Инженерный вестник Дона, №1 (2019)
ivdon.ru/ru/magazine/archive/n1y2019/5596

Требования к разработке автоматизированной обучающей системы в области информационной безопасности

Д.С. Колесникова, А.К. Рудниченко

Дальневосточный федеральный университет, Владивосток

Аннотация: В данной работе рассматривается вопрос улучшения качества подготовки специалистов в области информационной безопасности путем использования в обучении специализированной обучающей системы. Приведен обзор существующих аналогов. Приведены основные аспекты разработки автоматизированной обучающей системы.
Ключевые слова: обучающая система, автоматизированная обучающая система, информационная безопасность, защита информации, тренажёр, обучение, разработка, программирование.

В настоящее время наблюдается стремительный рост объема информации в мире. По прогнозам аналитиков, общий объем данных в мире к концу 2018 года должен был приблизиться к 33 зеттабайт (эквивалентно 33 триллионам гигабайт), а к 2025 году увеличится до 175 зеттабайт [1]. Можно смело утверждать, что начало третьего тысячелетия ознаменовало вступление человечества в эпоху главенства информации.

Несмотря на активное развитие идеи свободного доступа к информации, не все данные должны быть открытыми. Существует большое число видов тайн и их классификаций, но всех их объединяет одно: наряду с ростом объема данных увеличивается и число утечек ценной информации, а также способов атак на нее. В таких условиях возникает необходимость наличия на различных предприятиях (будь то государственное учреждение или частная организация) сотрудников, способных грамотно организовать мероприятия по обеспечению информационной безопасности, исключающие несанкционированный доступ к защищаемой информации.

Особенно остро стоит проблема подготовки будущих квалифицированных специалистов в данной области, что объясняется следующими причинами:

- использование устаревших методик преподавания, в то время как защита информации является активно развивающейся областью знаний;
- информационные технологии, даже при их наличии, применяются редко, либо не применяются вовсе;
- низкий уровень мотивации к обучению в данной области как у студентов, так и у преподавателей;
- отсутствие в профессорско-преподавательском составе университетов достаточного количества специалистов-практиков с опытом работы в данной области;
- отсутствие практического опыта у обучающихся для построения в будущем системы защиты информации в организации.

В качестве одного из способов решения перечисленных проблем предлагается использовать в обучении специализированную обучающую систему, особенности разработки которой представлены в данной статье. Подобная система в теории должна позволить обучающимся воссоздать реальную контролируемую ситуацию на вымышленном предприятии и дать возможность получения практических навыков по защите информации.

Понятие автоматизированной обучающей системы

Обучающая система обеспечивает обучение пользователя некоторой предметной области [2]. Главная задача обучающей системы – провести анализ знаний студента по определенному разделу предметной области, определить пробелы в знаниях и максимально ликвидировать их [3].

Автоматизированная обучающая система (АОС) – это комплекс программно-технических и учебно-методических средств, обеспечивающих активную учебную деятельность в некоторой предметной области с помощью графического материала [4]. Компьютерные обучающие системы могут быть представлены в виде компьютерных учебников, лабораторных

практикумов, тренажеров, систем контроля знаний и т. д. Каждое представление АОС в чистом виде имеет свои плюсы и минусы, поэтому в современных решениях применяется комбинирование представленных подвидов.

Основное средство взаимодействия обучаемого с автоматизированной обучающей системой – диалог [4]. Диалог обеспечивает возможность оперативной обратной связи с участником обучающего курса, создавая интерактивную среду и поддерживая интерес обучаемого. Одним из наиболее удачных примеров АОС можно считать тренажёры, так как они используют симуляционный подход к обучению. Обучение с помощью различных симуляторов является более эффективным за счёт моделирования приближенных к реальной жизни ситуаций.

Обзор существующих отечественных и зарубежных решений

В настоящее время существуют различные АОС, реализованные в виде тренажёров и направленные, прежде всего, на обучение навыкам взлома (для изучения деятельности злоумышленников), администрирования сетей, но вопросу организационной защиты и обеспечения информационной безопасности в целом на моделируемом объекте информатизации внимание практически не уделено. Далее приведен обзор наиболее интересных существующих игровых решений, которые также позволяют осваивать новые знания в области информационной безопасности.

