2. Вендеров, А.М. Проектирование программного обеспечения экономических информационных систем [Текст] : учебник / А.М. Вендеров – М.: Финансы и статистика, 2000. – 262 с.

3. В поисках идеальной CAPTCHA [Электронный ресурс] : статья / www.captcha.ru.

А.М. Геращенко

ОСУЩЕСТВЛЕНИЕ ПОДГОТОВКИ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ПОМОЩЬЮ АНГЛОЯЗЫЧНЫХ ОНЛАЙН-КУРСОВ

(Кубанский государственный технологический университет)

В связи со значительной и растущей ролью информационных технологий, особую значимость приобретает укрепление информационной безопасности. По этой причине существует необходимость как постоянного совершенствования подготовки профессионалов в данном направлении, так и повышения осведомленности в этой связи «среднестатистического обывателя», чья деятельность требует использования компьютерных и сетевых технологий. В силу быстрого и непрерывного технического развития рассматриваемой области, связанные с нею знания, умения и навыки нуждаются в постоянном совершенствовании и обновлении. При этом обеспечение информационной безопасности относится к числу тех сфер деятельности, где учеба на собственных ошибках, несмотря на свою значительную роль, представляется гораздо менее предпочтительной, нежели заблаговременная информированность о возможных угрозах. Соответственно, лица, задействованные в обеспечении информационной безопасности, нуждаются в своевременной подготовке к предупреждению и решению возможных проблем в этой связи.

При этом, для расширения профессионального кругозора, целесообразно обращаться как к отечественным достижениям, так и к опыту зарубежных стран – прежде всего тех, которые внесли наиболее весомый вклад в развитие информационных технологий. Дополнительную актуальность такой целесообразности способны придать также проблемы межгосударственных отношений, в результате которых осведомленность о положении вещей в сфере информационной безопасности соответствующих государств может принять характер знания сильных и слабых сторон вероятных противников.

Среди зарубежных стран, имеющих ценный опыт деятельности в плане разработки компьютерных систем и обеспечения информационной безопасности, важнейшее место занимают Великобритания и США. С целью знакомства с таким опытом, для специалиста в данной сфере было бы полезным прохождение соответствующих курсов в указанных странах. Этому способствует наличие значительного числа различных курсов по информационной безопасности (кибербезопасности), предлагаемых британскими и американскими учебными заведениями. Поскольку среднестатистический учащийся или работающий россиянин по различным причинам не может позволить себе полноценное очное

обучение (например, на степень бакалавра или магистра) в учебных заведениях Великобритании и США, особый интерес представляют такие из предлагаемых ими образовательных услуг, к которым можно прибегнуть без ущерба для трудовой или учебной деятельности в отечественном учреждении.

Это могут быть краткосрочные интенсивные курсы – такие, например, как «Cyber Insecurity – Hack the System», предлагаемый в рамках Международной летней школы британского Борнмутского университета. Слушатели указанного курса делятся на две группы, одна из которых в течение первой недели учится создавать и применять вредоносное программное обеспечение для проникновения в компьютерные системы, а другая в то же время учится анализировать, предотвращать и отражать кибератаки, после чего группы меняются ролями и готовятся к финальной учебной «кибервойне» [1].

Однако в ряде случаев возможность прохождения даже краткосрочного очного обучения в зарубежных учебных заведениях вообще отсутствует или представляется чрезвычайно затруднительной. Это может быть обусловлено, в частности, запретом на выезд за границу, проблемами при получении визы или же необходимостью экономии времени и финансовых средств. В таком случае выходом из сложившейся ситуации могут быть онлайн-курсы – дистанционные курсы, обучение на которых осуществляется через Интернет. Например, Вашингтонский университет США предлагает таким образом пройти на платной основе курсы на сертификаты по информационной безопасности и управлению рисками («Information Security & Risk Management» [2]) и безопасности информационных систем («Information Systems Security» [3]). Существует и возможность получения по итогам онлайн-обучения академических степеней – допустим, степени бакалавра наук (Bachelor of Science) по информационным системам и кибербезопасности (Information Systems and Cybersecurity), предлагаемой, в частности, американским Техническим институтом ИТТ [4] – разумеется, на возмездной основе.

Если же подобные вышеуказанным платные дистанционные курсы представляются неоправданно затратными в финансовом плане, существует значительное число возможностей пройти бесплатные «массовые открытые онлайн-курсы» (Massive Open Online Courses, сокращенно MOOC). Одной из популярных платформ по предоставлению таких курсов такого рода является «Coursera» [5] – проект, основателями которого являются профессора Стэнфордского университета Э. Нг и Д. Келлер. Данный ресурс содержит сотни бесплатных курсов, содержащих видеолекции и презентации для просмотра, тексты для чтения, задания для промежуточного и итогового контроля, имеющие вид тестов (проверяемых автоматически) и/или творческих работ (проверяемых другими слушателями соответствующих курсов), а также форумы для общения между преподавателями и слушателями курсов. Для получения возможности прохождения курсов необходима регистрация, требующая указания имени и электронного адреса пользователя. В большинстве случаев после успешного прохождения курсов «Coursera» (для чего необходимо своевременное выполнение контрольных заданий на определенном уровне) слушатель получа-

