УДК 378:37.031

РАЗВИТИЕ ГОТОВНОСТИ БУДУЩЕГО СПЕЦИАЛИСТА ПО ЗАЩИТЕ ИНФОРМАЦИИ К СИТУАЦИОННОМУ УПРАВЛЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Астахова Л.В.[1], Земцов И.В.[2]

[1] Федеральное государственное автономное образовательное учреждение высшего образования «Южно-Уральский государственный университет (национальный исследовательский университет)», Челябинск, e-mail: lvastachova@mail.ru;
[2] Федеральное государственное бюджетное образовательное учреждение высшего образования «Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева», Красноярск, e-mail: 9798866@gmail.com

В настоящей статье выявлено противоречие между новыми, актуальными задачами, поставленными перед высшим образованием российской и зарубежной наукой и практикой управления информационной безопасностью, национальной программой «Цифровая экономика Российской Федерации», отечественными профессиональными стандартами в области защиты информации, и низким уровнем отражения этих задач в содержании и организации отраслевого высшего образования страны. Обоснованы необходимость и педагогические условия развития готовности будущего специалиста по защите информации к ситуационному управлению информационной безопасностью в условиях вуза, связанные с содержанием, организацией и условиями образовательного процесса. Особое внимание уделено разработке и внедрению в учебный процесс новых организационных форм изучения ситуационного управления информационной безопасностью: обучению через опыт, перевернутому, адаптивному, социальному обучению. Научная новизна работы заключается в постановке и определении путей и средств решения проблемы освоения инновационного ситуационного подхода к сфере управления информационной безопасностью, а также в определении педагогических условий развития готовности к нему студентов. Практическая значимость исследования состоит в возможности реализации этих условий в вузах, что будет способствовать повышению не только результативности усвоения дисциплины «Управление информационной безопасностью» будущими специалистами по защите информации, но и уровня их цифровых компетенций и когнитивной культуры.

Ключевые слова: специалист по защите информации, информационная безопасность, управление, ситуационный подход, педагогические условия.

DEVELOPMENT OF THE FUTURE SPECIALIST'S READINESS FOR THE PROTECTION OF INFORMATION FOR THE SITUATIONAL MANAGEMENT OF INFORMATION SECURITY

Astakhova L.V. [1], Zemtsov I.V. [2]

[1]Federal State Autonomous Educational Institution of Higher Education «South Ural State University (national research university)», Chelyabinsk, e-mail: lvastachova@mail.ru;
[2] Reshetnev Siberian State University of Science and Technology, Krasnoyarsk, e-mail: 9798866@gmail.com

This article reveals a contradiction between the new, urgent tasks posed to higher education in Russian and foreign science and information security management practices, the National Program «Digital Economy of the Russian Federation», domestic professional standards in the field of information protection, and the low level of reflection of these tasks in the content and organization of sectoral higher education of the country. The necessity and pedagogical conditions of developing the readiness of a future specialist in information protection for situational management of information security in a university related to the content, organization and conditions of the educational process are substantiated. Particular attention is paid to the development and implementation in the educational process of new organizational forms for studying situational information security management: learning through experience, inverted, adaptive, social learning. The scientific novelty of the work lies in the formulation and determination of ways and means of solving the problem of developing an innovative situational approach to the field of information security management, as well as in determining the pedagogical conditions for the development of students' readiness for it. The practical significance of the study lies in the possibility of implementing these conditions in universities, which will increase the effectiveness of not only mastering the discipline «Information Security Management» by future information protection specialists, but also the level of their digital competencies and cognitive culture.

Keywords: information security specialist, information security, management, situational approach, pedagogical conditions.

