УДК 004.056, 372.862

АКТУАЛЬНЫЕ НАПРАВЛЕНИЯ ПРЕПОДАВАНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ «БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ»

А. М. Соболь[1)], В. П. Кочин[2)]

[1)] *Государственное предприятие «Центр информационных ресурсов и коммуникаций», Минск, Беларусь, sobol@circ.by*
[2)] *Белорусский государственный университет, Минск, Беларусь, kochyn@bsu.by*

В статье рассмотрены актуальные направления преподавания дисциплины «Безопасность информационных систем» для студентов различных профессиональных траекторий. Проведен анализ приказа ОАЦ № 130, предложены примеры лабораторных работ, проектных заданий и методических подходов. Обозначены перспективы развития дисциплины с учетом современных технологий.

Ключевые слова: информационная безопасность; приказ ОАЦ № 130; кибербезопасность; образовательные программы; SIEM; CTF.

CURRENT TRENDS IN TEACHING THE ACADEMIC DISCIPLINE “INFORMATION SYSTEMS SECURITY”

A. M. Sobol[a)], V. P. Kochyn[b)]

[a)] *State Enterprise “Center for Information Resources and Communications” Minsk, Belarus, sobol@circ.by*
[b)] *Belarusian State University, Minsk, Belarus, kochyn@bsu.by*

The article discusses current trends in teaching the discipline “Information Systems Security” to students of various professional trajectories. An analysis of OAC Order № 130 is provided, and examples of laboratory work, design tasks, and methodological approaches are proposed. The prospects for the development of the discipline, taking into account modern technologies, are outlined.

Keywords: information security; OAC Order No. 130; cybersecurity; educational programs; SIEM; CTF.

1. Введение

Развитие информационных технологий сопровождается ростом масштабов и сложности киберугроз, что предопределяет необходимость подготовки специалистов, обладающих компетенциями в области защиты ин-

формационных систем. В Республике Беларусь данное направление регламентируется рядом нормативных правовых актов, среди которых особое значение имеет приказ Оперативно-аналитического центра при Президенте Республики Беларусь (далее – ОАЦ) № 130 [1], определяющий порядок регистрации, классификации и анализа киберинцидентов. Актуализация содержания дисциплины «Безопасность информационных систем» обусловлена необходимостью интеграции национальных регуляторных требований с международными стандартами и лучшими практиками.

2. Современные направления преподавания дисциплины

Современная парадигма преподавания информационной безопасности и кибербезопасности определяется необходимостью подготовки специалистов, которые должны решать задачи как организационно-правовые, так и прикладного характера. В образовательной практике целесообразно выделить следующие ключевые направления.

1. Теоретико-методологическое направление, в котором систематизируются знания об угрозах, уязвимостях и способах их классификации. В данном направлении можно использовать такие инструменты как MITRE ATT&CK и CSV.

2. Криптографическое направление, в котором применяются современные методы шифрования и аутентификации основанные на стандартах Республики Беларусь.

3. Техническое направление, в котором изучаются принципы функционирования межсетевых экранов, систем обнаружения и предотвращения вторжения, средств защиты от атак.

4. Программно-ориентированное направление, в котором изучается безопасное программирование, аудит приложений и развертывание защищенной инфраструктуры.

5. Практико-ориентированное направление. В данном направлении изучается использование программных продуктов по обнаружению вторжения и расследования, такие как: SIEM, DLP, сканер уязвимости, «песочница», а также настройка политик информационной безопасности, согласно группам безопасности и моделирование атак.

6. Научно-исследовательское направление. Данное направление необходимо для самостоятельного повышения уровня компетенции студентов с помощью выполнение курсовых и рефератов на тематику актуальным новым уязвимостям и происшедшим киберинцидентов.

Современные образовательные программы должны учитывать различие в профилях подготовки студентов, даже если они изучают одну и ту

же дисциплину. В контексте курса «Безопасность информационных систем» можно выделить два крупных направления: студенты-программисты и студенты-специалисты по кибербезопасности.

