Научный поиск: личность, образование, культура. 2022. № 1. С. 27–32.
Scientific search: personality, education, culture. 2022. no. 1. pp. 27–32.

ПЕДАГОГИЧЕСКИЕ НАУКИ

Научная статья
УДК 004.056
ББК 16.8
DOI: 10.54348/SciS.2022.1.4

Обеспечение информационной безопасности участников образовательного процесса вуза

Владимир Вячеславович Иванов[1], Вадим Анатольевич Смирнов[2]
[1, 2] Ивановский государственный университет, Шуйский филиал, Шуя, Россия
[1] ivv.consultant.37@gmail.com
[2] v.a.d.i.m@bk.ru

Аннотация. Одной из актуальных и неразработанных проблем информационной безопасности участников образовательного процесса является смена функциональной роли с «абитуриент» на «студент». Для периода включения первокурсника в ЭИОС университета характерным является взаимный недостаток необходимых сведений у студента и сопровождающего информационного персонала, что затрудняет однозначную идентификацию друг друга в ходе информационного взаимодействия. При анализе текущего состояния проблемы был использован ряд источников, включающих опубликованные материалы в электронных СМИ и социальных сетях. В рамках обеспечения информационной безопасности участников образовательного процесса вуза необходима как защита от любых ситуаций, характерных для любой крупной организации, так и выполнение отдельного комплекса рекомендаций. Реализация обоснованного в статье комплекса рекомендаций позволит существенно снизить или даже полностью избежать информационных угроз, возникающих в указанный период образовательного процесса.

Ключевые слова: информационная безопасность, информационные технологии в высшем образовании, информационная безопасность личности, участники образовательного процесса, социальные сети, абитуриент.

Для цитирования: Иванов В. В., Смирнов В. А. Обеспечение информационной безопасности участников образовательного процесса вуза // Научный поиск: личность, образование, культура. 2022. № 1. С. 27–32. https://doi.org/10.54348/SciS.2022.1.4

Original article

Procuring of information security of participants of the educational process of the university

Vladimir V. Ivanov[1], Vadim A. Smirnov[2]
[1, 2] Ivanovo State University, Shuya Branch, Shuya, Russia
[1] ivv.consultant.37@gmail.com
[2] v.a.d.i.m@bk.ru

Abstract. One of the actual and undeveloped problems of information security of participants in the educational process is the change of the functional role from "entrant" to "student". For the period of inclusion of a first-year student in the EIEE (electronic information-educational environment) of the university, a mutual lack of necessary information of the student and the accompanying information staff is characteristic, which makes it difficult to unambiguously identify each other during information interaction. When analyzing the current state of the problem, a number of sources were used, including published materials in electronic media and social networks. As part of ensuring the information security of participants in the educational process of the university, both protection from any situations characteristic of any large organization and a separate set of recommendations are necessary. The implementation of the set of recommendations justified in the article will significantly reduce or even completely avoid

information threats arising during the specified period of the educational process.

Keywords: information security, information technologies in higher school education, information security of a person, participants in the educational process, social networks, entrant.

For citation: Ivanov V. V., Smirnov V. A. Procuring of information security of participants of the educational process of the university. *Nauchnyj poisk: lichnost', obrazovanie, kul'tura = Scientific search: personality, education, culture.* 2022. no. 1. pp. 27–32. (In Russ). https://doi.org/10.54348/SciS.2022.1.4

Актуальность. В качестве участников образовательного процесса мы будем понимать обучающихся (абитуриенты, студенты, слушатели и др.), педагогических работников университета, а также сопровождающий информационный персонал.

По нашему мнению, одним из самых уязвимых периодов для субъектов образовательного процесса университета является время их поступления в учебное заведение – в особенности, в 2020 и 2021 гг. В 2021 году практически во всех вузах инициированы процедуры отчислений «по собственному желанию» и дополнительного набора студентов на места, финансируемые из бюджетов различных уровней. Обладание бюджетным местом в таких условиях может рассматриваться как нематериальная ценность. Поэтому в период поступления/зачисления абитуриент и первокурсник являются более уязвимой категорией, нежели студенты старших курсов, что обосновывает актуальность проведения исследования.

Методы и организация исследования. Для рассмотрения текущего состояния проблемы использовались методы поиска и анализа статей по теме исследования, нормативных документов Министерства науки и высшего образования, опубликованных материалов в электронных СМИ и социальных сетях.

