

Подготовка онлайн курса-интенсива по информационной безопасности*Болтовский Гавриил Александрович**Приамурский государственный университет им. Шолом-Алейхема**Студент***Аннотация**

В данной статье описывается разработка массового онлайн курса по информационной безопасности. Разработана структура и содержание курса, созданный интенсив опубликован на платформе Stepik. Результатом исследования является созданный учебный материал с подробным описанием принципов его построения.

Ключевые слова: информационная безопасность, массовый онлайн курс, Stepik

Preparation of an intensive online course on information security*Boltovsky Gavriil Alexandrovich**Sholom-Aleichem Priamursky State University**Student***Abstract**

This article describes the development of a massive online course on information security. The structure and content of the course have been developed, and the intensive course has been published on the Stepik platform. The result of the research is the creation of educational material with a detailed description of the principles of its construction.

Keywords: information security, massive online course, Stepik

1 Введение**1.1 Актуальность исследования**

Разработка массового онлайн курса по информационной безопасности является актуальной в условиях стремительного роста числа киберугроз и необходимости формирования базовых навыков у широкого круга пользователей. Онлайн-формат позволяет обеспечить доступность образовательного материала для студентов, молодых специалистов и всех заинтересованных лиц независимо от географического положения. Кроме того, систематическое введение интерактивных практических заданий и инструментов информационной безопасности способствует формированию компетенций, необходимых для дальнейшего углубленного изучения дисциплины.

1.2 Обзор исследований

И. Д. Рудинский [1] отмечает, что подготовка специалистов по информационной безопасности в системе среднего профессионального образования сталкивается с рядом проблем, включая недостаточное практическое применение теоретических знаний и отсутствие стандартизированных учебных программ. Он подчеркивает необходимость интеграции современных образовательных технологий и практико-ориентированных подходов для повышения эффективности обучения. Д.Я. Околот [2] предлагает компетентностную модель специалиста по информационной безопасности, которая включает сочетание технических навыков, аналитических способностей и знаний нормативно-правовой базы. Автор выделяет, что эффективное обучение должно ориентироваться на формирование именно этих компетенций через практические задания и кейс-методы, что напрямую соотносится с концепцией предлагаемого курса. Д.А. Новиков, В. И. Борисов и А. Г. Остапенко [3] в своих исследованиях указывают на инновационные тренды в организации учебного процесса подготовки специалистов по защите информации, акцентируя внимание на формировании компетенций в области управления информационными рисками и обеспечения безопасности инфокоммуникационных технологий. Они отмечают, что применение интерактивных и практико-ориентированных инструментов, таких как лабораторные работы и тренажеры, значительно повышает эффективность усвоения материала. И. И. Баранкова [4] рассматривает компетентностно-ориентированный подход к созданию лабораторий и учебно-тренировочных средств при подготовке специалистов по информационной безопасности. Автор выделяет, что включение в учебный процесс практических модулей с реальными сценариями атак и защиты позволяет формировать у студентов навыки анализа угроз и принятия решений в условиях ограниченной информации.

Таким образом, современные исследования подтверждают необходимость практико-ориентированного, компетентностного подхода к обучению ИБ, который реализован в представленном онлайн курсе-интенсиве через модули с практическими заданиями и интерактивными кейсами.

1.3 Цель исследования

Целью исследования является создание онлайн курса-интенсива, который обеспечивает первичное освоение инструментов информационной безопасности и формирование базовых компетенций для дальнейшего углубленного обучения.

1.4 Постановка задачи

В рамках исследования была разработана структура курса-интенсива, включающая модули, уроки и практические задания, что позволило организовать учебный процесс логично и последовательно. Содержание курса было обосновано с учетом современных требований к компетенциям специалистов по информационной безопасности, а учебные материалы

включали практические кейсы, направленные на формирование навыков анализа угроз и применения инструментов ИБ. Для реализации курса была использована платформа Sterik с интерактивными заданиями и тестами, что обеспечило возможность оценки усвоения материала в онлайн-среде.