Kaspersky Interactive Protection Simulation (KIPS) [5] – игровой тренинг, погружающий специалистов по IT-безопасности из коммерческих компаний и правительственных учреждений в симулированную бизнес-среду, в которой возникает серия неожиданных киберугроз. При этом участникам надо максимально повысить прибыль и сохранить репутацию. Игра проводится по всему миру. На октябрь 2018 года игра переведена на 11 языков. У игры есть несколько сценариев, например: для банка, крупной

корпорации, транспортного или нефтегазового предприятия, водяной станции и др. Кроме того, в феврале 2017 года вышел онлайн-тренинг KIPS Online [6] – пошаговая ролевая стратегия «Лаборатории Касперского» про информационную безопасность бизнеса. KIPS Online стала дополнением к настольной игре-симулятору KIPS Live, запущенной в 2015 году.

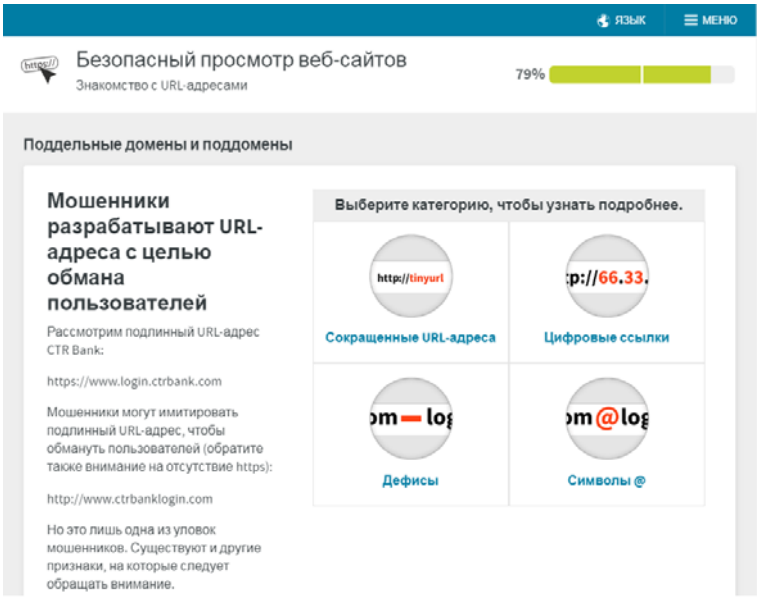

Рис. 1. – Скриншот из игры KIPS Online

Игра The Weakest Link [7], представленная в виде тестовых заданий на каждый из рабочих дней месяца, завоевала популярность среди аудитории благодаря наличию шуточной составляющей (в вариантах ответа).

Также, существует ряд игр в жанре choose-your-own adventure. Одна из них – Data Center Attack [8], в которой игрок выступает в роли начальника отдела информационной безопасности в медицинском учреждении. Игра представляет собой множество небольших видеороликов, в конце каждого из которых игроку предлагается выбрать один из вариантов решения текущей проблемы. От выбора игрока зависит дальнейшее развитие событий. Аналогом является игра Targeted Attack [9]

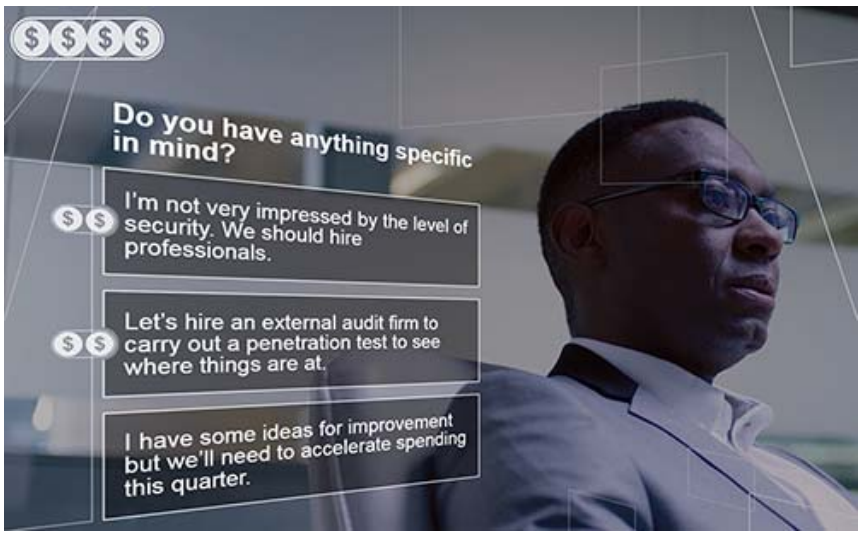

Рис. 2. – Скриншот из игры Data Center Attack

Uplink (Великобритания) [10]. Главный лозунг данной игры в переводе с английского: «Доверие – это слабость».

