително и оној со кој на неколку дена беше прекинат пристапот

до веб-страницата на Универзитетот, ја истакнаа критичната важност на комплексните мерки за безбедност на податоците, почнувајќи од прекршувања што ги компромитираат личните информации на учениците до напади што ја нарушуваат дејноста на факултетот.Ранливостите на системот го привлекува вниманието на злонамерници кои се обидуваат да ги искористат слабостите во софтверските инфраструктури. За да се справат со ваквите ескалирани ризици, високообразовните институции треба да бидат проактивни во изборот и имплементацијата на вистинските софтверски решенија што даваат приоритет на безбедноста на податоците без да ја загрозат функционалноста на институцијата.

Заштитата на чувствителните лични податоци изискува спроведување низа стратешки и процедурални мерки во рамки на универзитетите.

2.1. Основни принципи за заштита на личните податоци

Во продолжение се претставени клучните принципи што ја формираат основата за ефикасна заштита на личните податоци во академски контекст. Овие клучни стратегии се сметаат за клучни и се посочени во релевантните документи. (Solove, DJ, 2006; Solove, DJ, 2008; De Hert, P. и Gutwirth, S., 2006)

*2.1.1. Транспарентност и законитост: Л*ичните податоци треба да се обработуваат транспарентно и законски. Универзитетите мора да ги информираат субјектите за тоа како ќе се користат нивните податоци и кои се целите на обработка.

2.1.2. Цел на обработката: Податоците треба да се собираат за специфични, јасни и легитимни цели и не смеат понатаму да се обработуваат на начин што не е компатибилен со тие цели.

2.1.3. Минималност на податоци: Се собираат само оние податоци што се неопходни за исполнување на целта за која се обработуваат.

2.1.4. Точност и навременост: Податоците мора да бидат точни идоколку е потребно, треба да се ажурираат. Универзитетите треба да преземат чекори за да се осигураат дека неточните податоци се бришат или коригираат.

2.1.5. Безбедност и доверливост: Универзитетите мора да применуваат технички и организациски мерки за заштита на личните податоци од неовластен пристап, обработка или објавување.

Во натамошниот текст се анализираат релевантни извори кои се однесуваат на политиките, практиката и емпириските истражувања со фокус на техничките и организациските безбедносни мерки наУниверзитетот.

2.2. Технички и организациски мерки

Техничките и организациските безбедносни мерки преземени на универзитетите примарно имаат за цел да го намалат ризикот од неовластен пристап до чувствителни информации и лични податоци. Во релевантните извори за оваа проблематика се набројуваат повеќе можни стратегии. (ENISA, 2016; Kerkhove, TV и Charlier, N., 2021; Ifenthaler, D. и Schumacher, C., 2016, Jisc, 2018):

2.2.1. Шифрирање и анонимизација на податоци: Шифрирањето на податоците е фундаментална безбедносна мерка што вклучува кодирање на податоците така што до нив можат да пристапат само овластени лица со точен клуч за дешифрирање. Универзитетите треба да обезбедат услови за шифрирање и на веќе складираните податоци кои се во мирувањеи на податоците кои се во транзит и се пренесуваат преку мрежи. Оваа мерка помага да се заштитат чувствителните информации од неовластен пристап, дури и ако физичките уреди или комуникациските канали се компромитирани.

Употребата на енкрипција и анонимизација на податоците може значително да го намали ризикот од неовластен пристап. Специфичните видови енкрипција што ќе се користат ќе зависат од потребите на организацијата, природата на податоците што се обработуваат, регулаторните барања, постоечката инфраструктура и техничките услови. Имплементацијата на комбинираните методи на шифрирање ќе помогне да се обезбеди робусна и повеќеслојна одбрана од потенцијални прекршувања на безбедноста на податоците и неовластен пристап.

Три главни методи на енкрипција што е од суштинско значење за имплементација се шифрирање складирани податоци, шифрирање податоци во транзит и шифрирање од крај до крај:

2.2.1.1. Шифрирање складирани податоци се однесува на податоци во мирување кои се складирани на физички уреди како што се сервери, бази на податоци и системи за складирање. Ова спречува неовластен пристап доколку хардверот е украден или компромитиран.