3. Направления содержания дисциплины для различных направлений

Для студентов, чья основная деятельность связана с разработкой программного обеспечения, необходимо делать акцент на интеграцию безопасности в процесс разработки: студент должен не просто владеть языками программирования, но и понимать, какие ошибки ведут к критическим уязвимостям и как их предотвратить. На основании этого предмет должен содержать следующие модули:

– безопасная разработка – освоение методик безопасного проектирования и тестирования программных продуктов. Данный аспект включает в себя работу с практиками OWASP, применение статического и динамического анализа кода, использование инструментов для выявления уязвимостей;

– криптографические библиотеки и протоколы. Понимание правильного применения стандартных средств шифрования, аутентификации и цифровой подписи в прикладных системах;

– принципы безопасной архитектуры. Проектирование приложений с минимизацией возможных точек отказа и уязвимостей, применение концепций Zero Trust, микросервисной безопасности;

– практические навыки. Практические занятия могут включать написание безопасных REST API, внедрение многофакторной аутентификации, использование безопасных контейнерных решений (Docker, Kubernetes).

Студенты, ориентированные на защиту информационных систем в целом, должны комплексно оценивать уровень защищённости систем и управлять процессом реагирования на инциденты. На основании этого можно выделить следующие направления предмета:

– мониторинг и реагирование на инциденты. В этом направлении студенты изучат принципы работы центров кибербезопасности, применение SIEM-систем, методы анализа журналов и сетевого трафика [2, 3];

– управление рисками и соответствие нормативным требованиям предполагает изучение студентами белорусских регламентов (в том числе приказа ОАЦ №130), а также международных стандартов ISO/IEC 27001, NIST Cybersecurity Framework [4, 5];

– методы и средства защиты информации. В этом направлении студенты должны учиться использовать и настраивать межсетевые экраны, системы предотвращения вторжений (IDS/IPS), DLP, антивирусных решений корпоративного уровня [6, 7];

– практические навыки. Практические занятия могут включать анализ вредоносного программного обеспечения, моделирование кибератак (фишинг, SQL-инъекции, XSS), проведение тестирования на проникновения и разработку сценариев реагирования.

Подобное разделение содержания дисциплины оправдано по следующим причинам.

– Различие профессиональных траекторий. Программисты будут создавать программные продукты, а специалисты по ИБ – их защищать и обеспечивать контроль функционирования. Унификация подхода привела бы к чрезмерной поверхностности подготовки.
– Разные наборы компетенций. Для программистов важно научиться интегрировать защитные механизмы в код, тогда как для специалистов по ИБ приоритетом является понимание архитектуры угроз и администрирование систем безопасности.
– Практическая востребованность. Работодатели ожидают от программистов умения писать защищённый код, а от специалистов по ИБ – способности обнаруживать и предотвращать атаки. Следовательно, учебный процесс должен отвечать запросам рынка труда.
– Эффективность образовательного процесса. Дифференциация позволяет избежать перегрузки студентов избыточной информацией, которая не имеет прямого отношения к их будущей профессиональной деятельности.

Таким образом, разграничение содержания курса «Безопасность информационных систем» в зависимости от профиля подготовки не только обосновано, но и необходимо для формирования специалистов, способных эффективно работать в реальных условиях.

4. Методические подходы к преподаванию дисциплины «Безопасность информационных систем»

Преподавание дисциплины «Безопасность информационных систем» требует сочетания различных методических подходов, которые обеспечивают не только усвоение теоретического материала, но и формирование практических навыков, востребованных на рынке труда. Поэтому целесообразно дисциплину разделить на следующие модули.

1. Лекционный модуль. Лекции представляют собой основу курса, обеспечивая систематизацию знаний о ключевых понятиях, нормативных

требованиях и современных тенденциях в области информационной безопасности. Их задача заключается в формировании у студентов целостного представления о предметной области, знакомстве с национальными регуляторными документами (например, приказ ОАЦ №130 [1]) и международными стандартами (ISO/IEC 27001 [3], NIST CSF [4]). Важным является внедрение в лекционный курс элементов проблемного изложения и аналитических обзоров, позволяющих студентам самостоятельно выявлять закономерности в развитии киберугроз и средств защиты.

