SECURITY OF INFORMATION FLOWS IN HIGHER EDUCATION ADMINISTRATION: RISKS AND PROTECTION MEASURES*

EDA E. ZAKIR, DONIKA V. DIMANOVA

ABSTRACT: *The digitalization of administrative processes in higher education institutions leads to an increase in the volume and intensity of information exchange among different structural units, academic staff, students, and external institutions. This creates a need for systematic analysis of the risks associated with the processing, transmission, and storage of information. The paper examines the main vertical and horizontal information flows in university administration, identifies characteristic human, technological, and organizational risks, and analyzes appropriate measures for their mitigation. On this basis, guidelines are formulated for enhancing the security and resilience of the university information environment.*

KEYWORDS: *information flows, information security, higher education institution, cyber risks, access control, information protection*

DOI: https://doi.org/10.46687/MT26EEZ

СИГУРНОСТ НА ИНФОРМАЦИОННИТЕ ПОТОЦИ В АДМИНИСТРАЦИЯТА НА ВИСШЕ УЧИЛИЩЕ: РИСКОВЕ И МЕРКИ ЗА ЗАЩИТА

ЕДА Е. ЗАКИР, ДОНИКА В. ДИМАНОВА

АБСТРАКТ: *Дигитализацията на административните процеси във висшите училища води до увеличаване на обема и интензивността на информационния обмен между различни структурни звена, преподаватели, студенти и външни институции. Това създава необходимост от системен анализ на рисковете, свързани с обработването, предаването и съхранението на информация. В доклада се разглеждат основните вертикални и хоризонтални информационни потоци в университетската администрация, идентифицират се характерни човешки, технологични и организационни рискове и се анализират подходящи мерки за тяхното ограничаване. На тази основа се формулират насоки за повишаване на сигурността и устойчивостта на университетската информационна среда.*

1 Въведение

Дигитализацията на административните и академичните процеси във висшите училища води до значително увеличаване на обема, скоростта и разнообразието на обменяната информация. В ежедневната дейност на университетската администрация се обработват лични, академични, кадрови, финансови и служебни данни, които се предават между различни структурни звена, преподаватели, студенти и външни институции. Това превръща сигурността на информационните потоци в съществен елемент от надеждното функциониране на университетската среда [1, 2].

Информационните потоци представляват процес на създаване, обработване, предаване, използване и съхранение на информация между отделни участници и системи. Във висшето училище те могат да бъдат както вертикални - между различни управленски нива, така и хоризонтални - между равнопоставени административни и академични звена.

* Докладът е частично финансиран по проект РД-08-94/03.02.2026 г. „Експериментална и изследователска среда за моделиране, анализ и оптимизация на производствени процеси и технологии“

Ефективното им управление подпомага координацията, административното обслужване и процесите на вземане на решения, но едновременно с това създава необходимост от надеждна защита на използваните комуникационни канали и информационни ресурси [4, 5]. Уязвимостите на безжична компютърна мрежа, защитена с WPA2, са анализирани в [7].

Разнообразието от използвани информационни системи, електронна поща, системи за електронен документооборот, облачни услуги и други цифрови платформи увеличава възможностите за бърз обмен на информация, но също така разширява потенциалната повърхност за възникване на инциденти. Сред основните рискове се открояват неоторизираният достъп, загубата или неправомерното разкриване на данни, човешките грешки, неправилното управление на потребителските права, техническите неизправности и кибератаките [2, 3, 18].

Сигурността на информационните потоци не може да бъде осигурена единствено чрез технически средства. Необходимо е съчетаване на организационни правила, контрол на достъпа, ясни процедури, обучение на служителите, актуализиране на системите и надеждни механизми за архивиране и възстановяване. Подобен комплексен подход създава условия за ограничаване на рисковете и за поддържане на устойчиво функциониране на университетската информационна среда [1, 2].

Целта на настоящия доклад е да се анализират основните информационни потоци в администрацията на висше училище, да се идентифицират характерните рискове за тяхната сигурност и да се систематизират организационни и технически мерки за тяхното ограничаване.

За постигане на поставената цел се използват методите на анализ, сравнение и систематизиране на специализирани и нормативни източници, както и структурен анализ на основните информационни взаимодействия в университетската администрация.