ет возможность загрузить подтверждающий данный факт документ – «Statement of Accomplishment» (бесплатно) или, если конкретный курс имеет такую возможность, – «Verified Certificate» (доступный за сравнительно небольшую плату при условии предоставления фотографий слушателя и его удостоверения личности посредством веб-камеры и позиционирующийся как более весомое доказательство учебных достижений). Таким образом, пользователи могут не просто пройти обучение на бесплатной основе, но и документально подтвердить его факт (а владельцы ресурса имеют возможность сбора колоссального объема персональных данных – как минимум, электронных адресов, а в ряде случаев – и основных сведений из удостоверений личности).

К числу размещенных на платформе «Coursera» онлайн-курсов, с помощью которых можно осуществлять подготовку по информационной безопасности, относятся, например, предлагаемый Мичиганским университетом курс по истории, технологии и безопасности Интернета («Internet History, Technology and Security» [6]), предоставленный Лондонским университетом курс по вредоносному программному обеспечению и связанной с ним подпольной экономике («Malicious Software and its Underground Economy: Two Sides to Every Story» [7]), а также курсы от уже упомянутого Вашингтонского университета, посвященные различным аспектам информационной безопасности (и, видимо в связи с необходимостью продвижения аналогичных платных курсов, не предоставляющих возможности получения каких-либо документов о своем прохождении): «Information Security and Risk Management in Context» [8], «Building an Information Risk Management Toolkit» [9] и «Designing and Executing Information Security Strategies» [10].

Рассмотрим более подробно последний из перечисленных онлайн-курсов – рассчитанный на 10 недель при недельной учебной нагрузке от 4 до 6 часов курс по разработке и осуществлению стратегий информационной безопасности, который ведет главный инженер (Chief Technical Officer), эксперт по компьютерной безопасности М. Саймон. Данный курс отличается практической направленностью. В видеолекциях (сопровождаемых слайдами с основными вопросами и фактами) даются, в частности, описание структур компании, связанных с обеспечением информационной безопасности (в том числе характеристика должностных обязанностей конкретных функционеров), и детальное рассмотрение конкретных происшествий в сфере кибербезопасности с анализом различных подходов к их устранению. Слушателям курсов предлагается, следуя данным инструкциям и рекомендациям, выполнить три творческих задания – например, осуществить анализ рисков и выработать рекомендации применительно к предоставлению доступа к конфиденциальной информации для сотрудников недавно присоединенного к компании подразделения. Эти задания имеют вид письменных работ, которые должны быть к назначенному сроку поданы на рассмотрение на специальной странице онлайн-курса с тем, чтобы быть автоматически (без указания авторства) отправленными на проверку другим участникам курса. В свою очередь, слушатель, пославший свой труд на суд своих соучеников, должен прочесть и оценить ряд их работ, а затем, по истече-

нии недели, получает отзывы на свое сочинение. Таким образом, осуществляется знакомство с другими точками зрения на проблему. Для проверки знания терминов и прочих теоретических положений предлагаются тесты, которые проверяются автоматически, допускают ограниченное число попыток их выполнения и должны быть выполнены к определенному сроку (применительно к данному курсу – к дате его окончания). Доступ к материалам курса (копирование которых допускается для личного использования в учебных целях) сохраняется некоторое время после его окончания.

Если для сотрудников, занимающихся обеспечением информационной безопасности, равно как и для студентов, обучающихся в данном направлении, будут полезны содержащиеся в соответствующих курсах практические и теоретические данные (факты и рекомендации), то для преподавателей, осуществляющих преподавание дисциплин, связанных с информационной безопасностью, может представлять интерес также сам характер подачи учебного материала: тематическая структура курса, иллюстративный материал, типы тренировочных заданий, виды и формы контроля. Кроме того, стоит иметь в виду возможность использования указанных курсов для дополнительной подготовки студентов.

В заключение стоит подчеркнуть тот факт, что вышеописанные курсы представлены на английском языке, в связи с чем следует особо отметить важность подготовки по данному языку, в том числе, и для специалистов по информационной безопасности.