2.2.1.2. Шифрирање податоци во транзит се оденсува на податоците додека тие се пренесуваат низ мрежите, со што се осигурува дека информациите остануваат доверливи и безбедни за време на преносот, особено кога се пристапува до нив од далечина или преку услуги надигитален облак.

2.2.1.3. Шифрирање од крај до крај подразбира обезбедување услови податоците да останат шифрирани од моментот кога се генерирани сè додека не им пристапат овластени примачи, со што се минимизира изложеноста на потенцијални пресретнувачи.

Пристапот кон енкрипцијата опфаќа и други различни методи кои вреди да се имплементираат во безбедносната политика на организацијата.

2.2.2. Контрола на пристап подразбира ограничување на пристапот до лични податоци само на оние лица на кои податоците им се потребни за извршување на нивните работни задачи. Спроведувањето строги контроли на пристапот е клучно за да се овозможи само овластените вработени лицада може да пристапат до чувствителни податоци. Ова може да се постигне преку контрола на пристап базирана на улоги (RBAC), каде што правата за пристап се доделуваат врз основа на улогата на корисникот во рамките на универзитетот. Мултифакторската автентикација (MFA) додава дополнителен степен на безбедност со тоа што бара од корисниците да обезбедат повеќе форми на верификација пред да пристапат до податоци.

2.2.3. Редовни безбедносни ревизии

Спроведувањето редовни безбедносни ревизии помага во идентификување на ранливи точки и обезбедување усогласеност со безбедносните политики. Овие ревизии вклучуваат темелно испитување на ИТ инфраструктурата, политиките и процедурите на универзитетот за откривање потенцијални слабости и области за подобрување. Редовните ревизии исто така помагаат во одржувањеточекор со најновите безбедносни стандарди и најдобри практики.

2.2.4. Резервна копија и обновување податоци

Одржувањето редовни резервни копии на критичните податоци е од суштинско значење за ублажување на влијанието од пробивањето податоци, хардверските дефекти или други катастрофи. Универзитетите треба да имплементираат комплексна стратегија за резервна копија на податоците што вклучува резервни копии на лице место и вон него. Дополнително, постоењето на сеопфатен план за обновување од катастрофи гарантира дека податоците можат брзо да се обноват, минимизирајќи го застојот и губењето на податоци. Високообразовните организации сè повеќе стануваат мета на напади, каде што киберкриминалците шифрираат податоци и бараат плаќање за нивно објавување, што покрај финансиските заканиможе да предизвикува недозволено прекинување на перформансите. Поседувањето ажурирани резервни копии овозможува институциите да ги обноват податоците без да се потчинат на барањата за изнудување, заштитувајќи ги своите финансии и зачувувајќи го интегритетот на нивните информации.

2.2.5. Обука и свест за кибербезбедност

Човечката грешка е значаен фактор кај многу случаи на прекршувања на безбедноста на податоците. Затоа, едукацијата на студентите и вработените лица на факултетот за најдобрите практики за кибербезбедност е од витално значење. Редовните обуки и програмите за подигнување на свеста можат да им помогнат на поединците да препознаат обиди за фишинг, да креираат силни лозинки и да ја разберат важноста на заштитата на чувствителните информации.

Организирањето обука за кибербезбедност за вработените и студентите на факултетите е од суштинско значење за создавање култура на свест, одговорност и будност против киберзаканите. Со едукација на поединци за најдобрите практики за кибербезбедност и потенцијалните ризици, организацијата може значително да ја подобри својата целокупна безбедност на податоците, покрај мерките што се спроведуваат на ниво на ИТ администрација.

Оптимален пристап е да се организира разработена едукативна програма прилагодена на специфичните потреби на организацијата (на пр., безбедност на лозинки, безбедност на е-пошта, безбедно прелистување, ризици од социјалните медиуми, безбедно споделување датотеки) и богата со различни начини на обука на корисниците: работилници, онлајн модули, видеа, вебинари и интерактивни симулации, вклучувајќи и различни стилови на учење.

Исто така е корисно да се организираат еднократни или периодични гостински предавања, поканувајќи говорници и експерти да споделат нивни сознанија, искуства и добри практики, со што би се збогатила содржината на обуката.

