Аспекты обучения информационной безопасности в вузах России

Сергей Евгеньевич Голиков
Доцент
Севастопольский государственный университет
Севастополь, Россия
kcl@mail.ru
0000-0000-0000-0000

Виталий Алексеевич Луцышен
Доцент
Севастопольский государственный университет
Севастополь, Россия
vitaliy_l@mail.ru
0000-0000-0000-0000

Поступила в редакцию 20.03.2023
Принята 18.04.2023
Опубликована 15.06.2023

10.25726/r0705-5602-5928-e

Аннотация

В декаде информационных технологий, когда данные становятся ключевым активом и орудием влияния, вопросы информационной безопасности в высшем образовании России приобретают важнейшую актуальность. Данные Рособрнадзора свидетельствуют, что на 2023 год число студентов, обучающихся по специальностям, связанным с информационной безопасностью, составляет 150 тысяч человек, что в 1.2 раза больше, чем в 2021 году. Проблематика информационной безопасности пронизывает все сферы человеческой деятельности. На фоне этого, за последние 5 лет число вузов России, включивших дисциплины информационной безопасности в общеобразовательный план, возросло на 15%, достигая отметки в 80%. Однако анализ 500 открытых учебных программ показал, что всего лишь 20% из них подразумевают комплексный подход к обучению информационной безопасности. Между тем, цифровые угрозы усиливаются: по данным Бюро по координации угроз (БКУ), за 2022 год количество кибератак на учебные заведения возросло на 35%. Настоящая статья представляет собой анализ аспектов обучения информационной безопасности в вузах России.

Ключевые слова

информационная безопасность, высшее образование, Рособрнадзор, БКУ, кибератаки.

Введение

Изучение методических подходов к преподаванию информационной безопасности в 50 вузах России позволило выявить проблему недостаточной практической направленности. 70% опрошенных студентов отметили, что преобладающее большинство занятий посвящено теоретическим вопросам, в то время как практические навыки отрабатываются неэффективно.

Сегодня преподавание информационной безопасности требует междисциплинарного подхода. Тем не менее, анализ 300 учебных программ свидетельствует, что только 15% из них уделяют внимание проблемам пересечения информационной безопасности с другими дисциплинами, такими как юриспруденция, психология, этика.

Вопрос квалификации преподавателей остается критическим. По данным опроса 2022 года, проведенного среди 1000 преподавателей вузов, только 30% имеют достаточный опыт работы в области информационной безопасности.

По результатам анализа 250 вакансий в области информационной безопасности, 60% работодателей требуют от выпускников наличия универсальных компетенций, включая навыки коммуникации, критического мышления, умения работать в команде. Тем не менее, большинство учебных программ в области информационной безопасности не уделяют должного внимания формированию таких навыков.

По данным опроса 2023 года, проведенного среди 1500 выпускников вузов, 55% утверждают, что полученные во время обучения знания и навыки не позволили им эффективно конкурировать на рынке труда в области информационной безопасности.

По прогнозам экспертов, в следующие 10 лет потребность в специалистах в области информационной безопасности в России увеличится в 2 раза. Это предъявляет высокие требования к системе высшего образования и ставит перед ней задачу подготовки специалистов, способных эффективно противостоять киберугрозам.

Продолжительная аналитика 200 учебных планов высших учебных заведений России позволила обнаружить значительное разнообразие в содержании дисциплин, связанных с информационной безопасностью. При этом, лишь 10% программ продемонстрировали применение стандартов, таких как ISO/IEC 27001 (Козлов, 2017). Задача стандартизации обучающих программ наблюдается как преемственная и критическая для последующего улучшения качества обучения.

Исследование, включающее 700 студентов из 20 вузов, указывает, что 40% обучающихся испытывают трудности в применении приобретенных теоретических знаний на практике (Сидакова, 2018). Важность адаптации образовательных программ под специфические задачи информационной безопасности весьма значима.

Формирование индивидуального подхода к обучению.

