УДК 303.732.4, 004.056

О НОВОМ КОНЦЕПТУАЛЬНОМ ПОДХОДЕ ПОДГОТОВКИ БАКАЛАВРОВ ПО ПРОФИЛЮ «БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ»

Минзов Анатолий Степанович[1], Токарева Надежда Александровна[2], Немчанинова София Вадимовна[3], Шевченко Алексей Валерьевич[4]

[1]Доктор технических наук, профессор;
Государственный университет «Дубна»;
Россия, 141980, Московская обл., г. Дубна, ул. Университетская, 19;
e-mail: minzovas@gmail.com.

[2]Кандидат физико-математических наук, доцент;
Государственный университет «Дубна»;
Россия, 141980, Московская обл., г. Дубна, ул. Университетская, 19;
e-mail: tokareva@uni-dubna.ru.

[3]Старший преподаватель;
Государственный университет «Дубна»;
Россия, 141980, Московская обл., г. Дубна, ул. Университетская, 19;
e-mail: sbobylova94@gmail.com.

[4]Ассистент;
Государственный университет «Дубна»;
Россия, 141980, Московская обл., г. Дубна, ул. Университетская, 19;
e-mail: leviathan0909@gmail.com.

Представлен анализ опыта подготовки бакалавров кафедры информационных технологий по профилю «Безопасность информационных систем», определены тенденции развития этого направления подготовки и обоснование требований дальнейшего его развития с учетом современных повышенных требований к ИТ-проектам по безопасности и доверию к ним. При проведении исследований использовался системный анализ для анализа требований к специалистам ИТ и ИБ в условиях повышения уровня требований к надёжности, безопасности и уровня доверия к разрабатываемому программному обеспечению. Полученные результаты позволят провести коррекцию учебного плана и рабочих учебных программ для совершенствования компетенций выпускников по профилю «Безопасность информационных систем» в области обеспечения информационной безопасности ИТ-проектов и уровня доверия к ним.

Ключевые слова: программное обеспечение, безопасность приложений, обучение, образование, информационная безопасность, кибербезопасность, доверие.

Для цитирования:
О новом концептуальном подходе подготовки бакалавров по профилю «Безопасность информационных систем» / А. С. Минзов, Н. А. Токарева, С. В. Немчанинова, А. В. Шевченко // Системный анализ в науке и образовании: сетевое научное издание. 2024. № 3. С. 140-147. EDN: KMRMGP. URL: https://sanse.ru/index.php/sanse/article/view/630.

ABOUT THE NEW CONCEPTUAL APPROACH TO TRAINING BACHELOR'S DEGREE STUDENTS IN THE FIELD OF INFORMATION SYSTEMS SECURITY

Minzov Anatoly S.[1], Tokareva Nadezhda A.[2], Nemchaninova Sofia V.[3], Shevchenko Alexey V.[4]

[1]Grand PhD in Engineering science, professor;
Dubna State University;

19 Universitetskaya Str., Dubna, Moscow region, 141980, Russia;
e-mail: minzovas@gmail.com.

[2]PhD in Physical and Mathematical Sciences, associate professor;
Dubna State University;
19 Universitetskaya Str., Dubna, Moscow region, 141980, Russia;
e-mail: tokareva@uni-dubna.ru.

[3]Senior teacher;
Dubna State University;
19 Universitetskaya Str., Dubna, Moscow region, 141980, Russia;
e-mail: sbobylova94@gmail.com.

[4]Assistant;
Dubna State University;
19 Universitetskaya Str., Dubna, Moscow region, 141980, Russia;
e-mail: leviathan0909@gmail.com.

The analysis of the experience of the Department of Information Technology of training bachelors in the field of information systems security is presented. The trends in this field of training and the requirements for its enhancement, considering modern increased requirements on security for IT projects and trust in them are determined. During the research, a system analysis was used to analyze the requirements for IT and information security specialists in the context of increasing the level of requirements for reliability, security and the level of trust in the software. The results obtained will allow for the correction of the training plan to improve the competencies of graduates in the field of information security of IT projects and the level of trust in them.