Конечно, вработените треба да се обезбедат ресурси како што се совети, инфографици и референтни материјали до кои поединци ќе можат да пристапат по обуката.

2.2.6. Безбедна мрежна инфраструктура

Безбедната мрежна инфраструктура е столбот на безбедноста на податоците. Универзитетите треба да обезбедат заштитни механизми, системи за откривање и спречување на упади и безбедни Wi-Fi мрежи за заштита од неовластен пристап и кибернапади. Редовните ажурирања и поправки на мрежниот хардвер и софтвер се исто така неопходни за нивна заштита.

2.2.7. Усогласеност со законските и регулаторните барања

Универзитетите мора да се придржуваат кон различни законски и регулаторни барања поврзани со заштитата на податоците, како што се Општата регулатива за заштита на податоците (GDPR) која се однесува наевропските земји за разлика од Законот за семејни образовни права и приватност (FERPA) кој важи за Соединетите Американски Држави. Придржувањето кон овие регулативи е гаранција дека универзитетите ракуваат со податоците одговорно, а за неодговорното однесување следат законски казни. Универзитетите во Македонија се должни да се придржуваат кон националните и меѓународните регулативи за заштита на податоците, особено Законот за заштита на личните податоци, кој е усогласен со Општата регулатива за заштита на податоците (GDPR) на Европската Унија. Оваа правна рамка им наложува на високообразовните институции да спроведуваат технички и организациски мерки за да обезбедат законска, транспарентна и безбедна обработка на лични податоци. (Агенција

за заштита на лични податоци, 2020) Усогласеноста не само што ги штити правата на студентите, вработените и истражувачите, туку им помага и на универзитетите да избегнат законски санкции и да не си наштетат на угледот.

2.2.8. План за одговор на инциденти

Постоењето план за брз одговор на инциденти е клучно за ефикасно справување со повреди на податоци или други безбедносни инциденти. Овој план треба да ги наведе чекорите што треба да се преземат во случај на нарушување на безбедноста, вклучително и идентификување на случајот, ограничување на штетата, известување на засегнатите страни и спречување на идни инциденти. Добро подготвен тим за реагирање на инциденти може значително да го намали негативното влијание од повредатана правото на заштита на податоци.

3. Права на субјектите во врска со личните податоци

Централно место во рамката за заштита наподатоци има признавањето на правата на субјектите за заштита на личните податоци во процесот на нивно собирање, складирање и користење. Овие права се вградени и во правните инструменти како што се Општата регулатива за заштита на податоците на ЕУ (GDPR) и националниот Закон за заштита на личните податоци во Северна Македонија. Понатаму во текстот, ќе се осврнеме на клучните права што им се даваат на субјектите за заштита на личните податоци, вклучувајќи го правото на пристап, исправка, бришење, ограничување на обработката и преносливост. Разбирањето и почитувањето на овие права е од суштинско значење за поттикнување на транспарентност, отчетност и доверба во ракувањето со лични податоци во рамките на универзитетите.

3.1. Право на пристап: Студентите и вработените имаат право да знаат кои лични податоци се обработуваат за нив и за кои цели.

3.2. Право на исправка: Студентите и вработените имаат право на исправка на неточни или нецелосни податоци.

3.3. Право на бришење: Студентите и вработените имаат право на барање за бришење на лични податоци што се обработуваат нелегално или повеќе не се потребни.

3.4. Право на ограничување на обработката: Под одредени услови, студентите и вработените имаат право да побараат ограничување на обработката на нивните податоци.

3.5. Право на преносливост: Студентите и вработените имаат право да добијат копија од нивните лични податоци во структуриранаи дигитално читлива форма и да ги пренесат на друг контролор.

Примената на овие мерки и права помага да се обезбеди довербата на субјектите во заштитата на личните податоци во рамки на факултетот и ги штити од потенцијални злоупотреби и повреди на приватноста.