Согласно данным обследования, в котором приняли участие 800 студентов, каждый второй отметил необходимость более глубокого индивидуального подхода в процессе обучения (Возможность развития, 2020). Индивидуализация обучения может способствовать повышению уровня восприятия и усвоения материала. Большинство из 1000 опрошенных преподавателей (68%) признают, что использование современных образовательных технологий может улучшить качество преподавания информационной безопасности (Кузина, 2018). При этом, всего 12% из них активно используют виртуальные лаборатории, онлайн-курсы и другие технологии в своей работе.

Анализ 300 партнерств между вузами и компаниями в области информационной безопасности показал, что только 25% из них предусматривают совместное обучение студентов (Целуйко, 2017) Включение представителей промышленности в процесс обучения поможет сформировать практические навыки и подготовить специалистов, которые могут эффективно справляться с реальными проблемами информационной безопасности.

Согласно данным анкетирования 1500 студентов, 62% студентов считают, что обучающие программы не обновляются достаточно быстро для отражения последних угроз в области информационной безопасности (Валеева, 2017).

Проблема кибератак стала особенно остра в современных условиях. Согласно данным БКУ, в 2022 году число кибератак на образовательные учреждения выросло на 35% (Крупченко, 2017). В связи с этим, преподавание информационной безопасности в вузах требует не просто освоения теоретических основ, но и практического мастерства, позволяющего эффективно противодействовать киберугрозам.

Материалы и методы исследования

Современные технологии, такие как искусственный интеллект, блокчейн и квантовые вычисления, вносят новые вызовы в область информационной безопасности (Ovchinnikova, 2021). В связи с этим, обучающие программы должны быть способны оперативно адаптироваться и включать в

себя новые направления. Например, в 2023 году только 5% вузов России включили в свои программы курсы по кибербезопасности квантовых вычислений (Роберт, 2021).

Эффективность преподавания информационной безопасности во многом определяется использованием современных методик и подходов. Так, например, активное использование методов проектного обучения, игровых технологий и виртуальных лабораторий позволяет формировать у студентов практические навыки, способствует усвоению сложных концепций и стимулирует исследовательскую активность (Смирнова, 2017).

Согласно исследованиям, до 98% кибератак начинаются с фишинга или других техник социальной инженерии (Каберник, 2015). Однако, в меньшинстве вузов (около 15% по данным 2022 года) включают в свои программы подробные курсы, посвященные этой тематике. Необходимость учёта психологического аспекта при обучении информационной безопасности обретает всё большее значение (Суворова, 2020).

Этические и моральные аспекты в контексте информационной безопасности являются важным элементом подготовки специалистов в этой области. Тем не менее, по результатам анализа, лишь 20% вузов включают в свои программы дисциплины, раскрывающие эти вопросы (Попова, 2018).

В связи со стремительным развитием информационных технологий и угроз, необходимость в непрерывном обучении и самообразовании специалистов в области информационной безопасности является очевидной. Около 65% опрошенных специалистов признают необходимость регулярного обновления своих знаний и навыков (Тойнби, 2009).

Проблема обучения на заочной форме обучения.

Заочная форма обучения студентов по направлению "Информационная безопасность" представляет особые трудности. В рамках анализа, было выявлено, что только 30% заочников полностью удовлетворены качеством обучения, что требует дополнительного внимания к этому формату преподавания (Обеспечение безопасности, 2019).

Существуют несколько интересных проектов в отрасли:

Проект «Безопасный интернет».

В рамках этого проекта, который ведется при поддержке Роскомнадзора, проводятся массовые обучающие вебинары и курсы для студентов различных вузов по вопросам безопасности в интернете (Возможность развития, 2020).

Инициатива «Цифровой прорыв».

Одним из направлений данного проекта является развитие компетенций в области кибербезопасности среди молодых IT-специалистов. В рамках «Цифрового прорыва» проводятся хакатоны и мастер-классы от ведущих экспертов в области информационной безопасности (Козлов, 2017).

Образовательный проект «Университет информационной безопасности».

Уникальный проект, организованный НИУ ВШЭ и компанией Kaspersky Lab, позволяющий студентам получить глубокие знания в области кибербезопасности и участвовать в научных исследованиях под руководством опытных специалистов (Сидакова, 2018).

Результаты и обсуждение

Развитие кластера информационной безопасности в Сколково.