Keywords: software, application security, training, education, information security, cybersecurity, trust.

For citation:
Minzov A. S., Tokareva N. A., Nemchaninova S. V., Shevchenko A. V. About the new conceptual approach to training bachelor's degree students in the field of information systems security. *System analysis in science and education,* 2024;(3):104-147 (in Russ). EDN: KMRMGP. Available from: https://sanse.ru/index.php/sanse/article/view/630.

Введение

Более 10 лет назад по инициативе директора института системного анализа и управления Черемисиной Е. Н. кафедре информационных технологий была поставлена задача по разработке концепции нового образовательного профиля, в котором бы осуществлялась подготовка выпускников, владеющих компетенциями на стыке двух направлений: информационных технологий и информационной безопасности. Этому решению предшествовал наш анализ требований к профессиональным компетенциям ИТ специалистов в условиях интенсивного развития информационных технологий и методов искусственного интеллекта. Уже в то время стало вполне очевидно, что интенсивное развитие информационных технологий и разработки программного обеспечения требует повышенного внимания к обеспечению информационной безопасности, надёжности и повышения уровня доверия к создаваемому ПО. Это потребовало привлечения к проектной деятельности ИТ-специалистов с новыми расширенными компетенциями в сфере информационной безопасности. Была разработана модель выпускника, которая предполагала расширенный состав компетенций, включающий не только разработку, внедрение и сопровождение информационных систем и технологий, но и технологии построения систем защиты информации на основе международных стандартов [1-3] и нормативных документов ФСТЭК и ФСБ по защите конфиденциальной информации [4-9]. Выпускники этого профиля обладали компетенциями в области разработки архитектур информационной безопасности технических средств [10], защиты информации от утечки по акустическим, виброакустическим, электромагнитным, параметрическим, ПЭМИН и другим каналам.

Начиная с 2015 года ситуация в сфере развития методологии разработки ПО резко стала меняться. Появились новые технологии ускоренной разработки ИТ-проектов [11-15]. Этому во многом способствовало начало промышленной революции (*Industry* 4.0), основанной на массовом внедрении информационных технологий в промышленность, масштабной автоматизации бизнес-процессов и

распространении искусственного интеллекта. Интенсивное развитие информационных технологий (ИТ) и их повсеместное распространение привело к появлению новой проблемы, связанной с обеспечением их безопасного применения. При этом, под безопасным применением ИТ мы понимаем способность их функционирования, не приводящее к утечке информации, несанкционированному доступу к ней, а также способность ИТ противостоять атакам на них. Часть этих угроз может быть снята путем создания системы защиты на уровне архитектуры информационной безопасности и применением технических и организационных мер защиты. Однако, большая часть мер обеспечения безопасности связана с низким уровнем развития методологии защиты информации на этапе проектирования ИТ. Отсюда и возникла необходимость разработки новой модели выпускника профиля ИТ, способного обеспечивать разработку безопасного ПО с высоким уровнем доверия к нему.

В настоящее время стали применяться новые технологии проектирования ИТ *DevOps* (*development & operations*), представляющие собой набор методик и инструментов, позволяющих автоматизировать процессы разработки ПО. Эти технологии основаны на идее постоянного развития функциональности ИТ с периодом 2-3 недели, что создает большие проблемы с обеспечением безопасности и системы ее контроля. В этой технологии вопросы безопасности рассматриваются после проектирования новых функций ИТ, а модель угроз не разрабатывается вообще. Отсюда возникает и научная задача — развитие методологии проектирования безопасного ПО на всех этапах его жизненного цикла и разработка новой компетентностной модели подготовки выпускников кафедры ИТ, способных решать эффективно эти задачи. Сегодня необходимость совмещения этих направлений отражена в новых образовательных стандартах магистратуры по направлению информационная безопасность и в рекомендациях профильного УМО.