2 Информационни потоци в администрацията на висше училище

Информационните потоци в администрацията на висше училище представляват съвкупност от процеси по създаване, предаване, обработване, съхранение и използване на информация между различните участници в академичната и административната дейност. Те осигуряват координацията между ръководните органи, административните звена, преподавателите, студентите и външните институции и имат пряко значение за ефективността на управленските и обслужващите процеси [4, 5].

В зависимост от посоката на движение на информацията могат да бъдат разграничени два основни типа потоци - вертикални и хоризонтални. Вертикалните информационни потоци се осъществяват между различни йерархични равнища и осигуряват предаването на управленски решения, отчети, справки, указания и обратна връзка. Те подпомагат контрола върху изпълнението на поставените задачи и проследимостта на административните действия. Основните рискове при този тип обмен са свързани със забавяне на информацията, непълнота, дублиране, информационни изкривявания и недостатъчна координация между отделните управленски нива [4].

Хоризонталните информационни потоци се реализират между структурни звена и служители, намиращи се на едно и също организационно равнище. Те имат важно значение за координацията между факултети, катедри, учебни и административни отдели и подпомагат съвместното изпълнение на дейности, обмена на документи и подготовката на управленска информация. Използването на динамични масиви в MS Excel за обработка и анализ на данни в информационни системи е разгледано в [20]. Недостатъчната

комуникация, липсата на единни информационни стандарти и дублирането на дейности могат да намалят ефективността на този обмен [4, 5].

В университетската администрация могат да бъдат откроени няколко основни информационни взаимодействия (фигура 1). Потокът „Студент - Учебен отдел“ включва данни, свързани със записване, академичен статус, оценки, заявления и документи по дипломиране. Потокът „Преподавател - Администрация“ обхваща информация за преподавателска натовареност, учебни графици, изпитни протоколи и отчетност на учебната дейност. Съществено значение има и двупосочният обмен между факултетите и ректората, както и между университета и външни институции, при който се предават отчетни, нормативни, кадрови и статистически данни.



Фигура 1. Основни информационни потоци в администрацията на висше училище

Представената структура показва, че информационните потоци във висшето училище образуват взаимосвързана мрежа, в която нарушаването на сигурността в един канал или звено може да окаже влияние върху други административни и академични процеси [6].

Наред с външните взаимодействия, съществена роля имат и вътрешните административни потоци между отделите „Човешки ресурси“, финансово-счетоводните звена, деловодството и информационно-технологичните структури. Този обмен е необходим за поддържане на кадровите, финансовите и организационните процеси и се осъществява чрез вътрешни информационни системи, електронен документооборот, електронна поща и специализирани програмни продукти. Приложението на облачните технологии в образованието е разгледано в [10].

С развитието на цифровата среда значението на интегрираните информационни системи нараства, тъй като те позволяват еднократно въвеждане и многократно използване на данните, по-добра проследимост на обработката и по-ефективна координация между

отделните звена [5]. Същевременно концентрацията на значителни масиви от информация в електронна среда увеличава необходимостта от надеждно управление на достъпа, защита на комуникационните канали и ясно регламентиране на отговорностите при работа с данни.

От гледна точка на сигурността всеки информационен поток следва да бъде разглеждан като последователност от етапи: създаване, предаване, обработване, съхранение и последващо използване на информацията. На всеки от тези етапи могат да възникнат различни рискове, свързани с неправомерен достъп, загуба, изменение, неправилно адресиране или нарушаване на достъпността на данните. Поради това защитата следва да бъде насочена не само към отделните информационни системи, а към целия жизнен цикъл на информационния поток. Връзката между информационната и административната сигурност е разгледана в [9], а защитата на административните процеси от външни и вътрешни заплахи е обсъдена в [12].

3 Основни рискове за сигурността на информационните потоци

Рисковете за сигурността на информационните потоци могат да възникнат на всеки етап от движението на информацията - от нейното създаване и предаване до обработването, съхранението и последващото използване. Характерът на риска зависи от вида на информацията, използвания комуникационен канал, правата за достъп и организационните процедури, чрез които се осъществява конкретният информационен обмен. Анализът на причините и последствията като метод за управление на риска е разгледан в [14].

Основните рискове могат да бъдат систематизирани в три взаимно свързани групи: човешки, технологични и организационни. Подобно разграничение позволява по-ясно да бъдат установени уязвимите точки по движението на информацията и да бъдат определени подходящи мерки за защита.