Рис. 3. – Обложка и скриншот из игры Uplink

Сюжет игры дает возможность принять на себя роль специального агента, который зарабатывает на жизнь, выполняя задания для крупных корпораций. Задачи игрока включают в себя взлом конкурирующих компьютерных систем, кражу исследовательских данных, саботаж других компаний, отмывание денег, стирание улик, а также фальсификацию данных.

Street Hacker (США) [11]. Игроку дается старый компьютер и начальный капитал в 1000 долларов для реализации попыток взлома. Также, как и Uplink, получила большую популярность у любителей игр для хакеров, так как основная ее цель как раз и состоит во взломе чужих компьютеров в соответствии с заданием миссии.

Рис. 4. – Скриншот из игры Street Hacker

На интернет-ресурсе «Хабр» одним из авторов статей, который является научным сотрудником кафедры защиты информации, была разработана игра на базе офисной программы Microsoft Excel (MS Excel) [12].

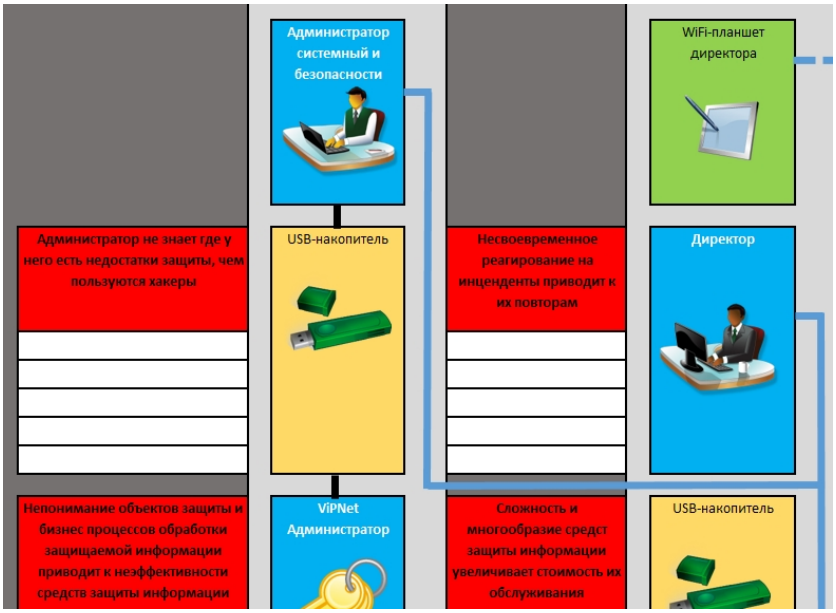

Рис. 5. – Скриншот игры в MS Excel по информационной безопасности

В качестве объекта в игре выступает информационная система небольшой организации (примерно 9 рабочих станций и 1 сервер с виртуальными машинами), исследуется моделирование угроз, а также построение и управление системой защиты информации в условиях финансовых ограничений.

Автор использовал данную игру в образовательном процессе среди своих студентов. По заверениям автора вовлеченность в игру была почти стопроцентная. Студенты и реально работающие специалисты играли с огромным интересом, подбирали стратегии, спорили, играли в команде, определялись лидеры. После большого количества игр у игроков возникает вопрос о выводе универсальной стратегии, гарантирующей выигрыш или желание «улучшить» игру. Этот момент является ключевым в переходе от игры к обучению профессиональным дисциплинам, которые позволяют решать ситуации, смоделированные игрой, наилучшим образом. Исходя из этого, в идею разрабатываемой обучаемой системы необходимо заложить аналогичный подход – привлечение обучающихся к знаниям теми средствами, которые имеются у нас в свободном доступе и которые были бы интересны самим студентам.