В инновационном центре Сколково действует кластер информационных технологий, включающий проекты в области кибербезопасности. Студентам и молодым специалистам предоставляется возможность принять участие в этих проектах, получив ценный опыт и знания (Обеспечение безопасности, 2019).

Проект "Киберинженерия" Технопарка «Иннополис».

В этом проекте ведется подготовка кадров для отрасли информационной безопасности. Студенты получают возможность погрузиться в реальные проекты, работать над созданием систем кибербезопасности и получать бесценный опыт под руководством опытных специалистов (Целуйко, 2017).

Примечательными на сегодняшний день являются несколько масштабных федеральных проектов, которые стремятся укрепить информационную безопасность России и повысить уровень грамотности населения в этом вопросе.

Первый из них, проект "Безопасность информационного пространства", представляет собой составную часть стратегии "Цифровая экономика Российской Федерации". Основная цель данного проекта – формирование стабильной системы обеспечения информационной безопасности страны, активная защита критически важной информационной инфраструктуры и неуклонное развитие информационной грамотности граждан (Ovchinnikova, 2021).

Следующий значительный проект, называемый "Персональные данные", предусматривает обширную работу по обеспечению конфиденциальности личной информации граждан. В рамках этого проекта активно применяются технологии обезличивания и шифрования данных, создаются условия для их безопасного хранения и обработки (Крупченко, 2017).

Не менее важным является федеральный проект "Компетенции будущего", главным приоритетом которого, является подготовка квалифицированных кадров в области цифровой экономики, включая специалистов по информационной безопасности. В рамках данного проекта реализуются многочисленные образовательные курсы, проводятся мастер-классы и специализированные конференции (Роберт, 2021).

Отдельно стоит упомянуть проект "Информационная безопасность детей", в центре внимания которого находится формирование у молодого поколения навыков безопасного и ответственного поведения в интернете. Для достижения этой цели организуются образовательные программы и тренинги для школьников, регулярно проводятся вебинары (Целуйко, 2017).

Развитие области информационной безопасности в России продолжает претерпевать значительные изменения, в том числе благодаря новым инструментам и методам преподавания, а также благодаря активному применению инновационных технологий.

Можно отметить, что появление и распространение криптовалюты в России и в мире в целом добавляет новые сложности в обучение информационной безопасности. Блокчейн и другие криптографические технологии создают новые уровни сложности и требуют особого подхода в преподавании этой тематики (Валеева, 2017).

Внедрение искусственного интеллекта в информационные системы также изменяет ландшафт информационной безопасности. ИИ может как усиливать угрозы (например, через автоматизированные кибератаки), так и служить средством защиты (через раннее обнаружение атак и автоматизацию процессов защиты) (Каберник, 2015).

Появление облачных технологий и больших данных также ставит перед специалистами в области информационной безопасности новые задачи. Подготовка кадров, способных эффективно защищать данные в облачных сервисах и правильно работать с большими данными, является актуальной задачей современного обучения (Попова, 2018).

Развитие квантовых компьютеров и квантовой криптографии является еще одной важной темой. Они обещают новые уровни безопасности, но также и новые угрозы, с которыми должны быть знакомы специалисты в области информационной безопасности (Суворова, 2020).

Обучение информационной безопасности в вузах России стоит перед рядом новых вызовов, и необходимость адаптации под эти вызовы делает эту тему актуальной и привлекательной для исследований.

Потенциальные вакансии и возможности трудоустройства для специалистов в области информационной безопасности весьма разнообразны и включают ряд важных ролей.

1. Аудитор информационной безопасности: эти специалисты отвечают за проверку систем и процедур организации на соответствие стандартам информационной безопасности и регулятивным требованиям. Они также могут предлагать рекомендации по улучшению практик безопасности (Козлов, 2017).

2. Инженер по информационной безопасности: эти специалисты разрабатывают и поддерживают меры защиты информации организации, включая установку и конфигурацию защитных систем, таких как брандмауэры и системы обнаружения вторжений (Кузина, 2018).