Човешките рискове възникват преди всичко при създаването, обработването и предаването на информация. Типични проявления са използването на слаби или повтарящи се пароли, споделянето на потребителски акаунти, неправилното адресиране на електронни съобщения, грешното изпращане на документи и недостатъчната способност за разпознаване на фишинг и други форми на социално инженерство [3]. Подобни действия могат да доведат до нарушаване на конфиденциалността и целостта на информацията дори когато са внедрени технически механизми за защита. Прилагането на FMEA за оценка на човешката надеждност е разгледано в [13].

Технологичните рискове са свързани с инфраструктурата и системите, чрез които се осъществява движението на информацията. Софтуерни уязвимости, технически неизправности, прекъсване на комуникационни услуги, компрометиране на потребителски профили, зловреден софтуер и ransomware могат да доведат до загуба, изменение или недостъпност на информацията [2, 18]. Рискът се увеличава, когато различни системи функционират без достатъчна интеграция или когато липсват последователни политики за актуализиране, удостоверяване и контрол на достъпа.

Организационните рискове произтичат от недостатъчно ясно регламентирани правила за движение и обработване на информацията. Липсата на единни процедури за предоставяне и прекратяване на права за достъп, обмен на електронни документи, архивиране, регистриране на инциденти и управление на риска може да доведе до дублиране, забавяне, непълнота и затруднена проследимост на информационните потоци [1].

Характерът на риска се различава и според конкретния административен поток. При взаимодействието „Студент - Учебен отдел“ основен акцент е защитата на личните и

академичните данни. При потока „Преподавател - Администрация“ особено значение имат целостта и точността на изпитните протоколи, учебните графици и отчетната информация. При обмена „Факултети - Ректорат“ и „Университет - Външни институции“ се увеличава значението на навременното и коректно предаване на управленски, кадрови, нормативни и статистически данни.

Особено чувствителни точки във всички тези потоци са електронната поща, системите за електронен документооборот и платформите за споделена работа. Неправилното адресиране, недостатъчният контрол върху споделените ресурси и неправилното управление на потребителските права могат да доведат до неоторизиран достъп, загуба или неправомерно разкриване на информация.

В обобщение, сигурността на информационните потоци зависи не само от защитата на отделните информационни системи, а от надеждността на целия процес на движение на информацията между източника, обработващото звено и крайния получател.

4 Организационни и технически мерки за защита на информационните потоци

Ефективната защита на информационните потоци изисква мерките за сигурност да обхващат всички етапи от техния жизнен цикъл: създаване, предаване, обработване, съхранение и архивиране на информацията. Организационните и техническите механизми следва да се прилагат съгласувано, тъй като надеждността на информационния обмен не може да бъде осигурена само чрез технологични решения [1, 2].

Организационните мерки трябва да определят правилата за движение на информацията между отделните звена, отговорностите на участниците и допустимите комуникационни канали. Особено значение имат процедурите за предоставяне, промяна и прекратяване на права за достъп, работа с електронни документи, обмен на чувствителна информация и реагиране при инциденти [1].

Класифицирането на информацията според нейната чувствителност позволява различните информационни потоци да бъдат защитени в съответствие с характера на предаваните данни. Публичната, служебната, поверителната и критичната информация изискват различни нива на достъп, контрол и проследимост. По този начин защитните механизми могат да бъдат съобразени не само със системата, в която се намират данните, но и с тяхното движение между различните участници.

Съществен организационен елемент е и проследимостта на информационния поток. Възможността да се установи кой е създал, получил, променил или предоставил дадена информация намалява риска от неоторизирани действия и подпомага анализа на възникнали инциденти. Наблюдението на комуникационните мрежи с Wireshark е разгледано в [16], компютърната сигурност и управлението на трафика в [17], а съвременните киберзаплахи в [18].

Техническите мерки следва да осигуряват защита както на самите информационни системи, така и на каналите, чрез които информацията се предава. Те включват надеждно удостоверяване, контрол на достъпа, многофакторна автентикация (MFA), криптиране при необходимост, актуализиране на системите и защита на електронните комуникации [2, 17].

Особено значение имат мерките за гарантиране на достъпността и непрекъсваемостта на информационните потоци. Редовното архивиране и периодичното тестване на процедурите за възстановяване ограничават последствията от технически повреди, човешки грешки и ransomware и позволяват възстановяване на критичните административни процеси.

По този начин защитата на информационните потоци следва да се реализира като система от взаимно допълващи се организационни и технически механизми, които осигуряват конфиденциалност, целостност, достъпност и проследимост на информацията през целия ѝ жизнен цикъл. По-общите проблеми на информационната защита в системата на националната и корпоративната сигурност са разгледани в [15].

