УДК 371.3:519.87

ПРОЕКТИРОВАНИЕ И ИССЛЕДОВАНИЕ МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ КАК МЕТОДИЧЕСКОЕ СРЕДСТВО ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

канд. техн. наук, доц. И. Б. БУРАЧЕНОК, канд. пед. наук, доц. В. С. ВАКУЛЬЧИК, канд. пед. наук, доц. А. П. МАТЕЛЕНОК
(Полоцкий государственный университет, Беларусь)

Аннотация. *Проблема обеспечения информационной безопасности является одной из самых актуальных задач современности. Качественное ее решение авторы статьи видят в практико-ориентированной подготовки студентов, будущих специалистов по кибербезопасности, и их серьезной подготовки по фундаментальным дисциплинам, в частности по высшей математике. Уверенное владение циклом математических дисциплин поможет им в дальнейшем создавать математические модели угроз информационной безопасности, что поможет в исследованиях и разработке алгоритмов по обнаружению и их ликвидации.*

Ключевые слова: *математические модели, информационная безопасность, прикладная направленность дисциплин.*

Несомненно, что сегодня, когда происходит стремительное развитие и повсеместное внедрение новейших информационно-коммуникационных технологий практически во все сферы человеческой жизни, проблема обеспечения информационной безопасности является актуальной задачей. О значимости и актуальности указанной проблемы, свидетельствуют проводимые исследования ведущих отечественных и зарубежных ученых в этой области, таких как Е.Б. Белов, В.П. Лось [1], А.А. Хорев [2], Д. П. Зегжда [3], Д.С. Лавров [3], В.Л. Цирлов[4] и др.

В результате ежегодного анализа Всемирного экономического форума основных рисков, с которыми сталкивается мир с точки зрения вероятности и воздействия по результатам на начало сентября 2021 года киберугрозы вошли в десятку наиболее опасных [5].

При этом необходимо отметить, что методологическая база теории проектирования и исследования математических моделей по информационной безопасности, как нового научного направления, в настоящее время находится в стадии формирования. Отдельной задачей становится противодействие информационным вмешательствам в деятельность страны (бизнеса). Поэтому научные исследования должны быть не только научно-теоретическими, но и постоянно совершенствоваться на практике. Анализ диссертационных исследований и научных статей показал, что значительное внимание в работах уделяется разработке формальных

моделей разграничения доступа, защищённых операционных систем и криптографической защиты информации. В то же самое время, вопросы, касающиеся разработки математических моделей информационных атак, процесса их обнаружения и оценки риска, пока не находят должного внимания. Возможную причину мы видим в недостаточной математической подготовке специалиста.

В нашем исследовании будем исходить из определения, что математическая модель в информационной безопасности – это описание сценариев в виде последовательности действий нарушителей и соответствующих ответных мер. Приближения таких моделей описывают процессы взаимодействия нарушителя с системой защиты и возможные результаты действий [6].

Специалист по информационной безопасности – это, прежде всего, высококвалифицированный специалист, обладающий разносторонними знаниями в области информационных технологий, владеющий не только языками программирования, но и сочетающий в себе навыки администрирования компьютерных сетей, умеющий настраивать групповые политики, настраивать системы защиты, разрабатывать сложные конфигурации межсетевых экранов и пр. У него должен быть солидный опыт практической работы с различными информационными технологиями. Все это требует не только практико-ориентированной подготовки, но серьезной подготовки по фундаментальным дисциплинам, в частности по высшей математике. Хорошее владение циклом математических дисциплин поможет специалистам в области информационной безопасности в дальнейшем создавать математические модели угроз информационной безопасности, что поможет в исследованиях и разработке алгоритмов по обнаружению и ликвидации их. Кроме того, модели могут использоваться для проведения мониторинга и аудита безопасности на этапах эксплуатации и сопровождения систем. Основу моделей обеспечения безопасности информации составляют следующие теории:

- формально-эвристический подход;
- теория вероятностей и случайных процессов;
- эволюционное моделирование;
- теория графов, автоматов и сетей Петри;
- теории игр и конфликтов;
- теория катастроф;
- теория нечетких множеств;
- энтропийный подход;
- модель Кларка-Вилсона;
- модель Белла-ЛаПадулы;
- модель Биба и другие.

Отличия большинства моделей заключаются в том, какие параметры они используют в качестве входных, а какие представляют в виде выходных после

проведения расчетов. Кроме того, в последнее время широкое распространение получают методы моделирования, основанные на неформальной теории систем: методы структурирования, методы оценивания и методы поиска оптимальных решений [7].