Всеобщая цифровизация ресурсов и функций является следствием глобального технологического прогресса. Стремительное развитие новых информационных технологий обусловило и переход концепции Образования 3.0 к концепции Образования 4.0, характеризующейся использованием инновационных образовательных технологий, направленных на повышение адаптивности выпускников вузов к быстро меняющимся требованиям практики. Конвергенция искусственного интеллекта, больших данных и технологий платформ показывает, что основная часть необходимых навыков в высшем образовании, которые еще предстоит развивать, – это потребность в большей активности и гибкости [1]. Востребованность высокой адаптивности, технологий гибридного обучения, конвергенции искусственного интеллекта, больших данных и технологий платформ ставит серьезные задачи перед подготовкой современных специалистов. Особенно это касается специалистов по защите информации, которые должны быть подготовлены к деятельности в условиях динамики информационных угроз и ситуационному управлению безопасностью компьютерных систем.

Цель исследования – обосновать проблему развития готовности будущего специалиста по защите информации к ситуационному управлению информационной безопасностью (здесь и далее – ИБ) в вузе в контексте современных требований науки и практики защиты информации и определить новые организационные формы ее решения в условиях вуза.

Материал и методы исследования. В процессе обоснования ситуационного управления ИБ как объекта освоения студентами вуза – будущими специалистами по защите информации использован информационно-деятельностный подход. Анализ деятельности специалиста по защите информации представлен в контексте информационного процесса – как различных видов информационной деятельности: потребительской, репродуктивной и созидательной. Основой для исследования процесса развития готовности к инновационной деятельности по ситуационному управлению ИБ послужили образовательные ситуации, ориентированные на активизацию студентов для решения названной инновационной проблемы в процессе обучения. Для выявления педагогических условий развития готовности студентов к этой деятельности был применен системный подход к образованию как системе содержания, организации и условий.

Результаты исследования и их обсуждение. Особенность специалиста по информационной безопасности заключается в том, что его деятельность обладает информационно-управленческой природой и самоорганизующимся характером: он работает с

объектами, которые сам создает. Поэтому такому специалисту необходимы стратегическое, глобальное мышление, аналитическая компетенция, знание бизнес-процессов и движения информации в организации, способность обеспечить баланс конкурирующих приоритетов, способность развивать и реализовать свои таланты и др. [2]. Ситуационное управление ИБ как объект изучения позволяет максимально развивать эти качества.

Реальность такова, что в современных информационных системах «по-прежнему доминируют традиции применения стандартных аппаратно-программных средств защиты информации, которые практически исчерпали свой потенциал относительно нейтрализации возможных информационных угроз. Одновременно существенно возросли технические возможности инструментальных средств, привлекаемых злоумышленниками для получения несанкционированного доступа к ресурсам и сервисам распределенной ИОС» [3, с. 30]. Обзор литературы по управлению рисками информационной безопасности, предпринятый зарубежными экспертами, выявил недостатки в практике оценки рисков информационной безопасности, которые неизбежно ведут к неправильному принятию решений и неадекватным стратегиям безопасности [4]. Поэтому в настоящее время все чаще в основу организации процесса управления ИБ закладывается более гибкая, адаптивная стратегия управления рисками – стратегия ситуационного управления. Освоение средств управления ИБ на основе ситуационного подхода весьма актуально, что подтверждают российские и зарубежные эксперты [5-7].

Отдельные аспекты принятия решений на основе ситуационного управления динамическими объектами изучены и описаны в публикациях. Так, например, эксперты пришли к выводу, что наиболее адекватна для защиты сетей трехуровневая процессно-сервисная модель системы управления ИБ. Эта модель включает процессы стратегического, тактического и операционного уровня: «управление рисками, обеспечение целостности сетевых ресурсов, корректировка политики ИБ верхнего уровня»; «разработка и настройка процедур защиты, развитие архитектуры системы ИБ, классификация и анализ состояния ИТ-ресурсов, мониторинг и управление инцидентами»; «разграничение прав доступа, управление сетевой безопасностью, проверка соответствия системы ИБ установленным стандартам» [3].

Зарубежные исследователи активно анализируют ситуационную осведомленность о кибербезопасности. Так, разработана система ситуационной осведомленности о кибербезопасности, состоящая из семи уровней: оценка данных, оценка объекта, оценка ситуации, оценка воздействия, уточнение процесса / управление ресурсами, уточнение пользователя / управление знаниями, управление миссиями [8]. Для повышения адаптивности выпускников на местах трудоустройства эти многоуровневые системы должны изучаться в вузах.