5 Насоки за повишаване на сигурността на информационните потоци

Повишаването на сигурността на информационните потоци следва да бъде насочено не само към внедряване на допълнителни технически средства, а към подобряване на начина, по който информацията се движи между отделните структурни звена и информационни системи.

На първо място е необходимо стандартизиране на информационните потоци чрез ясно определяне на източника, получателя, вида на информацията, допустимите комуникационни канали и отговорностите при всеки основен административен процес. Това би ограничило дублирането на данни, използването на неофициални канали и риска от неправилно адресиране на документи.

Второ направление е повишаването на проследимостта. Информационните системи и системите за електронен документооборот следва да осигуряват възможност за проследяване на основните действия с информацията: създаване, достъп, изменение, предаване и архивиране. Това позволява по-ефективен контрол и по-бързо установяване на причините при възникване на инцидент.

Съществен потенциал има интеграцията на административните информационни системи. Свързването на отделни системи и регистри може да ограничи многократното въвеждане на една и съща информация, да намали риска от несъответствия и да осигури по-висока актуалност на данните [5]. Интеграцията обаче следва да бъде съпроводена с ясно управление на правата за достъп и защита на обмена между системите.

Необходимо е също така да бъде въведен подход, основан на критичността на информационните потоци. Потокове, свързани с лични данни, академични резултати, финансови операции или кадрова информация, следва да бъдат идентифицирани като приоритетни и за тях да се прилагат по-високи изисквания за удостоверяване, контрол, архивиране и възстановяване.

Развитието на културата за информационна сигурност остава важен елемент, тъй като служителите са непосредствени участници в движението на информацията. Обученията следва да бъдат ориентирани към конкретни ситуации от ежедневната работа: изпращане на документи, работа с чувствителни данни, използване на електронна поща, разпознаване на фишинг и правилно реагиране при инциденти [1, 3]. Наред с подготовката за работа с текущо използваните информационни системи, обучението следва да развива и компетентности за критично и безопасно използване на нововъзникващи цифрови технологии [8, 11].

Сигурността на информационните потоци следва да бъде обект на периодична оценка и актуализиране. Промени в структурата на университета, въвеждането на нови системи или услуги и появата на нови рискове могат да променят начина, по който информацията се движи, и съответно да изискват адаптиране на защитните механизми. Модел за управление на административната сигурност в община е предложен в [19] и представлява отделен пример от публичната администрация.

В обобщение, устойчивото управление на информационните потоци предполага тяхното ясно дефиниране, стандартизиране, проследяване и защита през целия жизнен цикъл. Подобен подход позволява сигурността да бъде интегрирана в самата организация на информационния обмен, а не да се прилага като допълнителен слой след изграждането на административните процеси.

6 Заключение

Сигурността на информационните потоци в администрацията на висше училище е съществен фактор за надеждното функциониране на административните и академичните процеси. Разнообразието от участници, системи и комуникационни канали създава сложна информационна среда, в която рисковете могат да възникнат както вследствие на човешки грешки, така и поради технологични уязвимости и организационни слабости.

Анализът показва, че ефективната защита на информационните потоци изисква интегриран подход, който съчетава ясни организационни правила, надежден контрол на достъпа, подходящи механизми за удостоверяване, редовно актуализиране на системите, защита на комуникационните канали и устойчиви процедури за архивиране и възстановяване.

Особено значение има системното управление на риска и развитието на култура за информационна сигурност сред служителите. Прилагането на съгласувани организационни и технически мерки създава предпоставки за по-надежден, проследим и устойчив обмен на информация и подпомага ефективното функциониране на университетската информационна среда.

ЛИТЕРАТУРА:

[1] Василев, Д. Управление на информационна сигурност в образователните институции: политики, процедури и добри практики. Варна: Наука и икономика, 2024, с. 213–219. ISBN 978-954-21-1184-9.

[2] Димов, П., Здравков, З., Добрева, Х. Информационна сигурност. ВА „Г. С. Раковски“, София, 2021.

[3] Домозетов, Х. Човешки фактор и информационна сигурност. В: Information & Security: An International Journal, 1998, № 1, с. 46–60.

[4] Загорчева-Койчева, Д. П. Система за успешно управление на образователна институция. Университетско издателство „Епископ Константин Преславски“, Шумен, 2022.

