ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УНИВЕРСИТЕТАХ АВСТРИЙСКОЙ РЕСПУБЛИКИ

М.В. Павлова, *студент*
Научный руководитель: *Н.А. Каталкина, канд. филол. наук, доцент*
Санкт-Петербургский политехнический университет Петра Великого
(Россия, г. Санкт-Петербург)

DOI:10.24412/2500-1000-2026-5-1-361-366

Аннотация. *В статье проведен анализ политики информационной безопасности в университетской среде Австрийской Республики. В работе рассматриваются Австрийской стратегии кибербезопасности и положения национального законодательства о защите данных (DSG) в его взаимосвязи с Общеевропейским регламентом о защите персональных данных (GDPR). Проанализирована эволюция подходов к обеспечению информационной безопасности в академической среде, начиная с основополагающих принципов и заканчивая современными вызовами. В ходе исследования определены направления университетских политик: управление доступом, защита данных, реагирование на инциденты, обучение и повышение осведомленности пользователей. Сформулированы выводы о текущем состоянии и уровне зрелости систем управления информационной безопасностью в австрийских университетах, а также обозначены перспективные направления для их дальнейшего совершенствования в условиях постоянно растущих киберугроз.*

Ключевые слова: *информационная безопасность; кибербезопасность; политика безопасности; защита данных; GDPR; австрийские университеты; академическая среда; персональные данные; управление рисками.*

В эпоху цифровизации высшие учебные заведения становятся зависимыми от информационных технологий, которые пронизывают все аспекты их деятельности – от учебного процесса и научных исследований до административного управления. Университеты Австрии, являясь важными центрами образования и науки в Европе, аккумулируют и обрабатывают огромные объемы ценной информации, персональные данные студентов и сотрудников, результаты уникальных научных исследований, финансовую и административную документацию. Информационные активы представляют собой привлекательную цель для киберпреступников, что делает вопрос обеспечения информационной безопасности критически важным для стабильного функционирования и сохранения репутации академических учреждений.

Актуальность данного исследования обусловлена возрастающим количеством и сложностью киберугроз (фишинговые атаки, программы-вымогатели, утечки данных и кибершпионаж), с которыми сталкиваются университеты по всему миру. В Австрийской Республике проблема усугубляется необходимостью соблюдения строгого европейского и национального законодательства в области защиты данных, в первую очередь Общеевропейского регламента о защите персональных данных (GDPR) и национального Закона о защите данных.

Основная часть. Политика информационной безопасности в австрийских университетах формируется и реализуется стратегическими документами и законодательными актами (Закона о защите данных). Основным документом является Австрийская стратегия кибербезопасности и законодательство в области защиты данных. В 2013 году правительство Австрии приняло два основополагающих документа: «Австрийскую стратегию безопасности» [6] и «Австрийскую стратегию кибербезопасности» [1], которые признают киберугрозы одними из наиболее серьезных вызовов национальной безопасности в XXI веке. «Австрийская стратегия кибербезопасности» определяет комплексный подход к защите национального киберпространства, который содержит превентивные, реактивные и оперативные меры. Стратегия подчеркивает важность защиты критической инфраструктуры, частью которой, безусловно, являются и крупные университеты, как центры знаний и

инноваций. В документе отмечается необходимость повышения уровня осведомленности о киберугрозах и развития компетенций в области кибербезопасности на всех уровнях академического сектора. Как отмечает Х. Капониг, реализация национальной стратегии требует постоянной адаптации к меняющемуся ландшафту угроз и тесного сотрудничества между государственным и частным секторами, а также с научным сообществом [4]. Университеты, таким образом, выступают не только как объект защиты, но и как партнер государства в подготовке квалифицированных кадров и проведении исследований в области кибербезопасности.

Правовое регулирование информационной безопасности в Австрии был изменен с вступлением в силу 25 мая 2018 года Общеевропейского регламента о защите персональных данных (GDPR). Для имплементации и конкретизации положений GDPR в национальное законодательство принят обновленный Закон о защите данных (Datenschutzgesetz – DSG) [2]. Указанные нормативные акты устанавливают строгие требования к обработке персональных данных студентов, преподавателей и сотрудников университетов. Основными принципами, закрепленными в GDPR, являются законность, справедливость и прозрачность обработки, ограничение цели, минимизация данных, точность, ограничение хранения, целостность и конфиденциальность. Для университетов означает необходимость внедрения организационных и технических мер для обеспечения соответствия (согласие). Они обязаны назначать уполномоченного по защите данных, проводить оценку воздействия на защиту данных для рискованных процессов обработки, вести реестр операций по обработке данных и уведомлять надзорный орган и субъектов данных об утечках. Надзорным органом в Австрии является Управление по защите данных [3], которое уполномочено проводить проверки и налагать штрафы за нарушения. Кроме того, деятельность Управления по защите данных регулируется дополнительными актами, например, постановлением об аккредитации органов мониторинга в соответствии со ст. 41 GDPR [7], что свидетельствует о развитии комплексной системы контроля за соблюдением законодательства.