Результаты и их обсуждение. Общепринято подразделение мер по обеспечению информационной безопасности на правовые (законодательные), морально-этические, организационные (административные), физические и технические (аппаратные и программные) [Андрианов, 2003]. При этом в качестве морально-этического аспекта решения проблем обеспечения информационной безопасности личности образовательного процесса нередко называют формирование культуры личной информационной безопасности. Исследователь Э.В. Миндзаева полагает, что под культурой личной информационной безопасности следует понимать «совокупность знаний, умений, позволяющих личности действовать с целью удовлетворения возникающих информационных потребностей; готовность использовать традиционные, а также информационные и коммуникационные технологии на принципах защищенности личной информации; способность и готовность противостоять преднамеренным или непреднамеренным воздействиям, которые могут нанести вред личности, независимо от естественного или искусственного характера таких воздействий» [Развитие информатизации образования…, 2018, с. 18]. На текущий момент можно отметить следующие проблемы информационной безопасности, характерные для образовательного процесса в университете при поступлении и смене функциональной роли с «абитуриент» на «студент»:

1) Угроза доступности информации о текущем положении в списке претендентов на зачисление. Анализ новостных информационных источников подтверждает, что существует ряд университетов, сайты которых не смогли выдержать пиковой нагрузки, созданной в последний день приёма заявлений от поступающих на направления бакалавриата [«Рулетка» и «лотерея»…; Сайты четверти вузов…]. В большей степени решение данной проблемы должно находиться в организационном и правовом поле (например, право для университета самостоятельно устанавливать срок окончания приема заявлений). С технической стороны можно порекомендовать использование дополнительных виртуальных мощностей, которые могут быть на необходимый период предоставлены провайдерами облачных технологий.

2) Неоправданное расширение информации, предоставляемой об абитуриентах. В настоящее время в списках поступающих вместо ФИО публикуется номер СНИЛС абитуриента. Такой подход объясняется удобством и необходимостью более точной идентификации абитуриента, поскольку сочетание фамилии, имени и отчества может совпасть. Но при этом в приказах о зачислении большинства университетов попрежнему содержатся ФИО зачисленного. Исходя из количества набранных баллов и направления подготовки, в ряде случаев есть возможность сопоставить эти данные и получить реальный номер СНИЛС обучающегося. Оставшаяся часть университетов уже решают в правовом поле данную проблему одним из следующих способов: а) не публикуют приказы о зачислении (например, ВлГУ им. Столетовых); б) в приказах о зачислении указывают номер

СНИЛС вместо ФИО (например, МГТУ им. Баумана).

3) Недостаточная проработанность процесса аутентификации абитуриента в ЭИОС университета. Следует понимать, что современная ЭИОС включает не только Google.Classroom, Moodle и др. СДО, где создание учетных записей и подключение студентов к определённым курсам, как правило, контролируется преподавателями. Важной частью являются и сообщества во ВКонтакте и др. социальных сетях. Многие группы студентов самостоятельно создают беседы и/или закрытые группы в социальных сетях, чтобы более оперативно обмениваться информацией о занятиях, важными объявлениями и др. При этом процесс аутентификации студента при его включении в группу социальной сети заключается всего лишь в сравнении старостой (или др. обучающимся, ответственным за ведение группы) ФИО с информацией в журнале и, в ряде случаев, проверке сведений в профиле и фотографий на странице пользователя. В некоторых случаях попытки сбора пользователей в такую группу осуществляются даже до личного знакомства (рисунки 1, 2). Что касается активности пользователя в группах университета или факультета, то администраторы таких сообществ в ряде случаев вовсе не предпринимают никаких попыток аутентификации автора сообщения.