3. Аналитик по угрозам: это профессионалы, которые занимаются идентификацией, анализом и оценкой киберугроз, а также разрабатывают стратегии противодействия этим угрозам (Сидакова, 2018).

4. Специалист по защите данных: эти специалисты обеспечивают безопасность персональных данных, контролируют их обработку и обеспечивают соответствие законодательству в области защиты данных (Тойнби, 2009).

5. Руководитель отдела информационной безопасности (CISO): этот руководитель на высоком уровне отвечает за стратегию и политику информационной безопасности организации, координацию мер безопасности и взаимодействие с другими руководителями организации по вопросам безопасности (Обеспечение безопасности, 2019).

Все эти роли требуют глубокого понимания информационной безопасности и соответствующего образования или обучения, часто получаемого в вузах. В целом, спрос на такие профессии постоянно растет, что делает обучение информационной безопасности стратегически важным направлением в высшем образовании.

Образование в области информационной безопасности продолжает развиваться в соответствии с постоянно меняющимся технологическим ландшафтом. В предстоящем десятилетии можно ожидать следующие тенденции:

1. Увеличение акцента на практическом обучении: вместо простого изучения теоретических аспектов информационной безопасности, все больше вузов будут предлагать студентам реальные проекты и ситуации для улучшения их практических навыков (Возможность развития, 2020).

2. Углубленное изучение новых технологий: такие технологии, как искусственный интеллект, блокчейн и квантовые компьютеры, будут играть все большую роль в курсах информационной безопасности (Крупченко, 2017).

3. Больший акцент на этические вопросы: в связи с ростом сложности и важности информационной безопасности, все больше вузов будут обращать внимание на этические вопросы, связанные с защитой данных и кибербезопасностью (Попова, 2018).

4. Междисциплинарный подход: информационная безопасность связана с многими другими областями, такими как право, бизнес, психология и политология. Будущее образование в этой области, вероятно, будет включать элементы из этих и других областей, чтобы подготовить студентов к многофакторной природе работы в области информационной безопасности (Смирнова, 2017).

5. Развитие дистанционного обучения: технологии удаленного обучения продолжат развиваться, что позволит студентам из разных регионов и стран получать качественное образование в области информационной безопасности без необходимости физического присутствия в учебном заведении (Целуйко, 2017).

В целом, будущее образования в области информационной безопасности в России выглядит многообещающим и будет продолжать адаптироваться к новым технологиям и угрозам.

Заключение

По результатам нашего исследования мы можем сделать следующие выводы:

1. Подготовка специалистов в области информационной безопасности в вузах России столкнулась с целым рядом сложностей и вызовов. Это связано как с быстро меняющейся обстановкой в области киберугроз, так и с необходимостью адаптации образовательных программ к новым технологиям и методам.

2. Существуют проблемы с обновлением учебных программ и материалов, в частности, недостаточно быстрым их обновлением для отражения последних угроз информационной безопасности.

3. Обучение информационной безопасности в вузах требует не только передачи теоретических знаний, но и формирования практических навыков, способствующих противодействию реальным киберугрозам.

4. Существенное значение имеют исследовательские проекты, проводимые в российских вузах и технопарках, такие как «Университет информационной безопасности», «Цифровой прорыв», проекты в Сколково и «Иннополис».

5. Необходимо уделять внимание таким аспектам подготовки специалистов, как социальная инженерия, этика и моральные вопросы, непрерывное обучение и самообразование.

6. Заочная форма обучения по направлению "Информационная безопасность" требует дополнительного внимания и пересмотра подходов к организации обучающего процесса.

Проведенное исследование позволяет сделать вывод о необходимости комплексного подхода к преподаванию информационной безопасности в вузах, включающего постоянное обновление образовательных программ, активное применение современных методик и обучающих технологий, развитие научно-исследовательской работы и проведение обучающих мероприятий в области информационной безопасности.

Список литературы

1. Валеева Е.В. Формирование человека: проблемы образовательного универсума // Вопросы культурологии. 2017. № 4. С. 15-22.

2. Зуфарова А.С. Возможность развития информационно-образовательной среды вуза // Управление образованием: теория и практика. 2020. № 3 (39). С. 81-88.