Основные требования к разработке автоматизированной обучающей системы

Информационная безопасность, как процесс, состоит в применении организационных (разработка внутренней нормативной документации) и технических (применение программных и аппаратных средств защиты) методов защиты информации. В связи с этим, при обучении в данной области теоретические знания не могут дать тех навыков, которые будут необходимы в «боевых» условиях на предприятии. Зачастую высшие учебные заведения не могут похвастаться хорошей базой практических занятий в области защиты информации. Для того, чтобы отточить навыки защиты объекта информатизации, необходимо иметь сам объект информатизации – организацию, требующую специалиста по информационной безопасности.

Целевая аудитория АОС в области информационной безопасности – не только студенты, но и профессорско-преподавательский состав, а также сотрудники организаций: администраторы безопасности, ответственные за

информационную безопасность, за реагирование на инциденты и другие. Задача разрабатываемого программного обеспечения в данном случае – освежить в памяти основы защиты объекта информатизации, а также улучшить практические навыки в данной области.

Автоматизированная обучающая система в области информационной безопасности должна отвечать следующим требованиям [13]:

- процесс обучения должен вызывать интерес у обучающихся и преподавателей (в том числе касаемо проработки визуальной составляющей игры);
- интерфейс АОС должен быть интуитивно понятен пользователю;
- АОС должна предусматривать возможность симуляции разных ролей для всестороннего изучения вопроса;
- информационная база обучающего процесса должна соответствовать актуальным нормативно-правовым документам, содержать сведения об используемых организациями сертифицированных средствах защиты информации, а также информацию об угрозах безопасности информации. Представленный перечень станет основой для моделирования ситуаций в игре;
- интерактивный процесс обучения должен быть максимально приближен к реальным обстоятельствам в организации.

В процессе разработки АОС необходимо сформировать группу респондентов из 8-10 человек (фокус-группа), которая поможет провести качественный анализ разрабатываемой обучающей системы (тестирование). В число респондентов должны входить:

- специалисты в области информационной безопасности с опытом работы в данной области (особое внимание будет приковано именно к этой группе людей, так как их отзывы и рекомендации помогут улучшить

содержательную часть программы, касающуюся вопросов информационной безопасности);

- студенты по направлению информационной безопасности (непосредственно обучающиеся по данному направлению смогут определить, насколько информативен симулятор);
- преподаватели дисциплин соответствующего направления (они могут выявить, подходит ли такой формат для обучения и охватывает ли он в полной мере все аспекты учебного материала по определенной теме);
- группа людей, не специализирующихся на вопросах защиты информации (для определения степени интуитивности интерфейса симулятора).

В результате тестирования программного продукта будут собраны отзывы пользователей, которые будут учтены при последующей доработке программы.

Таким образом, реализация данной автоматизированной обучающей системы позволит взглянуть на процесс обучения вопросам информационной безопасности с другой стороны, а также усовершенствовать уже имеющиеся навыки в данной области.

Литература

1. The Digitization of the World // Seagate - Storing the world's digital content | Seagate US. URL: seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf (date of access: 10.01.2018).
2. Гаскаров Д.В. Интеллектуальные информационные системы. - М.: Высшая школа, 2003. - 432 с.
3. Джексон П. Введение в экспертные системы. - 3-е изд. - М.: Издательский дом "Вильямс", 2001. - 624 с.

4. Терминологический словарь библиотекаря: педагогические термины и понятия. URL: nlr.ru/cat/edict/PDict (дата обращения: 11.01.2018).

5. Kaspersky Interactive Protection Simulation. URL: ics.kaspersky.ru/media/KL_SA_KIPS_overview_RU.pdf (date of access: 11.01.2018).

6. Kaspersky Security Awareness // Повышение осведомленности о кибербезопасности | Лаборатория Касперского. URL: kaspersky.ru/enterprise-security/security-awareness (date of access: 11.01.2018).

7. The Weakest Link: A User Security Game. URL: isdecisions.com/user-security-awareness-game (date of access: 11.01.2018).

