Инженерный вестник Дона, №12 (2023)
ivdon.ru/ru/magazine/archive/n12y2023/8864

Использование виртуализации на ПК СВ «Брест» для обучения методам информационной безопасности

Г. В. Терещенко, Ю. А. Новикова

Санкт-Петербургский государственный университет аэрокосмического приборостроения

Аннотация: В сфере информационной безопасности (ИБ) технология виртуального моделирования применяется во многих областях, ее ценность доказана и привлекает внимание множества специалистов данной области. Виртуальное моделирование широко внедряется в информационные системы (ИС) и играет важную роль в исследованиях ИБ платформ больших данных. Целью данной работы является изучение и решение проблемы отсутствия экспериментальной среды для технологий ИБ в университетах и колледжах. После понимания основных моментов был проведен исследовательский проект обучения с широким использованием виртуальных моделей ИС. В результате эмпирического анализа, авторы пришли к выводу, что платформа для моделирования виртуального эксперимента может решить проблему формирования профессиональных компетенций у студентов в области ИБ, повысить интерес студентов к технологиям ИБ и достичь образовательной цели - развития независимого инновационного духа и практических навыков у студентов. Для реализации тестовой системы использованы программные комплексы средств виртуализации «БРЕСТ», установленные на физические сервера с операционной системой Astra Linux SE.

Ключевые слова: информационная безопасность, виртуализация, программный комплекс средств виртуализации «БРЕСТ», операционная система Astra Linux SE, обучение специалистов информационной безопасности.

Введение

В последние годы информационная безопасность (ИБ) стала очень важна как для государственных организаций, так и для частных компаний, и рыночный спрос на талантливых специалистов в области управления и внедрения ИБ также растет [1]. Но сейчас хороших специалистов в области ИБ по-прежнему не хватает. Согласно современному развитию информационных технологий, потребность общества в профессионалах в области информационной безопасности составляет около семи тысяч в год. Только на сайте hh.ru опубликовано более трех тысяч вакансий для специалистов в области ИБ. Чтобы решить эту проблему, требуется ускорить подготовку квалифицированных специалистов в области ИБ. Однако, поскольку обучение специалистов в области ИБ в РФ появилось лишь

недавно, подготовка специалистов еще не достигла необходимого уровня качества. В настоящее время практическое обучение ИБ, основанное на виртуальном моделировании, может как раз решить эту задачу. Данный вид обучения позволяет студентам использовать и настраивать реальное программное обеспечение для шифрования, моделировать различные виды сетевых атак, изучать работу сетевых экранов и систем обнаружения вторжений.

Использование виртуального моделирования позволяет наглядно имитировать реальное поведение информационных систем (ИС). Виртуальная среда обучения позволяет учащимся получать интуитивно понятные знания и улучшить свое понимание абстрактных принципы ИБ.

Аспекты ИБ, рассмотренные в образовательном проекте.

В нашем образовательном проекте мы заложили следующую концепцию. ИБ означает, что аппаратное и программное обеспечение информационной сети и данные в системе защищены от случайных или злонамеренных угроз, от повреждения, изменения или утечки, система работает непрерывно, надежно и нормально, а ИС выполняют свои функции бесперебойно [2]. ИБ в основном включает в себя следующие пять аспектов, а именно: конфиденциальность, подлинность, целостность, отсутствие утечек информации и безопасность. Сеть и данные в компьютерной информационной системе защищены от повреждения, изменения или утечки по случайным или злонамеренным причинам, а система всегда надежна и безопасна. Она работает непрерывно, не прерывая поставку информационных услуг конечным потребителям.

ИБ сама по себе является широким и абстрактным понятием. В центре внимания ИБ находится безопасность самой информации. Основная задача ИБ – это защитить информационные активы, предотвратить утечку, подделку, уничтожение информации [4]. Для определения информационной

безопасности не существует единого определения в международном масштабе. ИС относится к защите системы, обеспечивающей стабильное предоставление информационных услуг.

С технической точки зрения ИБ обычно относится к защите ИС (включая аппаратное обеспечение, программное обеспечение, данные, персонал, физическую среду и инфраструктуру) для предотвращения атак на систему и утечки информации, а также для обеспечения того, чтобы информационная система может работать нормально без прерывания работы и что предоставляемые услуги могут быть надежно гарантированы. В настоящее время с точки зрения ИС широко распространено мнение, что современная информационная безопасность включает в себя следующие области:

Современная информационная безопасность включает в себя широкий спектр областей и аспектов, включая:

1. Кибербезопасность: защита компьютерных систем, сетей и данных от кибератак [5], включая вредоносное программное обеспечение, хакерские атаки и кибершпионаж.

2. Защита данных: обеспечение конфиденциальности, целостности и доступности информации, включая защиту от утечек данных, кражи личной информации и других угроз [6].

3. Идентификация и аутентификация: методы проверки личности пользователей и устройств для обеспечения безопасного доступа к информационным ресурсам.

4. Управление доступом: контроль доступа пользователей к различным ресурсам и данным, включая ролевые модели доступа и многофакторную аутентификацию.