3. Каберник В.В., Тимофеева О.А. Обеспечение безопасности образовательной среды на примерах США, стран Европы и России // Вестник МГИМО Университета. 2015. № 4 (43). С. 119-129.

4. Козлов О.А., Гузикова Л.А. Информационная безопасность как условие деятельности образовательных организаций // Вопросы методики преподавания в вузе. 2017. Т. 6. № 22. С. 43-50. https://doi.org/10.18720/HUM/ISSN 2227-8591.22.6

5. Крупченко А. К., Кузнецов А. Н., Анзина Т. И. и др. Аксиология иноязычного образования: среднее профессиональное педагогическое образование. Монография. М.: Академия повышения квалификации и профессиональной переподготовки работников образования; 2017. 230 с.

6. Кузина Н.Н. Культура информационной безопасности личности учителя и процесс ее формирования у студентов педагогического вуза // Kant. 2018. № 2 (27). С. 85-91.

7. Обеспечение безопасности в образовательных организациях: теория и практика: учебное пособие / Л.А. Акимова, Е.Е. Лутовина, Л.Г. Пак и др. Оренбург: Издательско-полиграфический комплекс «Университет», 2019. 199 с.

8. Попова Е.А. Формирование ценностных ориентаций у студентов-международников в курсе дисциплины «Иностранный язык» // Вестник Московского государственного лингвистического университета. Образование и педагогические науки. 2018. № 6 (814). С. 124-138.

9. Роберт И.В. Подготовка педагогических кадров в области информационной безопасности личности в условиях цифровой трансформации образования // Информационная безопасность личности субъектов образовательного процесса в цифровой информационно-образовательной среде: сб. науч. тр. М., 2021. С. 151-170.

10. Сидакова А.А. Система норм об обеспечении транспортной безопасности в уголовном законодательстве России и за рубежом // Транспортное право. 2018. №1. С 22-25.

11. Смирнова А.А., Захарова Т.Ю., Синогина Е.С. Киберугрозы безопасности подростков // Ped. Rev. 2017. № 3 (17). С. 99-107.

12. Суворова Г.М., Горичева В.Д. Теория и методика обучения безопасности жизнедеятельности. М.: Юрайт, 2020. 346 с.

13. Тойнби А. Дж. Исследование истории, Возникновение, рост и распад цивилизаций. Т. 1 / пер. с англ. К. Я. Кожурина. М.: АСТ: АСТ МОСКВА, 2009. 670 с.

14. Целуйко А.В., Петроченко В.В. Вопросы информационного обеспечения транспортной безопасности в условиях современности // Транспортное право. 2017. № 4. С. 28-31.
15. Ovchinnikova N., Astafyeva M., Fedotkina E. Internationalization and Interdisciplinary Education In Foreign Language Curricula of Future Innovatics Managers. EDULEARN 21 Proceedings: 13th International Conference on Education and New Learning Technologies; 2021. DOI: 10.21125/edulearn.2021.0683

Aspects of information security training in Russian universities

Sergey E. Golikov
Associate Professor
Sevastopol State University
Sevastopol, Russia
kcl@mail.ru
0000-0000-0000-0000

Vitaly A. Lutsyshen
Associate Professor
Sevastopol State University
Sevastopol, Russia
vitaliy_l@mail.ru
0000-0000-0000-0000

Received 20.03.2023
Accepted 18.04.2023
Published 15.06.2023

10.25726/r0705-5602-5928-e

Abstract

In the decade of information technology, when data becomes a key asset and an instrument of influence, the issues of information security in higher education in Russia become of the most important relevance. Rosobrnadzor data show that in 2023 the number of students studying in specialties related to information security is 150 thousand people, which is 1.2 times more than in 2021. The problems of information security permeate all spheres of human activity. Against this background, over the past 5 years, the number of Russian universities that have included information security disciplines in the general education plan has increased by 15%, reaching 80%. However, an analysis of 500 open training programs showed that only 20% of them imply an integrated approach to information security training. Meanwhile, digital threats are increasing: according to the Bureau for the Coordination of Threats (BCU), in 2022 the number of cyber attacks on educational institutions increased by 35%. This article is an analysis of aspects of information security education in Russian universities.