1. *Состояние системы подготовки выпускников по профилю «Безопасность информационных систем» в институте системного анализа и управления*

Образовательная программа и учебный план были разработаны в соответствии с требованиями ФГОС 09.03.02 «Информационные системы и технологии». Этим стандартом объектами профессиональной деятельности выпускников, освоивших программы бакалавриата по этому направлению, были определены следующие: информационные процессы, технологии, системы и сети, их инструментальное (программное, техническое, организационное) обеспечение, способы и методы проектирования, отладки, производства и эксплуатации информационных технологий и систем в различных сферах деятельности и, в том числе, в сфере безопасности информационных систем. Учитывая потребности заказчиков и работодателей в особой экономической зоне города Дубна на выпускников институте системного анализа и управления (ИСАУ) государственного университета «Дубна», был сформирован профиль образовательной программы как «Безопасность информационных систем». Этот профиль получил направление близкое к 10.03.01 «Организация и технологии защиты информации» и, по существу, обеспечил подготовку бакалавров на стыке двух актуальных направлений. Выбор этого профиля был неслучайным, так как более половины всех видов деятельности специалистов в области информационных технологий связанные с вопросами разработки, внедрения сопровождения информационных систем в сфере защиты информации выполняются ИТ-специалистами. Учебный план профиля включал следующие дисциплины (табл. 1).

Табл. 1. Распределение специальных дисциплин для профиля «Безопасность информационных технологий»

№№	Специальные дисциплины	Кол-во часов
1	Управление информационной безопасностью	144
2	Модели конфиденциальности, целостности и доступности информации	144
3	Программно-аппаратные средства защиты информации	108
4	Криптографические методы и средства защиты информации	108
5	Инженерно-технические методы и средства защиты информации	108

6	Концепции международных стандартов по обеспечению информационной безопасности	72
7	Защита информации в смарт-контрактах и блокчейн	72
8	Интеллектуальные системы поддержки принятия решений в системах информационной безопасности	108
10	Методы и технологии расследования инцидентов информационной безопасности	108
11	Аудит информационной безопасности	108

В приведённом перечне дисциплин (табл.1) 612 часов относится к базовым дисциплинам, а 468 часов (1-6) к дисциплинам по выбору. Это значительно превышает уровень требований профессиональной переподготовки персонала по направлению «Информационная безопасность».

Темы выпускных работ бакалавров разрабатывались для решения задач в сфере информационной безопасности с использованием информационных технологий. В качестве примера можно привести следующие темы:

1. Технологии разработки безопасного программного обеспечения.
2. Методы и технологии обезличивания персональных данных.
3. Технологии обеспечения информационной безопасности в условиях удаленной работы.
4. Планирование непрерывности бизнеса в системе управления информационной безопасностью.
5. Разработка обучающего кейса по управлению рисками информационной безопасности.
6. Оценка возможности применения легковесных криптографических алгоритмов в Интернете вещей и др.

Оснащенность профиля «Безопасность информационных систем» обеспечивала проведение практических и лабораторных занятий по учебному плану. Эти занятия проводятся в специализированных классах «Технические средства защиты информации» и «Сетевая безопасность». В состав этих классов входит следующее оборудование:

1. Технические средства радиомониторинга (Касандра-210, индикаторы электромагнитного излучения, имитационные средства несанкционированного доступа к информации).
2. Многофункциональный поисковый прибор ST 500 ПИРАНЬЯ для поиска, идентификации и локализации закладных устройств.
3. Комплексы средств контроля и управления доступом (специализированный стенд).
4. Комплекс *Vipnet* для защиты каналов связи и рабочих мест.
5. Комплекс Континент-4 для защиты каналов связи и рабочих мест.
6. Специализированные стенды по исследованию безопасности сетей.
7. Специализированное программное обеспечение: *SIEM*, *DLP*, Антивирусы, *IDS*, *IPS*, а также свободно распространяемое программные обеспечение.