В Полоцком государственном университете на кафедре математики и компьютерной безопасности для обучения студентов специальности 1-98 01 01-01 компьютерная безопасность (математические методы и программные системы) на лекционных занятиях преподаватели (при преподавании математических дисциплин: теория вероятностей, дискретная математика, методы численного анализа) в качестве пропедевтической подготовки включают задачи, содержащие межпредметные связи с дисциплинами общепрофессионального и специального цикла. Приведем некоторые задачи указанного характера: 1) «создайте двоичный код Хаффмана для дискретного источника трех независимых символов A, B, C с вероятностями 0,95; 0,01; 0,11 и определите среднюю длину этого кода»; 2) «минимальное расстояние для линейного блочного кода равно 11, найдите максимальные возможности кода при исправлении ошибок, максимальные возможности при обнаружении ошибок и максимальные возможности этого кода при коррекции стираний для данной длины блока».

Другими словами, в цикл дисциплин высшей математики излагается с учетом принципа прикладной направленности. Систематическое использование различных криптографических понятий, решение различных задач по моделированию систем управления доступом, формальных моделей целостности и пр. позволяет студентам в ходе выполнения заданий не только приобрести опыт по планированию, прогнозированию, построению аналитических моделей, но опыт исследовательской работы и обработки результатов экспериментов. Применение указанных задач формирует у студентов положительное отношение к циклу дисциплин высшей математики и позволяет им достичь более высоких результатов не только при изучении специальных дисциплин, но и в процессе разработки и исследования математических моделей защиты информации.

Таким образом, при подготовке высококвалифицированного, конкурентноспособного на современном рынке труда специалиста в области информационной безопасности необходима фундаментальная подготовка по дисциплинам высшей математики с обязательным профессионально ориентированным решением задач. Это служит для поддержания мотивации студентов, а в дальнейшем успешному использованию полученного опыта при разработке и исследовании математических моделей. Анализ научно-методических исследований и педагогическая практика показали, что необходим спецкурс по изучению и преподаванию математических моделей, имеющихся в диссертационных исследованиях и научных работах по тематике информационной безопасности. Это позволит

повысить интерес студентов к общепрофессиональным и специальным дисциплинам и положительно повлияет на формирование профессиональной компетентности будущего специалиста указанного профиля.

ЛИТЕРАТУРА

1. Белов, Е. Б. О разработке профессиональных стандартов в области информационной безопасности / Е. Б. Белов, В. П. Лось // Доклады ТУСУР. – 2014. – № 2(32). – С. 327–331.
2. Хорев, А. А. Исследование возможности перехвата текстовых изображений, выводимых на экран монитора / Хорев А. А., Феизов С. А. // Состояние и перспективы развития современной науки по направлению «Информационная безопасность» : сб. ст. II Всерос. науч.-техн. конф. / Федеральное государственное автономное учреждение «Военный инновационный технополис «ЭРА»». – Анапа, 2020. – С. 55–67.
3. Лавров, Д. С. Моделирование сетевой инфраструктуры сложных объектов для решения задачи противодействия кибератакам / Лавров Д. С., Зегжда Д. П. Зайцева Е. А. // Вопросы кибербезопасности. – 2019. – № 2(30). – С. 13–20.
4. Цирлов, В.Л. Основы информационной безопасности автоматизированных систем [Электронный ресурс]. – 2008. – Режим доступа: https://ru.bmstu.wiki/%D0%A6%D0%B8%D1%80%D0%BB%D0%BE%D0%B2,_%D0%92%D0%B0%D0%BB%D0%B5%D0%BD%D1%82%D0%B8%D0%BD_%D0%9B%D0%B5%D0%BE%D0%BD%D0%B8%D0%B4%D0%BE%D0%B2%D0%B8%D1%87. – Дата доступа: 9.09.2021.
5. 2021 Global Risks Outlook [Электронный ресурс]. – 2021. – Режим доступа: https://www.visualcapitalist.com/visualized-a-global-risk-assessment-of-2021-and-beyond. – Дата доступа: 09.09.2021.
6. Щеглов, А. Ю. Математические модели и методы формального проектирования системы защиты информационных систем : учеб. пособие. / Щеглов А. Ю., Щеглов К. А. // СПб. : Университет ИТМО. – 2015.
7. Курилов, Ф. М. Моделирование систем защиты информации. Приложение теории графов / Ф. М. Курилов. – Текст : непосредственный // Технические науки: теория и практика : материалы III Междунар. науч. конф. (г. Чита, апрель 2016 г.). – Чита : Издательство Молодой ученый, 2016. – С. 6–9. – URL: https://moluch.ru/conf/tech/archive/165/9766/. – Дата доступа: 10.09.2021.