Академическая среда отличается от корпоративного или государственного секторов и создает специфические вызовы для обеспечения информационной безопасности. Как отмечали еще В. Махнич, Я. Уратник и Н. Забкар, основной миссией университетов является создание, сохранение и распространение знаний [5]. По мнению авторов, миссия предполагает культуру открытости, сотрудничества и свободного обмена информацией, что зачастую вступает в противоречие с принципами строгой конфиденциальности и контроля доступа, лежащими в основе классических моделей информационной безопасности.

К основным вызовам информационной безопасности в университетах Австрийской Республики относятся:

- Гетерогенность пользователей и устройств. Университетская сеть объединяет множество различных групп пользователей (студенты, преподаватели, административный персонал, исследователи, гости) с разными правами доступа и уровнями технической грамотности. Кроме того, распространение концепции BYOD (Bring Your Own Device) означает, что к сети подключается огромное количество личных устройств (ноутбуков, смартфонов, планшетов), которые находятся вне прямого контроля IT-служб университета и могут быть источником угроз.

- Децентрализованная структура. Многие университеты имеют сложную, децентрализованную структуру, состоящую из множества факультетов, институтов и исследовательских центров. Подразделения часто обладают значительной автономией в управлении своими IT-ресурсами, которые затрудняют внедрение единой, общеуниверситетской политики безопасности и создает «серые зоны» в периметре защиты.

- Ценность информационных активов. Университеты являются хранителями чрезвычайно ценной информации и не только персональные данные тысяч людей, но и результаты передовых научных исследований, которые представляют коммерческую или стратегическую ценность и быть объектом промышленного или государственного кибершпионажа.

- Баланс между безопасностью и открытостью, главный вызов заключается в поиске

оптимального баланса между необходимостью защиты информации и обеспечением открытой среды для обучения и исследований. Чрезмерно строгие меры безопасности могут препятствовать академической свободе и совместной работе, в то время как недостаточный контроль создает неприемлемые риски.

Для оценки практической реализации подходов к информационной безопасности был проведен анализ политик и документов ведущих государственных университетов Австрии. Результаты анализа сведены в таблицу 1.

Таблица 1. Сравнительная политика информационной безопасности в различных университетах Австрийской Республики [1, 2, 3, 6]

№	Университет	Особенности политики
1	Венский университет	Комплексный подход с выделенным отделом IT-безопасности. Публикуются регулярные предупреждения об угрозах. Основной документ " Руководящие принципы ИТ-безопасности ". Особое внимание уделяется защите от фишинга и безопасному использованию электронной почты. Наличие команды по работе с информационной безопасностью.
2	Венский технический университет	Сильный акцент на технических аспектах безопасности. Наличие собственной команды реагирования на инциденты. Политика использования IT-сервисов (условия эксплуатации) четко регламентирует права и обязанности пользователей. Рекомендации по настройке безопасного Wi-Fi.
3	Венский медицинский университет	Повышенные требования к безопасности в связи с обработкой чувствительных медицинских данных пациентов и участников исследований. Четкие инструкции по обращению с персональными и медицинскими данными. Обязательное обучение для сотрудников.
4	Венский университет экономики и бизнеса	Детально проработанные политики паролей и управления доступом. Разработаны отдельные руководства по безопасному использованию мобильных устройств и облачных сервисов. Проводятся кампании по повышению осведомленности.
5	Грацский университет имени Карла и Франца	Наличие общедоступной «Политики безопасности», определяющей цели и принципы ИБ. Развитая система управления учетными записями. Рекомендации по шифрованию данных и безопасному удалению информации.
6	Грацский технический университет	Наличие выделенной роли Директору по информационной безопасности (CISO). Развитая система классификации данных. Публикуются руководства по различным аспектам ИБ, безопасность веб-приложений и защиту конечных точек.
7	Инсбрукский университет имени Леопольда и Франца	Политика использования IT-ресурсов является основным регулирующим документом. Акцент на ответственности пользователей. Рекомендации по резервному копированию и защите от вредоносного ПО.
8	Зальцбургский университет	Четко структурированный портал по IT-безопасности. Наличие команды CERT. Политика информационной безопасности определяет организационную структуру управления ИБ. Регулярная информационная рассылка по вопросам безопасности.
9	Университет Иоганна Кеплера в Линце	Комплексный подход, имеющий технические и организационные меры. Наличие централизованной службы поддержки пользователей по вопросам ИБ. Руководства по безопасному поведению в сети и защите персональных данных.
10	Клагенфуртский университет	Основные правила изложены в "Условиях использования" IT-сервисов. Особое внимание уделяется правилам использования электронной почты и сети. Предоставляются инструкции по защите от спама и фишинга.