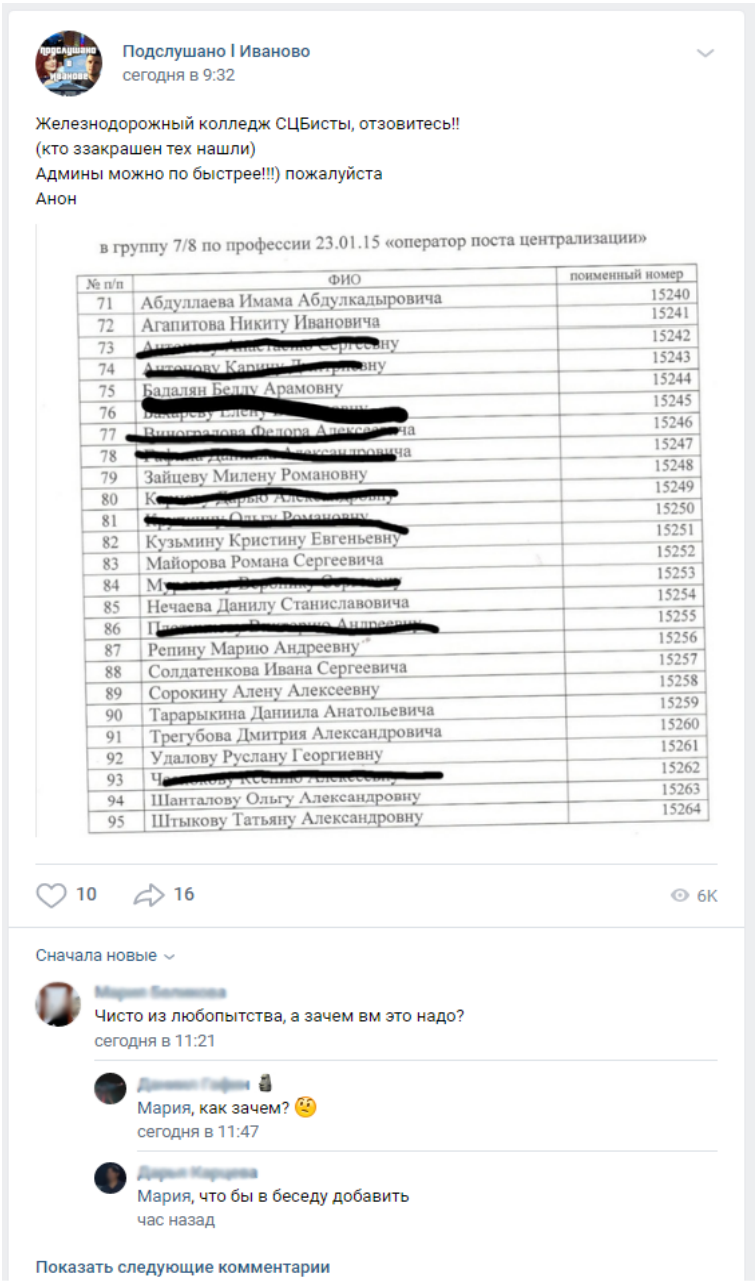

Рисунок 1. Сбор пользователей в беседу для студентов колледжа
Figure 1. Collecting Users in a Conversation for College Students

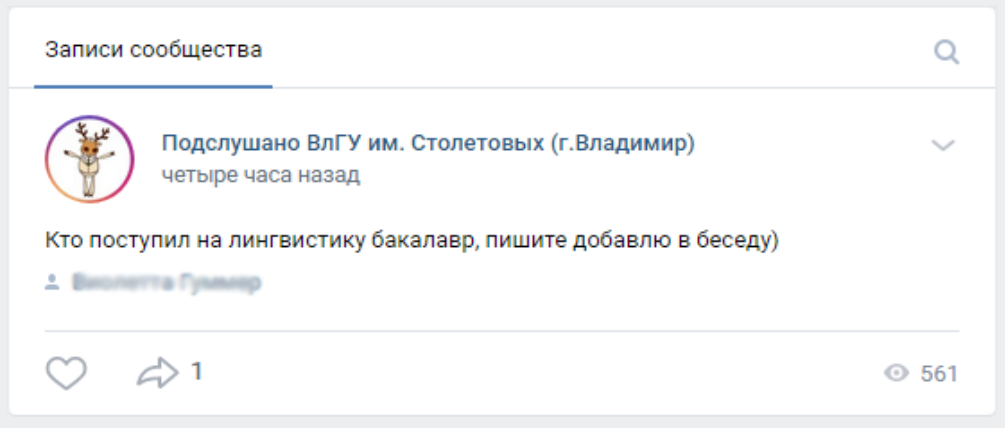

Рисунок 2. Сбор пользователей в беседу для направления подготовки
Figure 2. Collecting users into a conversation for a direction of preparation

В качестве одного из последствий недостатка таких проверок может быть размещение сообщений, содержащих недостоверную информацию. Например, достаточно высокий отклик и популярность обрели подозрительно сходные сообщения об охранниках, которые были размещены в группах МИФИ (https://vk.com/wall-166414649_60646), МГППУ (https://vk.com/wall-168945429_6782), ВСГИК (https://vk.com/wall-59531305_48024).