Мероприятия федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации» (утв. президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам, протокол от 24 декабря 2018 г. № 16) направлены в том числе на реализацию информационной безопасности и устойчивости сетей связи общего пользования, а также на разработку новых механизмов поддержки отечественных разработчиков программного обеспечения и компьютерного оборудования в сфере информационной безопасности [9]. Очевидно, что государство заинтересовано в новых технологиях защиты информации, обусловленных требованиями динамично развивающейся практики. К их числу относятся и технологии ситуационного управления ИБ.

Потребность в знаниях студентами ситуационного управления ИБ диктуют и профессиональные стандарты. Так, стандарт 06.033 «Специалист по защите информации в автоматизированных системах» содержит трудовую функцию «Управление защитой информации в автоматизированных системах», предполагающую трудовое действие «Анализ изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации» [10].

Известно, что профессиональные компетенции новых федеральных государственных образовательных стандартов (ФГОС 3++) формируются на основе профессиональных стандартов, соответствующих профессиональной деятельности выпускников, а также при необходимости – на основе анализа требований к профессиональным компетенциям, предъявляемых к выпускникам на рынке труда, на основе обобщения отечественного и зарубежного опыта, проведения консультаций с ведущими работодателями, объединениями работодателей отрасли, в которой востребованы выпускники [11].

Учитывая, что стандарт 06.033 «Специалист по защите информации в автоматизированных системах» относится к профессиональным стандартам, соответствующим профессиональной деятельности выпускников, освоивших программу по специальности 10.05.03 «Информационная безопасность автоматизированных систем», мы можем сделать вывод об императивах изучения ситуационного управления ИБ будущими выпускниками этой специальности. Эта инновационная тема должна найти более широкое отражение во ФГОС 3++ по направлению «Информационная безопасность». Профессиональные стандарты по информационной безопасности также нуждаются в дополнении: требуется более четко сформулировать необходимые умения и знания, касающиеся ситуационного управления ИБ. В учебные планы следует включать дисциплины, связанные с ситуационным подходом к управлению, а также посвящать этой проблематике разделы таких курсов, как «Управление ИБ», «Организационная защита информации»,

«Комплексные системы защиты информации» и др. На эти проблемы должны обратить внимание образовательные учреждения дополнительного профессионального образования, которые реализуют программы по повышению квалификации и переподготовке специалистов в области информационной безопасности.

Приоритетное место в числе названных дисциплин занимает дисциплина «Управление информационной безопасностью». Об этом свидетельствует наш опыт ее преподавания в рамках специальности 10.05.03 «Информационная безопасность автоматизированных систем». Для развития готовности студентов к ситуационному управлению ИБ в обозначенных выше содержательных границах необходимы новые подходы к организации учебного процесса, поэтому целесообразно использовать перевернутое, социальное, адаптивное обучение и обучение через опыт.

Технология *«Перевернутое обучение (flipped learning)»* [12, с. 71] основана на замене прямой передачи знаний из группового образовательного пространства в индивидуальное. При этом «групповое пространство обучения трансформировано в динамическое, интерактивное окружение, в котором преподаватель принимает роль консультанта и помогает обучающимся применить изученную теорию на практике, выработать навыки» [12, с. 71] для дальнейшего самостоятельного обучения и развития. Эта технология относится к моделям смешанного обучения. Они направлены на усиление индивидуализации образования, на учет потребностей, интересов и способностей обучающихся. При этом преподаватель выполняет роль помощника. Основы теории ситуационного управления ИБ студенты изучают индивидуально в рамках задания по сравнительному анализу традиционного и ситуационного управления ИБ как в России, так и за рубежом. Результаты сравнительного анализа студенты представляют в форме таблиц, схем и иного и обсуждают на аудиторных групповых занятиях.