4. Мерки и документи за обезбедување безбедност на податоците на Филозофскиот факултет при УКИМ Скопје

Целта на нашето истражување беше да се анализираат мерките и механизмите преземени на Филозофскиот факултет во Скопје за да се обезбеди заштита на личните податоци. За да се постигне истражувачката цел, спроведовме квалитативно истражување преку полуструктурирани интервјуа со клучни службени лица, вклучувајќи го советникот за настава и наука од Одделението за човечки ресурси на факултетот, офицерот за заштита на лични податоци, раководителот на одделението за студентски прашања и тројца виши соработници за студентски прашања на Филозофскиот факултет. Дополнително, извршивме анализа на содржината на релевантни документи, така што резултатите и заклучоците се изведени од примарните податоци добиени од овие интервјуа и секундарните податоци од прегледот на литература и анализа на документи. За поголема научна релијабилност спроведено е и квантитативно истражување со наставниот, административниот и студентскиот кадар како засегнати страни, но во овој труд главно ги содржи резултатите од квалитативното истражување.

Филозофскиот факултет во Скопје се придржува кон националните и меѓународните прописи за заштита на податоците. Од националното законодавство, примарни документиспоред кои се раководат надлежните лица се Законот за заштита на личните податоци (2020) кој стапи на сила во февруари 2020 година со измени и дополнувања во 2021 година и Правилникот за безбедност на обработка на личните податоци (2020),документи целосно усогласени со европските регулативи. Оваа легислатива ја спроведува и надгледува Агенцијата за заштита на личните податоци (АЗЛП) и се однесува на сите јавни и приватни субјекти, вклучително и универзитетите.

Во согласност со Законот, пред факултетот се поставени повеќе барања, како што се: да назначи службеник (офицер) за заштита на податоци, да води евиденција за активностите за обработка на податоци, да обезбеди согласност за користење на податоците во сите случаи каде што е потребно, да обезбеди минимизирање на податоците, ограничување на складирањето и безбедност на истите, да им овозможува на субјектите (на пр., студенти и вработени) да ги остваруваат своите права (пристап, исправка, бришење на податоци), да ги обучува вработените за заштита на податоците итн. Во согласност барањата, Филозофскиот факултет – Скопје има воспоставено соодветни акти и практики за заштита на личните податоци на сите засегнати страни. Особено се води грижа за безбедноста на информациите поврзани со податоците за студентите, резултатите од

испитите, дискусиите на дигиталните платформи и други податоци поврзани со основната дејност што ја врши факултетот.

Во последниве години, донесени се бројни акти за регулирање на процедурите за заштита на безбедноста на информациите од различна природа, како што се:

4.1. ПОСТАПКА за физички, технички и организациски мерки на Универзитетот „Св. Кирил и Методиј“ во Скопје

4.2. ПРАВИЛНИК за начинот на вршење на видеонадзор.

4.3. ПОСТАПКА за управување и користење лозинки на Филозофски факултет во Скопје

4.4. ПОСТАПКА за управување со правата за пристап на Филозофскиот факултет во Скопје

4.5. КОНЦЕПТ за дневници на Филозофскиот факултет во Скопје

4.6. ПОЛИТИКА за сигурност на интернет на канцелариски уреди и е-пошта на Филозофскиот факултет во Скопје

4.7. ПЛАН за известување, реакција и санација на инциденти до Агенцијата за заштита на лични податоци

4.8. ПОЛИТИКА за менаџмент и ангажирање на менаџери на Филозофскиот факултет во Скопје

4.9. ПОЛИТИКА за приватност на Филозофскиот факултет во Скопје – Универзитет „Св. Кирил и Методиј“ во Скопје

4.10. ПРАВИЛНИК за начинот на обработка на личните податоци на субјектите ангажирани на проекти на Филозофскиот факултет во Скопје.

4.11. ПОСТАПКА за активностите на службеното лице за заштита на личните податоци

4.12. ПОСТАПКА за остварување на правата на субјектот врз личните податоци

4.13. ПРАВИЛА за начинот на уништување на документи, како и начинот на уништување, бришење и чистење на медиумот

4.14. ПОСТАПКА за безбедносна копија (резервна копија) на личните податоци на Филозофскиот факултет во Скопје.

Сите овие документи се јавно достапни на веб-страницата на факултетот http://fzf.ukim.edu.mk/dataprotectiondocs/.