Литература

1. Cyber Insecurity – Hack the System [Электронный ресурс]. – Режим доступа:http://microsites.bournemouth.ac.uk/international-summer-school/courses/dec/cyber-insecurity-hack-the-system/

2. Certificate in Information Security & Risk Management [Электронный ресурс]. – Режим доступа:http://www.pce.uw.edu/certificates/information-security-risk-management.html

3. Certificate in Information Systems Security [Электронный ресурс]. – Режим доступа:http://www.pce.uw.edu/certificates/information-systems-security.html

4. Information Systems and Cybersecurity (Online Program): Bachelor of Science Degree [Электронный ресурс]. – Режим доступа: http://www.itt-tech.edu/campus/courses.cfm?prog_id=4124

5. Coursera [Электронный ресурс]. – Режим доступа:https://www.coursera.org/

6. Internet History, Technology and Security [Электронный ресурс]. – Режим доступа: https://www.coursera.org/course/insidetheinternet

7. Malicious Software and its Underground Economy: Two Sides to Every Story [Электронный ресурс]. – Режим доступа: https://www.coursera.org/course/malsoftware

8. Information Security and Risk Management in Context [Электронный ресурс]. – Режим доступа: https://www.coursera.org/course/inforiskman

9. Building an Information Risk Management Toolkit [Электронный ресурс]. – Режим доступа: https://www.coursera.org/course/inforisk

10. Designing and Executing Information Security Strategies [Электронный ресурс]. – Режим доступа: https://www.coursera.org/course/infosec

С.П. Горелик, В.С. Шумилин

ЗАЩИТА СЕТЕЙ СВЯЗИ В УСЛОВИЯХ ПРОГРАММНЫХ ВОЗДЕЙСТВИЙ

(Академия ФСО России, г. Орел)

С развитием информационных и телекоммуникационных технологий, становится актуальным процесс развития сетей связи, путем цифровизации и интеграции их в общемировое телекоммуникационное пространство, что в свою очередь, существенно увеличивает возможности нарушителей по идентификации, вскрытию и воздействию на их элементы.

Анализ элементов сети связи осуществляется нарушителем посредством ведения несанкционированного мониторинга (рисунок 1).

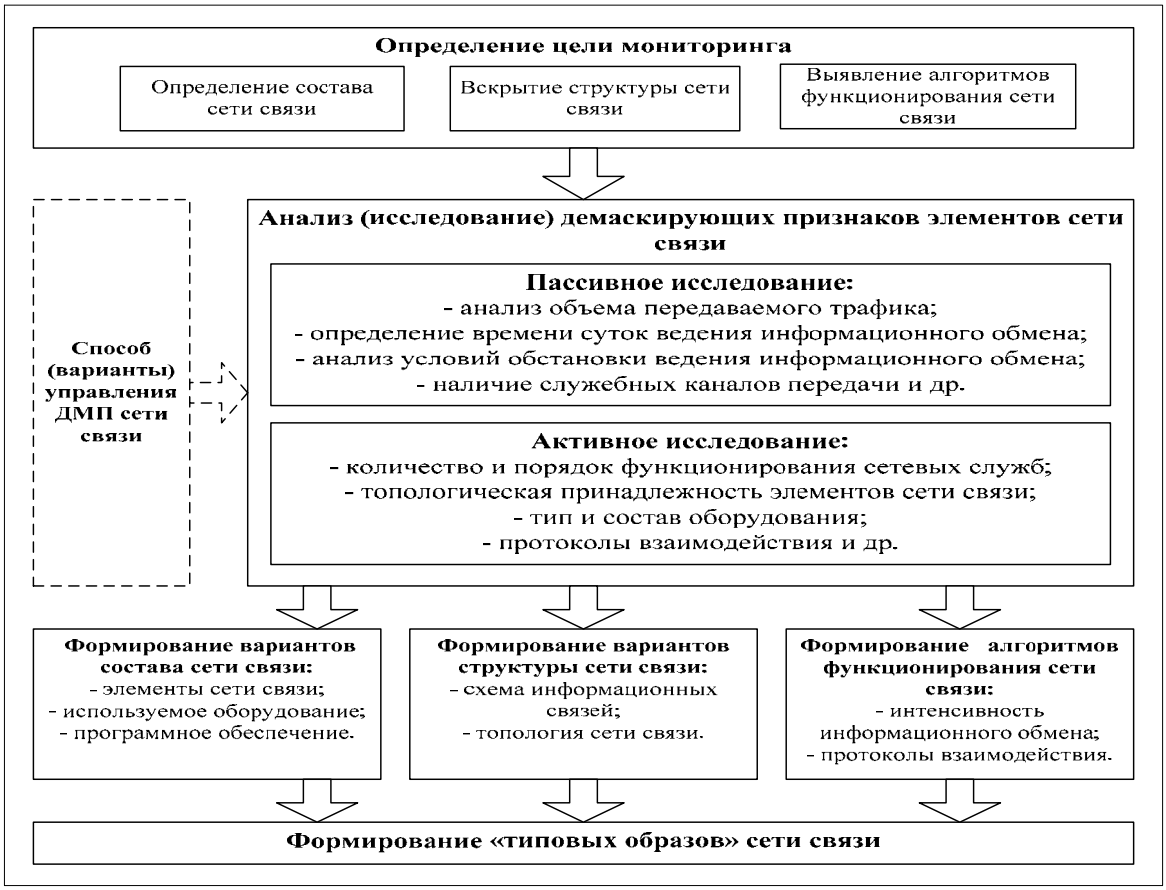

Рис. 1. Обобщенный порядок проведения несанкционированного мониторинга элементов сети связи (вариант)