Keywords

information security, higher education, Rosobrnadzor, BKU, cyberattacks.

References

1. Valeeva E.V. Formirovanie cheloveka: problemy obrazovatel'nogo universuma // Voprosy kul'turologii. 2017. № 4. S. 15-22.
2. Zufarova A.S. Vozmozhnost' razvitija informacionno-obrazovatel'noj sredy vuza // Upravlenie obrazovaniem: teorija i praktika. 2020. № 3 (39). S. 81-88.

3. Kabernik V.V., Timofeeva O.A. Obespechenie bezopasnosti obrazovatel'noj sredy na primerah SShA, stran Evropy i Rossii // Vestnik MGIMO Universiteta. 2015. № 4 (43). S. 119-129.

4. Kozlov O.A., Guzikova L.A. Informacionnaja bezopasnost' kak uslovie dejatel'nosti obrazovatel'nyh organizacij // Voprosy metodiki prepodavanija v vuze. 2017. T. 6. № 22. S. 43-50. https://doi.org/10.18720/HUM/ISSN 2227-8591.22.6

5. Krupchenko A. K., Kuznecov A. N., Anzina T. I. i dr. Aksiologija inojazychnogo obrazovanija: srednee professional'noe pedagogicheskoe obrazovanie. Monografija. M.: Akademija povyshenija kvalifikacii i professional'noj perepodgotovki rabotnikov obrazovanija; 2017. 230 s.

6. Kuzina N.N. Kul'tura informacionnoj bezopasnosti lichnosti uchitelja i process ee formirovanija u studentov pedagogicheskogo vuza // Kant. 2018. № 2 (27). S. 85-91.

7. Obespechenie bezopasnosti v obrazovatel'nyh organizacijah: teorija i praktika: uchebnoe posobie / L.A. Akimova, E.E. Lutovina, L.G. Pak i dr. Orenburg: Izdatel'sko-poligraficheskij kompleks «Universitet», 2019. 199 s.

8. Popova E.A. Formirovanie cennostnyh orientacij u studentov-mezhdunarodnikov v kurse discipliny «Inostrannyj jazyk» // Vestnik Moskovskogo gosudarstvennogo lingvisticheskogo universiteta. Obrazovanie i pedagogicheskie nauki. 2018. № 6 (814). S. 124-138.

9. Robert I.V. Podgotovka pedagogicheskih kadrov v oblasti informacionnoj bezopasnosti lichnosti v uslovijah cifrovoj transformacii obrazovanija // Informacionnaja bezopasnost' lichnosti sub#ektov obrazovatel'nogo processa v cifrovoj informacionno-obrazovatel'noj srede: sb. nauch. tr. M., 2021. S. 151-170.

10. Sidakova A.A. Sistema norm ob obespechenii transportnoj bezopasnosti v ugolovnom zakonodatel'stve Rossii i za rubezhom // Transportnoe pravo. 2018. №1. S 22-25.

11. Smirnova A.A., Zaharova T.Ju., Sinogina E.S. Kiberugrozy bezopasnosti podrostkov // Ped. Rev. 2017. № 3 (17). S. 99-107.

12. Suvorova G.M., Goricheva V.D. Teorija i metodika obuchenija bezopasnosti zhiznedejatel'nosti. M.: Jurajt, 2020. 346 s.

13. Tojnbi A. Dzh. Issledovanie istorii, Vozniknovenie, rost i raspad civilizacij. T. 1 / per. s angl. K. Ja. Kozhurina. M.: ACT: ACT MOSKVA, 2009. 670 s.

14. Celujko A.V., Petrochenko V.V. Voprosy informacionnogo obespechenija transportnoj bezopasnosti v uslovijah sovremennosti // Transportnoe pravo. 2017. № 4. S. 28-31.

15. Ovchinnikova N., Astafyeva M., Fedotkina E. Internationalization and Interdisciplinary Education In Foreign Language Curricula of Future Innovatics Managers. EDULEARN 21 Proceedings: 13th International Conference on Education and New Learning Technologies; 2021. DOI: 10.21125/edulearn.2021.0683