Во однос на начинот на прибирање на податоците, сè се собира во хартиена форма, во согласност со Законот за високо образование и Статутот на Универзитетот „Св. Кирил и Методиј“. Овие документи одредуваат кои податоци треба да се обработуваат во досиејата на студентите. Во процесот на запишување на Факултетот, студентите потпишуваат согласност за обработка на нивните лични податоци. Во исто време, личните податоци се обработуваат само во обем неопходен за соодветната цел и со соодветни технички и организациски методи за заштита на нивната безбедност.

5. Безбедност на електронскиот систем

Филозофскиот факултет како единица на Универзитетот „Св. Кирил и Методиј“ во Скопје ги обработува податоците за студентите во дигитална форма преку електронски систем наречен „I know“, кој го одржува Универзитетот. Во овој систем секој вработен на факултетот и секој регистриран студент може да пристапи до информации за своите активности по извршено безбедносно овластување.

Е-сервисот на Универзитетот „Св. Кирил и Методиј“ во Скопје (УКИМ), кој опфаќа платформи како iKnow, iLearn и Репозиториум, вклучува неколку безбедносни мерки за заштита на податоците на корисниците и обезбедување на интегритетот на системот.

5.1. Применети безбедносни мерки

5.1.1. Еднократно најавување (SSO) преку SEN-UKIM: UKIM го користи системот SEN-UKIM, овозможувајќи им на корисниците пристап до сите електронски услуги со едно најавување. Оваа централизирана автентикација ја подобрува безбедноста со намалување на ризикот од пробивање на лозинката и потенцијалните точки на влез со неовластен пристап.

5.1.2. Централизирана поддршка од службата за помош: Наменската служба за помош го олеснува пријавувањето и решавањето на технички проблеми, обезбедувајќи навремени одговори на потенцијални безбедносни проблеми.

5.2. Размислувања и потенцијални ранливи точки

И покрај придобивките од е-сервисите, како што се транспарентноста и поедноставените процеси, сè уште постои ранливост и можност за хакерски упади. Ова ја нагласува важноста на континуираните безбедносни проценки и ажурирања.

Една од најслабите точки во безбедносната рамка на е-системот на Филозофскиот факултет при Универзитетот „Св. Кирил и Методиј“ е дигиталната инфраструктура, која може да се окарактеризира како скромна. Оваа констатирана слабост не е нова, таа произлегува од долгогодишна нерешена состојба на високообразовните институции во однос на вработување стручен кадар, следствено отсуство на посветен ИТ кадар одговорен за управување и одржување на дигиталните системи на факултетот. Повеќе од една деценија, овој недостатокја изложува инфраструктурата на низа ризици, вклучително и застарен софтвер и недоволно развиени технички услови.

Ограничените финансиски и човечки ресурси дополнително ги ограничуваат можностите на факултетот да имплементира модерни про-

токоли за кибербезбедност. Без соодветен кадар и инвестиции во инфраструктура, основните мерки како што се редовни ажурирања на системот, проценки на ранливите точки и проактивно откривање на закани не можат успешно да се спроведуваат. Ова не само што ги компромитира локалните системи, туку може да создаде и потенцијални точки за упад во пошироките платформи на ниво на целиот универзитет.

Во современата дигитална поставеност, каде што универзитетите сè повеќе се потпираат на интегрирани платформи за администрирање на академските активности и за управување со учењето и истражувачките податоци, ваквите слаби точки претставуваат значителни ризици. За да се реши овој недостаток, потребна е стратешка посветеност и на факултетско и на универзитетско ниво при што треба да се даде приоритет на кибербезбедноста, да се распределат потребните ресурси и да се воспостават технички услови за одржување на дигиталниот екосистем.

6. Заклучок

Заштитата на податоците на универзитет е сложена, но суштествена задача што бара повеќестран пристап. Со спроведување на комплексни безбедносни мерки, спроведување редовни проверки, со едукација на академската заедница и обезбедување усогласеност со законските барања, универзитетите можат да создадат безбедна средина во која ќе се заштитени чувствителните информации,а со тоа ќе се одржи довербата на сите засегнати страни.

Резултатите од истражувањето покажуваат дека Филозофскиот факултет при УКИМ – Скопје воспоставил соодветни политики и практики за заштита на личните податоци на сите засегнати страни. Во последниве години, донесени се дваесетина регулаторни акти за обезбедување различни видови информации, а тие се јавно достапни на веб-страницата на факултетот.