В ходе работы требуется применение *обучения через опыт (experiential learning), которое определено как* «совокупность образовательных технологий, предполагающих участие обучающихся в какой-либо деятельности и приобретение соответствующего опыта, а также оценку этой деятельности и приобретенного опыта, идентификацию и усвоение новых знаний и умений» [12, с. 64]. Студенты выполняют задание по подготовке аналитической справки для руководителя предприятия, цель которой – выявление проблем разработки и внедрения платформ ситуационного управления ИБ и путей их решения. Таких проблем немало: сбор и аналитико-синтетическая переработка информации об угрозах сетям, выбор алгоритмов и процедур ситуационного управления рисками информационной безопасности [3] и др.

Особое внимание в учебном процессе мы уделили проблеме влияния фактора объекта защиты на объем и границы ситуационной системы управления ИБ. Поскольку существует

пять уровней информации (эмпирический, синтаксический, семантический, прагматический и социальный), студентам было предложено представить ее в 4 формах на этих уровнях: знаки, логические структуры, значения и сообщения, а затем выбрать формы представления информации в целях ее защиты [13]. При этом следовало показать возможности снижения пределов применимости мер информационной безопасности организации и исключения неэффективных мер. Таким способом будущие специалисты с помощью моделирования ситуационного подхода к объектам защиты конкретной организации могли увидеть пути повышения эффективности ее системы управления ИБ. Попытки решить эти и другие проблемы помогают студентам освоить материал, стимулируют проблемное инновационное мышление будущих специалистов, позволяют смоделировать опыт общения с работодателем.

В процессе освоения дисциплины целесообразно использовать также «*адаптивное обучение (adaptive learning)»,* позволяющее выстраивать индивидуальную траекторию обучения с учетом способностей, целей, мотивации и др. [12, с. 67]. Созданное авторское знание студенты по выбору (в зависимости от уровня готовности, способности и желания) могут ретранслировать в открытую информационную среду в разных формах: в форме презентации, записи в блоге, графического экстракта (схемы или таблицы), тезисов научной статьи, создания проблемного сайта и др. Описанные проблемные задания весьма непросты, поэтому студентам следует предоставлять возможность объединяться в группы по 2–3 человека.

В образовательном процессе успешно можно применить также «*социальное обучение (social learning)»,* дающее возможность в образовательном процессе обмениваться информацией и опытом, создавать совместные продукты, обсуждать их в социальных медиа [12, с. 69]. Оно может быть реализовано на платформе специально созданной группы в социальной сети.

В ходе исследования мы пришли к выводу о том, что в процессе обучения студенты не только осваивают новейшие российские и зарубежные технологии ситуационного управления информационной безопасности, но и повышают уровень когнитивной культуры. Для цифровой эпохи когнитивная культура – важнейший компонент профессионализма специалиста высшей квалификации, предполагающий наличие его способности к мотивированному восприятию, рациональному познанию и критической оценке в процессе информационного взаимодействия в ходе всех видов его информационной деятельности: потребительской, репродуктивной и созидательной [13, с. 102]. Обучающиеся не только потребляют уже готовое знание, но и создают собственные смыслы – авторское знание, представляют и обсуждают его в группе в ходе дискуссий.

В результате проведенного исследования мы сформулировали педагогические условия развития готовности будущего специалиста по защите информации к ситуационному управлению ИБ, соответствующие системным компонентам образовательного процесса (содержание, средства, среда): а) соответствие образовательной программы развития готовности будущего специалиста по защите информации к ситуационному управлению ИБ в вузе системе информационной деятельности личности (потребительской, репродуктивной и созидательной); б) усиление мотивации студентов к развитию их готовности к ситуационному управлению ИБ с помощью новых организационных форм, соответствующих принципам «Образования 4.0»: перевернутого, социального, адаптивного обучения и обучения через опыт и др.; в) расширение образовательной среды вуза за счет виртуального знакомства с реализованными платформами ситуационного управления ИБ на предприятиях.