Анализ данных, представленных в таблице, показал, что все ведущие австрийские университеты признают важность информационной безопасности и имеют специализированные отделы или, как минимум, выделенных ответственных лиц, занимающихся этим вопросом. У большинства крупных университетов (например, Венский университет, Грацский технический университет, Венский технический университет, Университет Зальцбурга) созданы собственные команды реагирования на инциденты информационной безопасности (CERT – Группа реагирования на компьютерные инциденты), что свидетельствует о высоком уровне зрелости их подхода.

Основным документом, регулирующим поведение пользователей, в большинстве случаев является «Политика использования IT-

сервисов» (условия эксплуатации) или аналогичный документ. Указанные документы носят обязывающий характер для всех студентов и сотрудников и устанавливают базовые правила поведения в цифровой среде университета. Однако, такие документы как «Политика информационной безопасности» или «Руководство по IT-безопасности», определяющие стратегические цели, организационную структуру и распределение ответственности, доступны публично не во всех университетах [5].

Также, наблюдается общая тенденция к усилению внимания к защите персональных данных, которое является прямым следствием вступления в силу Общеевропейского регламента о защите персональных данных (GDPR). Университеты активно информируют пользователей о правилах обработки данных, публикуют политики конфиденциальности и предоставляют контакты уполномоченных по защите данных. Особенно высокие требования предъявляются в медицинских университетах (как, например, в Венский медицинский университет), где обрабатываются особо чувствительные категории персональных данных.

Значительное внимание уделяется повышению осведомленности пользователей. Университеты используют свои веб-сайты для публикации новостей, предупреждений о текущих угрозах (особенно о фишинговых кампаниях), а также предоставляют подробные инструкции и рекомендации по таким вопросам, как создание надежных паролей, безопасное использование Wi-Fi, шифрование данных и защита от вредоносного ПО.

Несмотря на общие подходы, существуют и различия. Технические университеты (Грацский технический университет, Венский технический университет) делают больший акцент на технических аспектах и стандартах безопасности, в то время как классические университеты больше фокусируются на правилах поведения пользователей. Уровень детализации и доступности публичной информации также варьируется. Некоторые университеты, как Грацский университет имени Карла и Франца, предоставляют структурированную и детальную информацию о своей системе управления информационной безопасностью (CISO и принципов классификация данных).

В целом, можно констатировать, что австрийские университеты демонстрируют ответственный и системный подход к обеспечению информационной безопасности, стремясь соответствовать как национальным стратегическим целям, так и строгим требованиям законодательства о защите данных.

Перспективными направлениями для дальнейшего совершенствования политик информационной безопасности в австрийских университетах является:

- гармонизация и стандартизация базовых подходов между университетами для облегчения межуниверситетского сотрудничества;
- дальнейшее развитие риск-ориентированного подхода с внедрением формализованных процедур оценки рисков и классификации информационных активов;
- усиление практической составляющей в обучении пользователей, проведение регулярных симуляций фишинговых атак;
- активное участие в национальных и международных инициативах по обмену информацией об угрозах и передовом опыте в области академической кибербезопасности.

Заключение. Проведенное исследование политики информационной безопасности в университетах Австрийской Республики показало, что академический сектор страны достиг значительного прогресса в создании и поддержании безопасной цифровой среды. Деятельность университетов в этой области строится на прочном фундаменте национального законодательства, в частности Закона о защите данных (DSG) и общеевропейского регламента GDPR, а также соответствует целям, заложенным в Австрийской стратегии кибербезопасности.