2 Результаты и обсуждения

Курс состоит из двух основных модулей, каждый из которых включает по пять уроков, что в сумме даёт десять уроков. Первый модуль ориентирован на базовое знакомство с информационной безопасностью и освоение базовых инструментов, второй модуль – на практическое применение знаний и подготовку к более сложным темам, таким как анализ угроз, работа с уязвимостями и понимание человеческого фактора. Кроме того, в курсе предусмотрена дополнительная тема – социальная инженерия и человеческий фактор – как отдельный урок, который логично завершает интенсив, связывая техническую и организационную стороны ИБ (табл. 1).

Таблица 1 – Структура курса

Модуль	№ урока	Название урока	Темы урока	Практическая задача
Модуль 1: Основы информационной безопасности и базовые инструменты	1	Введение в информационную безопасность	СИА-триада, типы угроз и нарушителей, направления ИБ	Определить активы, угрозы и меры защиты для условной компании (мини threat modeling)
	2	Операционные системы и безопасность	Роль ОС в ИБ, различия Windows/Linux, права доступа, базовые команды Linux	Настроить пользователей и права доступа в Linux, выявить потенциальные риски конфигурации
	3	Сетевые основы для ИБ	TCP/IP, порты, протоколы, локальные и глобальные сети, firewall, NAT, VPN, обзор сетевых атак	Проанализировать сетевую схему и определить потенциальные уязвимые точки
	4	Инструменты сетевого анализа	Wireshark, анализ сетевого трафика, выявление сетевых аномалий	Проанализировать pcap-файл и определить подозрительный трафик
	5	Основы криптографии	Симметричное и асимметричное шифрование, хэш-функции,	Использовать OpenSSL для хэширования и шифрования

			цифровые подписи	данных, сравнить результаты
Модуль 2: Практическое знакомство с защитой и атаками инструментами	6	Уязвимости и их классификация	Понятие уязвимости, CVE, CVSS, OWASP Top 10, жизненный цикл уязвимости	Проанализировать описание CVE и оценить её критичность для системы
	7	Инструменты сканирования уязвимостей	Nmap, vulnerability scanning, ограничения сканеров	Выполнить сканирование хоста с помощью Nmap и интерпретировать результаты
	8	Основы веб-безопасности	Работа веб-приложений, типовые веб-атаки (XSS, SQLi), анализ HTTP	Проанализировать HTTP-запросы и выявить небезопасные параметры
	9	Логи и основы мониторинга	Зачем нужны логи, типы логов, основы SIEM	Проанализировать набор логов и обнаружить подозрительное событие
	10	Итоговый практикум и пути развития	Связь всех тем курса, сценарии атак и защиты, дальнейшие направления обучения	Разобрать упрощённый инцидент ИБ: от обнаружения до предложений по защите
Дополнительно	11	Социальная инженерия и человеческий фактор	Понятие социальной инженерии, типовые атаки (phishing, vishing, smishing), pretexting, baiting, tailgating, организационные меры защиты	Проанализировать набор писем и сообщений, определить признаки социальной инженерии и предложить меры защиты для компании

Каждый урок курса включает теоретическую часть, где подробно рассматриваются основные концепции, терминология и механизмы работы инструментов ИБ, а также практическую задачу, ориентированную на отработку конкретных навыков. Практические задания формулируются таким образом, чтобы слушатели могли самостоятельно применять изученные методы, анализировать реальные или смоделированные сценарии и принимать решения по защите информации. Такой подход обеспечивает сочетание

обучения «знаниями» и «умениями», что важно для формирования компетентностного уровня у начинающих специалистов.