Заключение

Проблема готовности студентов к ситуационному управлению ИБ в высшем образовании весьма актуальна в условиях парадигмы «Образование 4.0», национальной программы «Цифровая экономика Российской Федерации» и внедрения российских профессиональных стандартов. Обоснованы необходимость и педагогические условия развития готовности будущего специалиста по защите информации к ситуационному управлению ИБ в условиях вуза, связанные с содержанием, организацией и условиями образовательного процесса. Особое внимание уделено разработке и внедрению в учебный процесс новых организационных форм изучения ситуационного управления ИБ: обучения через опыт, перевернутого, адаптивного, социального обучения. Реализация обоснованных путей и средств решения проблемы освоения инновационного ситуационного подхода к сфере управления ИБ будет способствовать повышению не только результативности усвоения дисциплины «Управление информационной безопасностью» будущими специалистами по защите информации, но и уровня их цифровых компетенций и когнитивной культуры.

Список литературы

1. Hildebrandt C.K. Whose interest is educational technology serving? Who is included and who is excluded? RIED. Revista Iberoamericana de Educación a Distancia. 2019. Vol. 22. No. 1. P. 207–220.
2. Harkins M.W. The 21st Century CISO. Managing Risk and Information Security. Apress, Berkeley, CA. 2016. P. 139–153.
3. Надеждин Е.Н. Стратегия ситуационного управления ИБ в корпоративных вычислительных сетях образовательных учреждений // Научный поиск. 2014. № 2.5. С. 30-32.

4. Webb J., Ahmad A., Maynard S.B., Shanks G. A situation awareness model for information security risk management. Computers & Security. 2014. Vol. 44. P.1-15.

5. Astakhova L., Zemtsov I. Situational approach to information security // Proceedings - 2018 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology, USBEREIT. 2018. P. 136-139.

6. Имамвердиев Я.Н. Модель ситуационного управления ИБ электронного правительства // Информационные технологии. 2014. № 8. С. 24-33.

7. Yao J., Fan X., Cao N. Survey of Network Security Situational Awareness. In: Vaidya J., Zhang X., Li J. (eds) Cyberspace Safety and Security. CSS 2019. Lecture Notes in Computer Science. 2019. vol 11982. P. 34-44.

8. Kokkonen T. Architecture for the Cyber Security Situational Awareness System. Conference: International Conference on Next Generation Wired/Wireless Networking Conference on Internet of Things and Smart Spaces. 2016. DOI: 10.1007/978-3-319-46301-8_24.

9. Паспорт национальной программы "Цифровая экономика Российской Федерации" (утв. президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам протокол от 24 декабря 2018 г. N 16) [Электронный ресурс]. URL: https://base.garant.ru/72190282/ (дата обращения: 22.01.2020).

10. Профессиональный стандарт 06.033 «Специалист по защите информации в автоматизированных системах», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016г. No 522н (зарегистрирован Министерством юстиции Российской Федерации 28 сентября 2016г., регистрационный No43857). [Электронный ресурс]. URL: http://fgosvo.ru/uploadfiles/profstandart/06.033.pdf (дата обращения: 22.01.2020).

11. Федеральный государственный образовательный стандарт высшего образования – специалитет по специальности10.05.03 Информационная безопасность автоматизированных систем. ПРОЕКТ [Электронный ресурс]. URL: http://fgosvo.ru/uploadfiles/ProjFGOSVO3++/Spec3++/100503_C_3plus_06092019.pdf (дата обращения: 23.01.2020).

12. Обучение цифровым навыкам: глобальные вызовы и передовые практики. Аналитический отчет к III Международной конференции «Больше чем обучение: как развивать цифровые навыки» / Корпоративный университет Сбербанка. М.: АНО ДПО «Корпоративный университет Сбербанка», 2018. 122 с.

13. Астахова Л. В. Понятие когнитивной культуры студента: определение и условия развития // Образование и наука. 2019. Т. 21, № 10. С. 89–115. DOI: 10.17853/1994-5639-2019-10-89-115.