Более чем 10-летний опыт подготовки бакалавров по этому профилю показал, что выпускники этого профиля достаточно легко адаптируются к разработке, внедрению и эксплуатации программного обеспечения для защиты информации в корпоративных информационных системах. В отдельных случаях выпускники этого профиля используются для решения задач в сфере информационных безопасности. Кроме того, уровень их подготовки позволяет пройти дальнейшее обучение в магистратуре по направлению 10.04.01 (информационная безопасность).

Однако, переход нашего общества к концепции *Industry* 4.0 поставил перед системой подготовки ИТ-специалистов новую и весьма сложную задачу – ***разработка методов и технологий ускоренного безопасного проектирования ИС с требуемым уровнем доверия к ним.*** Это потребовало перехода к другой концепции обучения, в которой бы при проектировании информационных систем предусматривалась одновременная работа ИТ-специалистов и специалистов в области безопасности разработки ИТ на каждом этапе работ. Одним из таких направлений является технология *DevOps* [11-14], в которой предусматривается работа специалиста по информационной безопасности, контролирующего статические и динамические свойства программного модуля на наличие в нём недекларированных функций, скриптов, ссылок на недоверенные внутренние и внешние источники, опасных конструкций, позволяющих перехватывать управление или обходить контролирующие процессы и выполнять другие функции, относящиеся к информационной безопасности. Это и послужило началом разработки такой концепции.

2. Основное содержание нового концептуального подхода к разработке безопасного ПО

Новый концептуальный подход к разработке безопасного программного обеспечения включает следующий полный цикл работ, связанных с обеспечением безопасного проектирования:

1. Моделирование угроз. Этот этап осуществляется на начальном этапе проектирования. Для этого проводится разработка архитектуры безопасности проекта ИТ путем описания класса ***ADV*** [10]. Этот класс определяет, в конечном счете, политику безопасности по отношению к функциям в ПО, которые определены в проекте ИТ. В настоящее время в технологиях *DevOps* этот этап не предусматривается, а модель угроз не создается.
2. *SAST* (статическое тестирование безопасности приложений): внедрятся на ранних этапах разработки, включением в интегрированную среду разработки (*IDE*), чтобы обеспечить мгновенную обратную связь с разработчиками.
3. *DAST* (динамическое тестирование безопасности приложений): применяется для тестирования версий программного обеспечения перед выпуском ПО, гарантируя выявление и устранение уязвимостей.
4. Тестирование на проникновение – обычно проводится как заключительная проверка перед развертыванием приложения, позволяющая получить представление о его безопасности с точки зрения злоумышленника.

3. Предложения по практической реализации нового концептуального подхода в системе подготовки бакалавров по профилю «Безопасность информационных систем»

Для практической реализации новой концепции подготовки бакалавров по профилю «Безопасность информационных систем» требуется провести изменения в блоке дисциплин, относящихся к информационным технологиям и системам и в блоке дисциплин, относящихся к дисциплинам по защите информации и проектированию безопасного программного обеспечения. Перечень дисциплин по направлению информационных технологий представлен в табл. 2.

Табл. 2. Перечень специальных дисциплин по направлению информационные технологии и системы

№№-	Специальные дисциплины по направлению ИТ	Кол-во час.
1	Введение в программирование	144
2	Объектно-ориентированное программирование	144
3	Архитектура и проектирование вычислительных систем	144
4	Структуры и алгоритмы обработки данных	144
5	Разработка приложений с использованием технологии баз данных	144
6	Технологии программирования	144
7	Веб технологии и разработка веб-приложений	144
8	Стандартизация и сертификация программных средств	72
9	Машинное обучение и анализ данных	144
10	Проектирование и тестирование пользовательского интерфейса программных продуктов	108
11	Тестирование программного обеспечения	72

Общий объем дисциплин направления ИТ составляет 1404 часов. Он формируется за счёт перераспределение нагрузки по дисциплинам первого и второго блоков дисциплин по направлению ИБ и проектирование безопасного программного обеспечения.

В табл. 3 представлены дисциплины блока направления ИБ.