Понатаму резултатите од истражувањето покажуваат дека се воспоставени безбедносни мерки, особено во однос на заштита на личните податоци на студентите и вработените, резултатите од испитите и други податоци поврзани со основната дејност на факултетот. Редовни ревизии и усогласеност со законските стандарди се од суштинско значење за одржување на довербата и интегритетот во академската средина.

Универзитетскиот електронски систем покажува посветеност на безбедноста преку централизирана автентикација и наменски структури за поддршка. Сепак, покажаните ранливи точки и инфраструктурни ограничувања на факултетот укажуваат на можности за подобрување. Во однос на корисниците, придржувањето кон најдобрите практики, како што се користење силни, уникатни лозинки и брзо пријавување на сомнителни активности, може дополнително да ја подобри личната безбедност во рамките на системот.

БИБЛИОГРАФИЈА:

- Закон за заштита на лични податоци (2020). Службен весник на Република Северна Македонија бр. 42 /The Law on Protection of Personal Data (2020), Official Gazette of the Republic of Macedoniano. 42.https://azlp.mk/law on personal data protectioni.pdf
- Закон за изменување и дополнување на законот за заштита на лични податоци (2021). Службен весник на Република Северна Македонија бр. 294 / The Law on Amending and Supplementing the Law on Personal Data Protection (2021). Official Gazette of the Republic of Macedoniano. 294. https://azlp.mk/law on amending the law on personal data protection.pdf
- Правилник за безбедност на обработка на личните податоци (2020). Службен весник на Република Северна Македонија бр. 122 / Rulebook on the Security of Personal Data Processing (2020). Official Gazette of the Republic of North Macedonia No. 122.
- Agency for Personal Data Protection (АЗЛП).(2020). Law on Personal Data Protection [online]. Skopje: Агенција за заштита на личните податоци. Available at: https://dzlp.mk [Accessed 21 May 2025].
- De Hert, P. and Gutwirth, S.(2006). Privacy, data protection and law enforcement: Opacity of the individual and transparency of power. In: E. Claes, A. Duff and S. Gutwirth, eds. Privacy and the criminal law. Antwerp: Intersentia, pp.61–104.
- De Hert, P. and Papakonstantinou, V. (2012). The proposed data protection regulation replacing Directive 95/46/EC: A sound system for the protection of individuals. Computer Law & Security Review, 28(2), pp.130–142.
- ENISA (2016). *Privacy and data protection by design – from policy to engineering*. [online] European Union Agency for Cybersecurity. Available at: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design [Accessed 21 May 2025].
- European Union.(2016). General Data Protection Regulation (EU) 2016/679. Official Journal of the European Union, L119, pp.1–88.
- Greenleaf, G. (2021). Global data privacy laws 2021: Despite COVID delays, 145 laws show GDPR dominance. Privacy Laws & Business International Report, (170), pp.10–13.
- Ifenthaler, D. and Schumacher, C. (2016). Student perceptions of privacy principles for learning analytics. *Educational Technology Research and Development*, 64(5), pp.923–938.

- International Organization for Standardization.(2013). *ISO/IEC 27001:2013 - Information technology — Security techniques — Information security management systems — Requirements*. Geneva: ISO.
- Jisc.(2018). Protecting research data: Managing information security in higher education. [online] Available at: https://www.jisc.ac.uk/guides/protecting-research-data [Accessed 21 May 2025].
- Kerkhove, T.V. and Charlier, N. (2021). Data protection in higher education: A review of data governance policies and practices. *Journal of Higher Education Policy and Management*, 43(5), pp.521–537.
- Smith, R. (2021). Data protection compliance in higher education: A comparative study of GDPR implementation. Journal of Higher Education Policy and Management, 43(3), pp.241–257.Information for Students/e – Services (accessed May 20, 2025). https://ukim.edu.mk/en/studii/informacii-za-studentite/e-servisi/?utm_source=chatgpt.com
- Solove, D.J.(2006). A taxonomy of privacy. University of Pennsylvania Law Review, 154(3), pp.477–560.
- Solove, D.J. (2008). Understanding privacy. Cambridge, MA: Harvard University Press.