В рамках первого модуля участники изучают основные понятия информационной безопасности, модели угроз, структуру операционных систем, основы сетевых технологий и криптографию. Такой порядок построен на принципе «от общего к частному»: сначала создаётся фундаментальное понимание ключевых концепций и структуры безопасности, затем слушатели осваивают инструменты, которые позволяют применять эти знания на практике. Практические задачи включают threat modeling, настройку прав доступа, анализ сетевого трафика и базовое шифрование, что формирует уверенность в работе с основными инструментами ИБ.

Второй модуль строится на знаниях, полученных в первом, и направлен на углублённое понимание угроз и методов их анализа. Он включает темы классификации уязвимостей, сканирования систем на предмет уязвимостей, основы веб-безопасности и мониторинга событий безопасности. Последний урок модуля посвящён социальному фактору – социальной инженерии и защите от атак на человеческий фактор. Такой финальный шаг выбран не случайно: он показывает слушателю, что информационная безопасность – это не только технологии, но и организационные и психологические аспекты, что формирует комплексное понимание предмета. Практические задачи второго модуля ориентированы на применение сканеров уязвимостей, анализ HTTP-запросов, работу с логами и выявление инцидентов, что позволяет студентам почувствовать реальные сценарии работы специалистов по ИБ.

Таким образом, структура курса построена по принципу наращивания сложности: от базовых знаний и инструментов к практическим кейсам и анализу инцидентов. Она сочетает теоретическое введение с практическими заданиями на каждом этапе, что соответствует компетентностному подходу в образовании и обеспечивает формирование навыков, необходимых для дальнейшего углубленного изучения информационной безопасности. Главная страница курса изображена на рисунке (рис. 1)

Интенсив по информационной безопасности

Курс предназначен для начинающих специалистов, которые хотят познакомиться с ключевыми принципами информационной безопасности и научиться работать с базовыми инструментами анализа и защиты. В ходе интенсива слушатели изучат работу веб-приложений, сетевые основы, криптографию, типовые уязвимости и атаки, а также... [Ещё](#)

Начальный уровень



О курсе

Чему вы научитесь

- Понимать базовые принципы информационной безопасности, включая конфиденциальность, целостность и доступность данных.
- Разбираться в архитектуре веб-приложений, серверов и баз данных, а также понимать их точки уязвимости.
- Анализировать HTTP-запросы и ответы, выявлять подозрительные или небезопасные параметры.
- Понимать типовые веб-атаки, такие как XSS и SQL-инъекции, и оценивать потенциальные риски для приложений.

Бесплатно

[Поступить на курс](#)

Учиться можно сразу

В курс входят
10 уроков

Рисунок 1 – Главная страница курса

3. Выводы

Таким образом, создан онлайн курса доступный для прохождения [5].

Библиографический список

1. Рудинский И. Д. Проблемы и задачи подготовки специалистов по информационной безопасности в системе среднего профессионального образования // Известия Балтийской государственной академии рыбопромыслового флота: психолого-педагогические науки. 2017. № 4(42). С. 63-69.
2. Околот Д. Я. Компетентностная модель специалиста по информационной безопасности // Балтийский морской форум: материалы VI Международного Балтийского морского форума: в 6 томах, Калининград, 03–06 сентября 2018 года. Том 6. Калининград: Обособленное структурное подразделение «Балтийская государственная академия рыбопромыслового флота» федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Калининградский государственный технический университет», 2018. С. 238-242.
3. Инновационные тренды в организации учебного процесса подготовки специалистов по защите информации: формирование компетенций в области управления информационными рисками и обеспечения безопасности инфокоммуникационных технологий / Д. А. Новиков, В. И. Борисов, А. Г. Остапенко [и др.] // Информация и безопасность. 2014. Т. 17, № 3. С. 360-365.
4. Баранкова, И. И. Компетентностно-ориентированный подход к формированию лабораторий и учебно-тренировочных средств при подготовке специалистов в области информационной безопасности // Информационное противодействие угрозам терроризма. 2015. Т. 1. № 25. С. 46-50.
5. Интенсив по информационной безопасности. URL: <https://stepik.org/course/270540/> (дата обращения: 14.01.2026).