Австрийские университеты перешли от фрагментарного, преимущественно технического подхода к информационной безопасности к комплексной системе управления, которая имеет административные, организационные и образовательные компоненты. Практически все ведущие университеты имеют формализованные политики, регламентирующие использование IT-ресурсов, и уделяют большое внимание информированию и обучению пользователей, для снижения рисков, связанных с человеческим фактором. Создание спе-

циализированных подразделений и команд реагирования на инциденты (CERT) свидетельствует о высоком уровне институциональной зрелости в вопросах кибербезопасности.

Сравнительный анализ показал наличие общих подходов, таких как обязательное регулирование прав и обязанностей пользователей, управление доступом на основе учетных записей и активная борьба с фишингом. Вместе с тем, были выявлены и различия в степени детализации и публичной доступности стратегических документов, а также в акцентах, которые расставляются в зависимости от профиля университета (технический, медицинский, гуманитарный).

Несмотря на достигнутые успехи, перед университетским сообществом Австрии стоят и будущие вызовы. К ним относятся постоянно эволюционирующие киберугрозы, необходимость обеспечения информационной безопасности в условиях использования облачных технологий и мобильных устройств. Также постоянный поиск баланса между безопасностью и академической открытостью, о котором писали исследователи еще на заре становления университетских информационных систем.

В целом, политика информационной безопасности в австрийских университетах представляет динамично развивающуюся систему, которая адекватно реагирует на современные вызовы и создает необходимые условия для защиты ценных информационных ресурсов в сердце европейской науки и образования.

Библиографический список

1. Austrian Cyber Security Strategy. – Vienna, 2013. – [Электронный ресурс]. – Режим доступа: https://www.bmi.gv.at/504/files/130415_strategie_cybersicherheit_en_web.pdf.

2. Austrian Data Protection Act 2018 (DPA 2018). Rechtsinformationssystem des Bundes. – [Электронный ресурс]. – Режим доступа: https://www.ris.bka.gv.at/Dokumente/Erv/ERV_1999_1_165/ERV_1999_1_165.pdf.

3. Austrian Data Protection Authority. – [Электронный ресурс]. – Режим доступа: https://www.dsb.gv.at.

4. Kaponig, H. Austria’s National Cyber Security and Defense Policy: Challenges and the Way Forward / H. Kaponig // ICT & Cyber Security Center, Austrian Armed Forces. – 2020. – Vol. 1. – P. 21-37.

5. Mahnic, V. Information Security of University Information Systems / V. Mahnic, J. Uratnik, N. Zabkar // Zukunft der Netze – Die Verlezbarkeit meistern: 16. DFN-Arbeitstagung über Kommunikationsnetze, Düsseldorf. – 2002. – P. 97-105.

6. Österreichische Sicherheitsstrategie: Sicherheit in einer neuen Dekade – Sicherheit gestalten. – Vienna, 2013. – [Электронный ресурс]. – Режим доступа: https://www.bmi.gv.at/502/files/130717_Sicherheitsstrategie_Kern_A4_WEB_barrierefrei.pdf.

7. Regulation of the Austrian Data Protection Authority on the requirements for accreditation of a monitoring body pursuant to Art 41 (1) GDPR (Federal Law Gazette II No. 264/2019).

INFORMATION SECURITY POLICY AT UNIVERSITIES OF THE REPUBLIC OF AUSTRIA

M.V. Pavlova, *Student*
Supervisor: *N.A. Katalkina, Candidate of Philological Sciences, Associate Professor*
Peter the Great St. Petersburg Polytechnic University
(Russia, St. Petersburg)

Abstract. *The article analyzes the information security policy in the university environment of the Republic of Austria. The paper examines the Austrian Cybersecurity Strategy and the provisions of national data protection legislation (DSG) in its relationship with the Pan-European Regulation on Personal Data Protection (GDPR). The article analyzes the evolution of approaches to ensuring information security in the academic environment, starting with the fundamental principles and ending with modern challenges. The research identified areas of university policy: access management, data protection, incident response, training and user awareness. Conclusions are drawn about the current state and maturity of information security management systems at Austrian universities, and promising areas for their further improvement in the face of ever-increasing cyber threats are outlined.*

Keywords: *information security; cybersecurity; security policy; data protection; GDPR; Austrian universities; academic environment; personal data; risk management.*