Табл. 3. Перечень специальных дисциплин по направлению ИБ и проектирование безопасного ПО

№№	Специальные дисциплины ИБ	Кол-во часов
1	Управление информационной безопасностью	144
3	Программно-аппаратные средства защиты информации	108
4	Криптографические методы и средства защиты информации	144
5	Инженерно-технические методы и средства защиты информации	108
8	Интеллектуальные системы поддержки принятия решений в системах информационной безопасности	74
10	Методы и технологии расследования инцидентов информационной безопасности	74
11	Аудит информационной безопасности	74
12	Методы и технологии безопасной разработки программного обеспечения	108
13	Методы и технологии построения архитектуры информационной безопасности ИТ-проекта	108
14	Технологии проведения статического анализа исходного кода	108
15	Технологии проведения динамического анализа исходного кода	108
16	Тестирование на проникновение приложения	74

Общий объем дисциплин по направлению ИБ и проектировании безопасного ПО составляет 1232 часа. В основе этого блока дисциплин положены технологии разработки безопасного ПО [16-25].

Заключение

Предложен новый концептуальный подход к формированию профиля направления 09.03.02 «Информационные системы и технологии», позволяющий управлять безопасностью ИТ-проекта на всех этапах его разработки с использованием модели угроз, архитектуры информационной безопасности, технологии статического исследования исходного кода, технологии динамического исследования кода на выявление уязвимостей в среде разработки проекта и тестирования ИТ-проекта на проникновение на завершающем этапе работ. Такой подход позволяет сформировать у выпускника направления 09.03.02 профессиональное мышление в сфере информационной безопасности способного принимать участие в проектировании безопасного ПО в технологиях *DevOps* и решать другие задачи, связанные с разработкой и эксплуатацией систем управления информационной безопасностью.

Список источников

1. ГОСТ Р ИСО/МЭК 27001-2021. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности : дата введения – 01.01.2022 / Федеральное агентство по техническому регулированию и метрологии // Электронный фонд нормативно-технической и нормативно-правовой информации. – АО «Кодекс», 2024. – URL: https://docs.cntd.ru/document/1200181890.
2. ГОСТ Р ИСО/МЭК 27002-2021. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности : дата введения – 30.11.2021 / Федеральное агентство по техническому регулированию и метрологии // Электронный фонд нормативно-технической и нормативно-правовой информации. – АО «Кодекс», 2024. – URL: https://docs.cntd.ru/document/1200179669.
3. ГОСТ Р ИСО/МЭК 27005-20010. Информационная технология. Методы и средства обеспечения информационной безопасности. Менеджмент риска информационной безопасности : дата