8. Data Center Attack // Trend Micro the Game. URL: datacenterattacks.trendmicro.com (date of access: 12.01.2018).

9. Targeted Attack: The Game. URL: targetedattacks.trendmicro.com/cyoa/en (date of access: 12.01.2018).

10. Uplink. URL: introversion.co.uk/uplink (date of access: 15.01.2018).

11. Streethacker. URL: streethacker.com (date of access: 15.01.2018).

12. Проблемно-игровой метод мотивации студента специальности «Информационная безопасность» // Хабр. URL: habr.com/ru/post/286114/ (дата обращения: 16.01.2018).

13. Орлов С.А., Цилькер Б.Я. Технологии разработки программного обеспечения: Учебник для вузов. 4-е изд. Стандарт третьего поколения. СПб.: Питер, 2012. С. 539-542.

14. Верещагина Е.А., Колесникова Д.С., Рудниченко А.К., Особенности разработки информационной системы для предприятия // Инженерный вестник Дона, 2019, №1. URL: ivdon.ru/ru/magazine/archive/n1y2019/5533.

15. Юренко И.К., Фандеев Е.И., Нефедов В.В., Программно-технические и тренажеро-моделирующие комплексы для разработки,

испытаний, управления и обслуживания современных локомотивов // Инженерный вестник Дона. 2013. №3. URL: ivdon.ru/ru/magazine/archive/n3y2013/1826.

16. Тихонова О.Б., Русляков Д.В., Интерактивные обучающие программы в образовательном процессе по бытовой холодильной технике // Инженерный вестник Дона. 2014. №1. URL: ivdon.ru/ru/magazine/archive/n1y2014/2256.

References

1. Seagate - Storing the world's digital content. Seagate US. URL: seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf (date of access: 10.01.2018).

2. Gaskarov D.V. Intellektual'nye informatsionnye sistemy [Intelligent Information Systems]. M.: Vysshaya shkola, 2003. 432 p.

3. Dzhekson P. Vvedenie v ekspertnye sistemy [Introduction to expert systems]. 3-e izd. M.: Izdatel'skiy dom "Vil'yams", 2001. 624 p.

4. Terminologicheskiy slovar' bibliotekarya: pedagogicheskie terminy i ponyatiya [Librarian Terminology Dictionary]. URL: nlr.ru/cat/edict/PDict (date of access: 11.01.2018).

5. Kaspersky Interactive Protection Simulation. URL: ics.kaspersky.ru/media/KL_SA_KIPS_overview_RU.pdf (date of access: 11.01.2018).

6. Kaspersky Security Awareness. Kaspersky Lab. URL: kaspersky.ru/enterprise-security/security-awareness (date of access: 11.01.2018).

7. The Weakest Link: A User Security Game. URL: isdecisions.com/user-security-awareness-game (date of access: 11.01.2018).

8. Trend Micro the Game. URL: datacenterattacks.trendmicro.com (date of access: 12.01.2018).

9. Targeted Attack: The Game. URL: targetedattacks.trendmicro.com/cyoa/en (date of access: 12.01.2018).

10. Uplink. URL: introversion.co.uk/uplink (date of access: 15.01.2018).

11. Streethacker. URL: streethacker.com (date of access: 15.01.2018).

12. Problemno-igrovoy metod motivatsii studenta spetsial'nosti «Informatsionnaya bezopasnost'» [Problem-game method of motivating a student of the specialty "Information Security"]. Habr. URL: habr.com/ru/post/286114/ (date of access: 16.01.2018).

13. Orlov S.A., Tsil'ker B.Ya. Tekhnologii razrabotki programmnogo obespecheniya [Software Development Technologies]: Uchebnik dlya vuzov. 4-e izd. Standart tret'ego pokoleniya. SPb.: Piter, 2012. pp. 539-542.

14. Vereshchagina E.A., Kolesnikova D.S., Rudnichenko A.K. Inženernyj vestnik Dona (Rus), 2019, №1. URL: ivdon.ru/ru/magazine/archive/n1y2019/5533.

15. Yurenko I.K., Fandeev E.I., Nefedov V.V. Inženernyj vestnik Dona (Rus), 2013, №3. URL: ivdon.ru/ru/magazine/archive/n3y2013/1826.

16. Tikhonova O.B., Ruslyakov D.V. Inženernyj vestnik Dona (Rus), 2014, №1. URL: ivdon.ru/ru/magazine/archive/n1y2014/2256.