2. Семинарский модуль. Семинарские занятия направлены на развитие навыков критического мышления и анализа практических кейсов. Здесь целесообразно обсуждать реальные киберинциденты, рассматривать правоприменительную практику и проводить дискуссии по этическим аспектам информационной безопасности. В качестве методических приёмов могут использоваться дебаты, анализ судебных дел, работа с открытыми отчётами (например, DBIR [5]). Такой формат стимулирует студентов к самостоятельному поиску решений и обоснованию своих позиций.

3. Лабораторный модуль. Практические занятия являются ключевым элементом подготовки. Лабораторные работы должны охватывать широкий спектр задач: от настройки межсетевых экранов и систем обнаружения атак до анализа журналов событий и проведения форензики. Для программистов упор делается на выявлении уязвимостей в коде и безопасном программировании (OWASP Top 10 [4]), а для специалистов по кибербезопасности – на использовании инструментов SIEM, IDS/IPS и средств анализа трафика. Важно, чтобы лабораторные задания имели пошаговую методику выполнения и завершались мини-отчётами, формирующими у студентов навыки документирования своей работы.

4. Проектный модуль. Проектная деятельность предполагает выполнение заданий, направленных на интеграцию теоретических и практических знаний. Примеры таких проектов может быть: разработка регламента информационной безопасности для учебного подразделения, создание прототипа защищённого веб-приложения, моделирование сценариев реагирования на инциденты. Работа в проектных группах позволяет сформировать навыки командной деятельности и управления распределёнными задачами, что особенно актуально для будущих специалистов в сфере кибербезопасности.

5. Соревновательный модуль. Современные методики преподавания предполагают использование игровых и соревновательных форматов (CTF, Red Team vs. Blue Team). Эти подходы позволяют студентам работать в условиях, максимально приближённых к реальным кибератакам. Формат CTF способствует закреплению навыков поиска уязвимостей и их устранения, а сценарии «красная команда против синей команды» учат взаимодействию между атакующей и обороняющейся сторонами.

6. Инновационные формы обучения. Перспективным направлением является внедрение дистанционных лабораторных комплексов и киберполигонов, где студенты могут отрабатывать практические сценарии без привязки к физической инфраструктуре. Дополнительно можно рассмотреть использование адаптивных образовательных платформ, которые подстраивают сложность заданий под уровень знаний обучающихся.

5. Заключение

Преподавание дисциплины «Безопасность информационных систем» является ключевым элементом подготовки специалистов. Опора на национальные регуляторные акты (приказ ОАЦ № 130) обеспечивает соответствие национальным требованиям, а интеграция международных стандартов формирует универсальные компетенции. Разделение по профессиональным траекториям (программисты, специалисты по кибербезопасности) позволяет учитывать специфику деятельности, а модульный методический подход обеспечивает преемственность знаний.

Библиографические ссылки

1. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь №130 от 25.07.2023 «О мерах по реализации Указа Президента Республики Беларусь от 14 февраля 2023 г. № 40». URL: https://www.oac.gov.by/public/content/files/files/law/prikaz-oac/2023%20-%20130.pdf (дата обращения: 10.09.2025).
2. *Sobol A., Kochyn V*. Modeling the state of information security of a smart campus // Open Semantic Technologies for Intelligent Systems (OSTIS) : Research Papers Collection / Belarusian State University of Informatics and Radioelectronics ; eds.: V. V. Golenkov [et al.]. Minsk, 2024. Issue 8. P. 353–358.
3. *Sobol A., Kochyn V., Huk A. //* "Information Security System Models in Smart Campuses," 2024 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM), Sochi, Russian Federation, 2024, P. 750–754.
4. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования (ISO/IEC 27001:2022). Введ. 01.11.2022. Минск: Госстандарт, 2022.
5. National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. Gaithersburg, MD: NIST, 2018.
6. OWASP Foundation. OWASP Top Ten Web Application Security Risks 2021. URL: https://owasp.org/Top10 (date of access: 13.09.2025).
7. Verizon. Data Breach Investigations Report (DBIR). 2023. URL: https://www.verizon.com/business/resources/reports/dbir (date of access: 14.09.2025).