введения – 01.12.2011 / Федеральное агентство по техническому регулированию и метрологии // Электронный фонд нормативно-технической и нормативно-правовой информации. – АО «Кодекс», 2024. – URL: https://docs.cntd.ru/document/1200084141.
4. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных : постановление Правительства РФ N 1119 от 01.11.2012 // Электронный фонд нормативно-технической и нормативно-правовой информации. – АО «Кодекс», 2024. – URL: https://docs.cntd.ru/document/902377706.
5. Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений : постановление Правительства Российской Федерации N 127 от 8.02.2018 // Электронный фонд нормативно-технической и нормативно-правовой информации. – АО «Кодекс», 2024. – URL: https://docs.cntd.ru/document/556499040.
6. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах : приказ Федеральной службы по техническому и экспортному контролю № 17 от 11.02.2013 // Электронный фонд нормативно-технической и нормативно-правовой информации. – АО «Кодекс», 2024. – URL: https://docs.cntd.ru/document/499002630.
7. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных : приказ Федеральной службы по техническому и экспортному контролю № 21 от 18.02.2013 // Электронный фонд нормативно-технической и нормативно-правовой информации. – АО «Кодекс», 2024. – URL: https://docs.cntd.ru/document/499005278.
8. Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды : приказ ФСТЭК России № 31 от 14.03.2014 // Электронный фонд нормативно-технической и нормативно-правовой информации. – АО «Кодекс», 2024. – URL https://docs.cntd.ru/document/499084780.
9. Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации : приказ ФСТЭК России № 239 от 25.12.2017 (ред. от 20.02.2020) // Электронный фонд нормативно-технической и нормативно-правовой информации. – АО «Кодекс», 2024. – URL: https://docs.cntd.ru/document/542616931.
10. ГОСТ Р ИСО/МЭК 15408-3-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности: дата введения – 01.09.2014 / Федеральное агентство по техническому регулированию и метрологии // Электронный фонд нормативно-технической и нормативно-правовой информации. – АО «Кодекс», 2024. – URL: https://docs.cntd.ru/document/1200105711
11. Дэвис Д., Дэниелс К. Философия DevOps. Искусство управления IT. – СПб.: Питер, 2017. – 416 с.
12. Вехен Д.. Безопасный DevOps. Эффективная эксплуатация систем. – Санкт-Петербург : Питер, 2020. – 432 с.
13. ГОСТ Р 56939-2016. Защита информации. Разработка безопасного программного обеспечения : дата введения – 01.06.2017 / Федеральное агентство по техническому регулированию и метрологии.
14. Гришин М. И., Марков А. С., Цирлов В. Л. Практические аспекты реализации мер по разработке безопасного программного обеспечения // ИТ-Стандарт. – 2019. – №. 2. – С. 29-39.
15. Горбатов В. С., Мещеряков А. А. Курс тренинга по безопасной разработке программного обеспечения // Безопасность информационных технологий. –2017. – Т. 24., №. 2. – С. 35-41. DOI: http://dx.doi.org/10.26583/bit.2017.2.04.
16. Synthesis of secure software development controls / A. Barabanov [et al.] // SIN '15 Proceedings of the 8th International Conference on Security of Information and Networks. – Sochi : Association for Computing Machinery, 2015. – С. 93–97. – DOI: https://doi.org/10.1145/2799979.2799998
17. Мельникова А. Е., Рычков В. А. Использование технологии контейнеризации при безопасной разработке программного обеспечения //Материалы Второго Международного научно-практического форума по экономической безопасности «VII ВСКЭБ». – 2021. – С. 75-83.

18. OWASP Secure Coding Practices - Quick Reference Guide. – OWASP Foundation, Inc, 2024. – URL: https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/stable-en/02-checklist/05-checklist (дата обращения: 20.09.2024).
19. Josang A.,Odegaard M, Oftedal E. Cybersecurity Through Secure Software Development // 9th IFIP WG 11.8 World Conference. – Springer, 2015. – No 453. – Pp. 53-63. – URL: https://dblp.uni-trier.de/db/conf/ifip11-8/ifip11-8-2015.html (дата обращения: 10.08.2024).
20. Microsoft Security Development Lifecycle. – URL: https://www.microsoft.com/en-us/sdl/ (дата обращения: 15.02.2024).
21. Cisco Secure Development Lifecycle. – Cisco and/or its affiliates, 2021. – URL: https://www.thestack.technology/content/files/c/dam/en_us/about/doing_business/trust-center/docs/cisco-secure-development-lifecycle.pdf (дата обращения: 15.09.2023).
22. Software Assurance Maturity Model. OWASP SAMM. – URL: https://owaspsamm.org/model/ (дата обращения: 15.08.2024).
23. CLASP Security Principles. – URL: https://www.owasp.org/index.php/CLASP_Security_Principles (дата обращения: 15.02.2017).
24. BSIMM: с чего начинается AppSec в компании : [блог компании Positive Technologies] / Positive Technologies // Хабр : [сайт]. – Habr, 2006–2024. – Дата публикации: 08.04.2024. – URL: https://habr.com/ru/companies/pt/articles/805395/.
25. ZAP 2.15 Getting Started Guide // ZAP : Zed Attack Proxy. – ZAP Dev Team, 2024. – URL: https://www.zaproxy.org/pdf/ZAPGettingStartedGuide-2.15.pdf (дата обращения: 20.03.2024).