[5] Игнатов, И. И. Интегрирана информационна система за управление на процесите и дейностите във Военна академия „Г. С. Раковски“. В: Сборник доклади от Годишна научна конференция „110 години традиция, качество, престиж“, част III. София: Военна академия „Г. С. Раковски“, 2022.

[6] Методиева, Ц., Анализ на индикаторите в образователните услуги за сектор сигурност. Сборник с доклади от дискусионна кръгла маса на тема: Академични партньорства в сферата на националната сигурност, 12-13 май 2022 г., стр. 37-43, ISBN 978-619-201-571-8.

[7] Николов Л. Анализ на уязвимостта на безжична компютърна мрежа, защитена с криптографски протокол WPA2. Proceedings of the XXVI International Scientific Conference Trans&Motauto, Burgas, 2018, Vol. 2, pp. 252–253, ISSN 1313-5031 (Print), ISSN 2535-0307 (Online).

[8] Стоицов, Г. Информационна и комуникационна сигурност. ПУ „Паисий Хилендарски“, Пловдив, 2020.

[9] Симеонова И. Дефиниране на информационната сигурност като основен канал на административната сигурност. Научна конференция с международно участие MATTEX 2022, Шуменски университет „Епископ Константин Преславски“, Шумен, 13–14 май 2022.

[10] Стоянова, В. Облачни технологии в образованието. Сборник научни трудове на факултет „Артилерия, ПВО и КИС“ на НВУ „Васил Левски“, Шумен, 2011, с. 76–82. ISSN 1313-7433.

[11] Tasinov, T. Y., Toncheva, S. K. Anticipatory Technological Preparation and Digital Health Competencies in Nursing and Midwifery Education. In: Conference Proceedings, XIX National Forum of Health Care Specialists and Poster Session for Students „Fair Access to Quality Health Care“, Shumen, 24–25 October 2025, pp. 97–103.

[12] Тахиров М., Симеонова И. Защита на административните процеси от външни и вътрешни заплахи. Научна конференция на НВУ „Васил Левски“, Велико Търново, 12–14 ноември 2025.

[13] Arabadzhieva-Kalcheva N., Tsankov Ts., Todorova M., Marinova G. Application of Failure Mode and Effects Analysis for Evaluating Human Reliability. Scientific Conference with International Participation MATTEH 2024, Conference Proceedings, Vol. 2, Shumen, 2024, ISSN 1314-3921, pp. 147–152. https://doi.org/10.46687/BOIK9859

[14] Arabadzhieva-Kalcheva N., Tsankov Ts., Todorova M. Cause-Consequence Analysis as a Risk Management Method. Annual of Konstantin Preslavsky University of Shumen, Vol. XIV E, Faculty of Technical Sciences, 2024, ISSN 1314-8818, pp. 184–188. https://doi.org/10.46687/YT24NEL

[15] Denev, D., Konstantinova, E. Main Issues in the Protection of Information in the System of National and Corporate Security. Proceedings of the Scientific Conference with International Participation MATTEH 2020, Vol. 2, Communication and Computer Technologies, Shumen, 2020.

[16] Denev, D. Surveillance with Wireshark and its Use in Communication Networks. Annual of Konstantin Preslavski University of Shumen, Vol. XIII E, 2023, pp. 104–109, ISSN 1314-8818.

[17] Iliev, D., Denev, D. Computer Security and Traffic Management in Communication Networks. Proceedings of the Scientific Conference with International Participation MATTEH 2024, Vol. 2, Communication and Computer Technologies, Shumen, 2024, pp. 161–169, ISSN 1314-3921.

[18] Nikolov, L., Slavyanov, K. On the Contemporary Cybersecurity Threats. Proceedings of the First International Scientific Conference CONFSEC 2017, Borovets, 11–14 December 2017, pp. 142–144, ISSN 2603-2945 (Print), ISSN 2603-2953 (Online).

[19] Simeonova, I., Metodieva, Ts. Model for administrative security management in a municipality. Journal Scientific and Applied Research, Vol. 26, 2024, pp. 93–105, ISSN 1314-6289 (Print), ISSN 2815-4622 (Online).

[20] Todorova-Lazarova, V. P. Dynamic Arrays in MS Excel for Data Processing and Analysis in Information Systems. International Scientific Conference UNITECH 2025, Gabrovo, 2025, pp. 1–6, ISSN 1313-230X.