Решение данной проблемы лежит не только в правовой и организационной, но и морально-этической стороне информационной безопасности. Во-первых, администраторы групп должны быть обучены навыкам обнаружения «фальшивых» сообщений, мониторинга и контроля активности аккаунтов в сообществах и т.д. Во-вторых, необходима работа по верификации обучающихся при их включении в данные сообщества, которая подразумевает не только использование общедоступных данных в профиле (фотографий и сведений о пользователе). Стоит отметить, что приемная комиссия университета знает адреса электронной почты и номера телефонов большинства абитуриентов, в связи с чем возможна централизованная работа по созданию закрытых групп и бесед в социальной сети, в которые были бы включены только студенты университета. Технической стороной данного вопроса является создание системы, автоматизирующей создание таких групп посредством возможностей ЭИОС университета и API социальных сетей.

4) Новый вид мошенничества, заключающийся в создании страниц социальной сети, внешний вид которых говорит о принадлежности члену администрации университета, кафедры или деканата («фейковых» страниц [Нестулей, 2018]). В ряде случаев такая ситуация может угрожать исключительно потерей цифровой репутации. С другой стороны, возможны и нарушения конфиденциальности информации, поскольку запросы о предоставлении копии паспорта студента и др. персональных данных с такой страницы у многих обучающихся не вызовут подозрений.

Обладатель такой «фейковой» страницы может изначально «добавиться в друзья» к студентам университета. В результате каждый следующий студент будет видеть своих одногруппников в списке друзей страницы, а вследствие этого его доверие к такой странице будет выше. Поэтому культура информационной безопасности должна затрагивать каждого субъекта образовательного процесса. Описанной ситуации можно избежать, если все участники будут стремиться не вносить и не оставлять в «списке друзей» непроверенных лиц или тех, кого они не знают.

5) Помимо «фейковых» аккаунтов, злоумышленник может использовать и взломанные аккаунты. В случае рассмотрения крупной организации можно говорить не только о взломе аккаунтов с общими целями (инструмент массовой рассылки спама и др.), но и направленном на конкретный административный персонал или преподавателей. При этом ценностью для дальнейшего использования может обладать не только доступ к аккаунту как таковой, но и получение и анализ сообщений, которые позволят выявить стиль общения педагога и какие-либо закрытые сведения. Такие данные могут использоваться для более убедительной атаки с «фейковых» страниц в социальных сетях, новой электронной почты и др.

Многие из данных проблем остаются актуальными и после зачисления абитуриента, в процессе его обучения. Но кроме этого возникает ряд проблем, связанных с необходимостью хранения субъектами образовательного процесса персональной информации обучающихся. Например, работник деканата вынужден хра-

нить паспортные данные студентов университета для выполнения должностных обязательств по составлению отчётной документации.

В итоге важным аспектом информационной культуры личности, наряду с умением анализировать информацию, обеспечивать её доступность и целостность, становятся и навыки хранения конфиденциальной информации, предполагающие не только меры по ограничению доступа к ней, но и её своевременное уничтожение. И студент, и преподаватель, обладающие какой-либо ценной (в особенности, чужой персональной) информацией, должны не только принимать меры по обеспечению сохранности своего аккаунта от взлома, но и не хранить информацию дольше, чем это необходимо. В противном случае эта информация будет получена злоумышленником, если аккаунт будет скомпрометирован.

Помимо перечисленных выше проблем, учебное заведение не свободно от любых ситуаций, которые можно прогнозировать для любой достаточно крупной организации (защита информации от утери в результате действия внешних и внутренних факторов различного характера, защита конфиденциальной информации обучающихся, обеспечение доступности учебной информации для всех участников образовательного процесса и др.). Поэтому комплексная защита образовательного учреждения не ограничивается только соблюдением представленных выше рекомендаций, а предполагает длительный процесс, связанный с резервным копированием, установкой средств антивирусной защиты, ограничением полномочий сотрудников и др. [Рычков, 2012].

