Грейс Митчелл, стажер ПИР-Центра

В центре сюжета не технологии, а драматическая история. Однако именно технологические детали в этой книге представляют интерес — когда они наконец раскрываются, выясняется, что они весьма актуальны и в реальности.

Рецензия на книгу «Флорентийский обман» (The Florentine Deception. Carey Nachenberg. Open Road Distribution, 2015. 334 p.)

«Флорентийский обман» - первый авторский опыт ИТ-специалиста и вице-президента компании Symantec Кэри Наченберга (Carey Nachenberg), он уже удостоился похвалы среди экспертов по кибербезопасности, хотя ее вряд ли можно отнести к специализированной технической литературе В принципе, это обыкновенный детектив, в котором компьютеры и интернет играют важную роль. Но у него есть одна особенность: сам автор - эксперт по безопасности в киберпространстве, и все, что происходит в его книге, - воображаемые события, основанные на реальных технических возможностях.

В начале истории, молодой программист Алекс Файф (Alex Fife) “чистит” компьютер недавно умершего профессора, чтобы дать его новому пользователю. Но в этом процессе Алекс узнаёт, что у этого профессора была другая, более опасная профессия, и что где-то в его богатом доме есть сокровище, которое ищут агенты не одного государства. Чтобы достать это сокровище, Алекс и его друзья ищут тайные комнаты в особняке профессора, занимаются спелеологией, крадутся в морг за трупом, и участвуют в многих других приключениях. Ситуация настолько осложняется, что Алекс жалеет о своем решении расследовать эту загадку, но в конце концов, именно его технические знания предотвращают мировую катастрофу.

Как детектив, книга прекрасно выполняет свою задачу — она насколько захватывает читателя, что от сюжета сложно оторваться. Персонажи очень

реалистичны, а сюжет грамотно выстроен. Нет ни одной детали, которая не понравилась бы Чехову (ведь, по его словам, «если в первом акте на стене висит ружье, то в последнем оно обязательно выстрелит»). Все персонажи и предметы, которые появляются в первых главах, вновь возвращаются в сюжет в последних. И они удивительным образом оказываются очень важными: например, старый преподаватель главного героя помогает ему благодаря не только техническому знанию, но и своей национальности. К тому же, «флорентийское сокровище» и намерения персонажей остаются тайной достаточно долго, чтобы читатель поразмыслил над загадками и возможными вариантами ответов на них.

Всё в самом деле очень реалистично: приложения, кибератаки и уязвимости, описанные в книге, являются вполне вероятными, и принципы их действия изложены ясно и доступно даже для неспециалистов в области компьютерной науки. То есть, эта книга может быть интересна и для экспертов по ИТ, и для людей без опыта в этой сфере.

Действительно, в центре сюжета не технологии, а драматическая история. Однако именно технологические детали в этой книге представляют интерес — когда они наконец раскрываются, выясняется, что они весьма актуальны и в реальности. Уязвимость, от которой возникает главная проблема в сюжете, появилась тогда, когда только закладывались принципы работы интернета и компьютерных сетей, и нынешних возможностей у киберпреступников еще не было. Сети в то время были еще небольшими, и самая важная информация в них не хранилась. Теперь же много критических данных и систем управления находятся в сетях: государственная информация, секретные документы, финансовые инструменты компаний, управление электростанциями, сотовой связью и т.п. Слабое место, показанное в этой книге, подчеркивает риски широкого проникновения интернета и его воздействия на все подключенные компьютеры, в том числе, те, в которых хранятся государственные базы данных, и те, которые входят в системы управления объектами критически важных предприятий, а также и обычные ПК. Вся эта инфраструктура попадает под угрозу хакеров в книге Наченберга.

Уязвимость в базовом программном обеспечении, подобная описанной в книге, может грозить целым странам прекращением работы телекоммуникаций, транспорта и больниц, ограничением всех государственных, деловых и военных действий, потерей управления на заводах и электростанциях. И эта уязвимость, как подтверждает ИТ эксперт Юджин Спаффорд в введении книги Наченберга, вполне реальная. Не вдаваясь в детали, можно сказать, что в итоге она окажется удивительно простой, даже очевидной. А пользователи интернета живут с такими «дырами» в «щитах» своей защиты, потому что не понимают структуру интернета и возможную опасность. Страшно читать книгу и понимать, что это все реалистично, и такой сценарий может происходить на самом деле. Но можно надеяться, что мировые ИТ-специалисты заинтересовались описанной в книге ситуацией и стали решать данную проблему.

Враги главных героев этой повести правдоподобны – российские хакеры достаточно активны в Америке, даже если и не так же, как китайские. В целом, при чтении «Флорентинского Обмана» становится ясно, что какой-нибудь

группе хакеров довольно легко совершить киберпреступление, которое повредит или даже уничтожит сотни тысяч компьютеров. Таких групп много в современном мире, и их число постоянно растет — ведь в них включаются и государственные агенты, и террористические группировки, и анонимные анархисты, и многие другие.

Российским читателям стоит иметь ввиду, что поскольку автор произведения - американец, русские персонажи в книге полностью основаны на стереотипах: они пьют водку, ругаются матом, независимо от того, являются ли они положительными героями или нет. Не стоит обижаться – это просто «классика жанра»!

Эта книга – увлекательное чтение для любителей детективных историй на основе современных технологий, а специалистов не будет раздражать дилетантский подход к техническим деталям. Более того, автор ставит важную проблему в сфере современных ИКТ, которая должна дать пищу для дальнейших размышлений.