Выводы. В результате анализа различных источников были выявлены проблемы информационной безопасности, характерные для высших учебных заведений при организации приемной компании и включении первокурсников в ЭИОС. Таковыми являются: повышенный риск отказа информационной системы в критический для выпускников момент окончания срока приема заявлений на зачисление, возможность получения номера СНИЛС и ФИО поступающего путем анализа приказа о зачислении и списка поступающих, недостаточная проработанность процесса аутентификации абитуриента в ЭИОС университета, а также высокий риск использования злоумышленниками «фейковых» или взломанных аккаунтов администрации вуза для реализации методов социальной инженерии. Целенаправленное комплексное исполнение представленных соображений будет способствовать повышению уровня информационной безопасности участников образовательного процесса в учебных заведениях различных уровней и профилей подготовки.

Список источников

Андрианов С. В. Обеспечение безопасности информации в коммутационных вычислительных сетях / С. В. Андрианов, Б. П. Пальчун, А. Ю. Шатраков // Известия ТРТУ. 2003. № 4 (33). С. 32-36.

Надеждин Е.Н., Ермошин А.В. Особенности защиты персональных данных в информационно-образовательной среде педагогического университета // Научный поиск. 2015. № 2. С. 67-72.

Нестулей Е. А. Правовой режим фейковых аккаунтов в социальных сетях // Конституционные права и свободы человека и гражданина в Российской Федерации: проблемы реализации и защиты: Материалы межвузовской (ежегодной) студенческой конференции, Иркутск, 30 ноября 2017 года / отв. ред. В.Н. Шутова. Иркутск : Иркутский институт (филиал) ВГУЮ (РПА Минюста России), 2018. С. 56-60.

Развитие информатизации образования в школе и педагогическом вузе в условиях обеспечения информационной безопасности личности / С. А. Бешенков, Я. А. Ваграменко, В. А. Касторнова и др. Москва : Институт управления образованием Российской академии образования, 2018. 105 с.

«Рулетка» и «лотерея»: абитуриенты и их родители возмутились новыми правилами зачисления в вузы. URL: https://www.bfm.ru/news/479311

Рычков А. В. Способы защиты от компьютерных вирусов // Ученые записки Российского государственного социального университета. 2012. № 3(103). С. 212-215.

Сайты четверти вузов Петербурга в последний день зачисления на бюджет работали с перебоями. URL: https://www.fontanka.ru/2021/08/12/70075841/

References

Andrianov S. V. Ensuring the security of information in switching computer networks / S. V. Andrianov, B. P. Palchun, A. Yu. Shatrakov. *Izvestiya TRTU = Izvestiya TRTU.* 2003. no. 4 (33). pp. 32-36. (In Russ).

Nadezhdin E.N., Ermoshin A.V. Peculiarities of Personal Data Protection in the Information and Educational Environment of the Pedagogical University. *Nauchnyj poisk = Scientific search.* 2015. no. 2. pp. 67-72. (In Russ).

Nestuley E. A. Legal regime of fake accounts in social networks // Constitutional rights and freedoms of man and citizen in the Russian Federation: problems of implementation and protection: Materials of the interuniversity

(annual) student conference, Irkutsk, November 30, 2017 / executive ed. V. N. Shutova. Irkutsk: Irkutsk Institute (branch) VSUYu (RPA of the Ministry of Justice of Russia). 2018. pp. 56-60. (In Russ).

Development of informatization of education in schools and pedagogical universities in the context of ensuring information security of the individual / S. A. Beshenkov, Ya. A. Vagramenko, V. A. Kastornova et al. Moscow: Institute of Education Management of the Russian Academy of Education, 2018. 105 p. (In Russ).

"Roulette" and "lottery": applicants and their parents were outraged by the new rules for admission to universities. URL: https://www.bfm.ru/news/479311 (In Russ).

Rychkov A. V. Methods of protection against computer viruses. *Uchenye zapiski Rossijskogo gosudarstvennogo social'nogo universiteta = Scientific notes of the Russian State Social University*. 2012. no. 3 (103). pp. 212-215. (In Russ).

The websites of a quarter of St. Petersburg universities worked intermittently on the last day of admission to the budget. URL: https://www.fontanka.ru/2021/08/12/70075841/ (In Russ).

Статья поступила в редакцию 14.09.2021; одобрена после рецензирования 14.10.2021; принята к публикации 01.03.2022.

The article was submitted 14.09.2021; approved after reviewing 14.10.2021; accepted for publication 01.03.2022.