5. Физическая безопасность: защита физических объектов, таких как серверные комнаты и центры обработки данных, от несанкционированного доступа и повреждений.

6. Социальная инженерия: предотвращение манипуляций и обмана со стороны злоумышленников, направленных на получение доступа к конфиденциальной информации.

7. Защита от внутренних угроз: мониторинг и предотвращение угроз со стороны сотрудников и контрагентов компании, включая утечку данных и злоупотребление привилегиями.

8. Защита от внешних угроз: защита от кибератак, включая DDoS-атаки, фишинг и другие виды мошенничества.

Большая часть перечисленных аспектов ИБ моделировалось в нашем образовательном проекте.

Ключевые технологии ИБ

Основным вопросом ИБ в современных информационных системах является криптографическая теория и ее приложения, а ее основой является структура и оценка надежности ИС.

ИБ включает в себя использование различных ключевых технологий для обеспечения защиты компьютерных систем, сетей и данных. Некоторые из основных технологий в этой области включают в себя [7]:

1. Криптография: использование математических методов для защиты информации путем шифрования и дешифрования данных, а также обеспечение целостности и подлинности сообщений.

2. Сетевые экраны: использование программного и аппаратного обеспечения для мониторинга и контроля трафика в сети, чтобы предотвратить несанкционированный доступ и атаки.

3. Идентификация и аутентификация: применение методов биометрии, многофакторной аутентификации и других технологий для проверки личности пользователей и устройств.

4. Управление доступом: использование программного обеспечения для управления привилегиями пользователей, контроля доступа к ресурсам и мониторинга действий пользователей.

5. Системы обнаружения вторжений (IDS) и предотвращения вторжений (IPS): использование специализированных систем для обнаружения и предотвращения несанкционированных попыток доступа к сети или системе.

6. Антивирусное программное обеспечение: установка и обновление антивирусных программ для защиты от вредоносных программ и атак [8].

7. Физическая безопасность: технологии, обеспечивающие защиту физических ресурсов информационной системы, таких, как серверные помещения, дата-центры, коммуникационное оборудование и т.д. Это может включать системы контроля доступа, видеонаблюдение, охранную сигнализацию и другие меры.

Это лишь некоторые из ключевых технологий, используемых в ИБ, и специалисты в этой области постоянно разрабатывают и внедряют новые методы и технологии для борьбы с постоянно меняющимися угрозами. Все данные технологии моделировались в виртуальной среде.

Разработка стенда для изучения

Для обучения работе студентов с отечественными продуктами для обеспечения ИБ нами был выбран Программный комплекс средств виртуализации «БРЕСТ» (ПК СВ «Брест») [9]. Наш выбор был обоснован следующими факторами.

Система виртуализации ПК СВ «Брест» - это инновационное решение, которое предназначено для обеспечения безопасности информации и защиты

компьютерных систем от внешних угроз. Эта система предоставляет возможность создания изолированных виртуальных сред, в которых могут выполняться различные приложения и операционные системы, не взаимодействуя с основной операционной системой компьютера.

Основная цель системы виртуализации ПК СВ «Брест» - это предотвращение утечек конфиденциальной информации и защита от вредоносных программ. Благодаря изоляции виртуальных сред, даже в случае заражения одной из них, остальные среды остаются неповрежденными. Это значительно повышает уровень безопасности компьютерных систем и снижает риск возникновения угроз.

Одним из ключевых преимуществ системы виртуализации ПК СВ «Брест» является возможность быстрого восстановления системы после атаки или вирусного заражения. Благодаря технологии создания резервных копий виртуальных сред, можно быстро восстановить работоспособность компьютера и избежать потери данных.

Кроме того, система виртуализации ПК СВ «Брест» обеспечивает удобство использования и экономию ресурсов. Пользователи могут запускать различные операционные системы и приложения на одном компьютере, не заботясь о конфликтах и несовместимости программного обеспечения. Это позволяет сэкономить время и ресурсы на поддержку нескольких физических компьютеров.

Таким образом, система виртуализации ПК СВ «Брест» является эффективным инструментом для обеспечения информационной безопасности и защиты компьютерных систем от угроз. Ее использование позволяет повысить уровень защиты данных, обеспечить надежную работу компьютеров и снизить риски возникновения угроз безопасности.

Для реализации макета инфраструктуры был выбран следующий вариант развертывания платформы виртуализации. Данный вариант

предназначен для реализации широкого круга задач по виртуализации информационной инфраструктуры.

Для обеспечения отказоустойчивости сервера с одинаковыми ролями дублируются. В макет включены следующие сервера (рис 1):

Два сервера управления, которые размещаются на физических серверах под управлением операционной системы Astra Linux SE (10).

Два контроллера домена с Astra Linux Directory (ALD), которые размещаются на физических серверах управления в виде виртуальных машин

Четыре ПК СВ БРЕСТ – сервера виртуализации для обеспечения отказоустойчивости ВМ.

Программно-определяемое хранилище Ceph в конвергентном режиме (4 сервера).

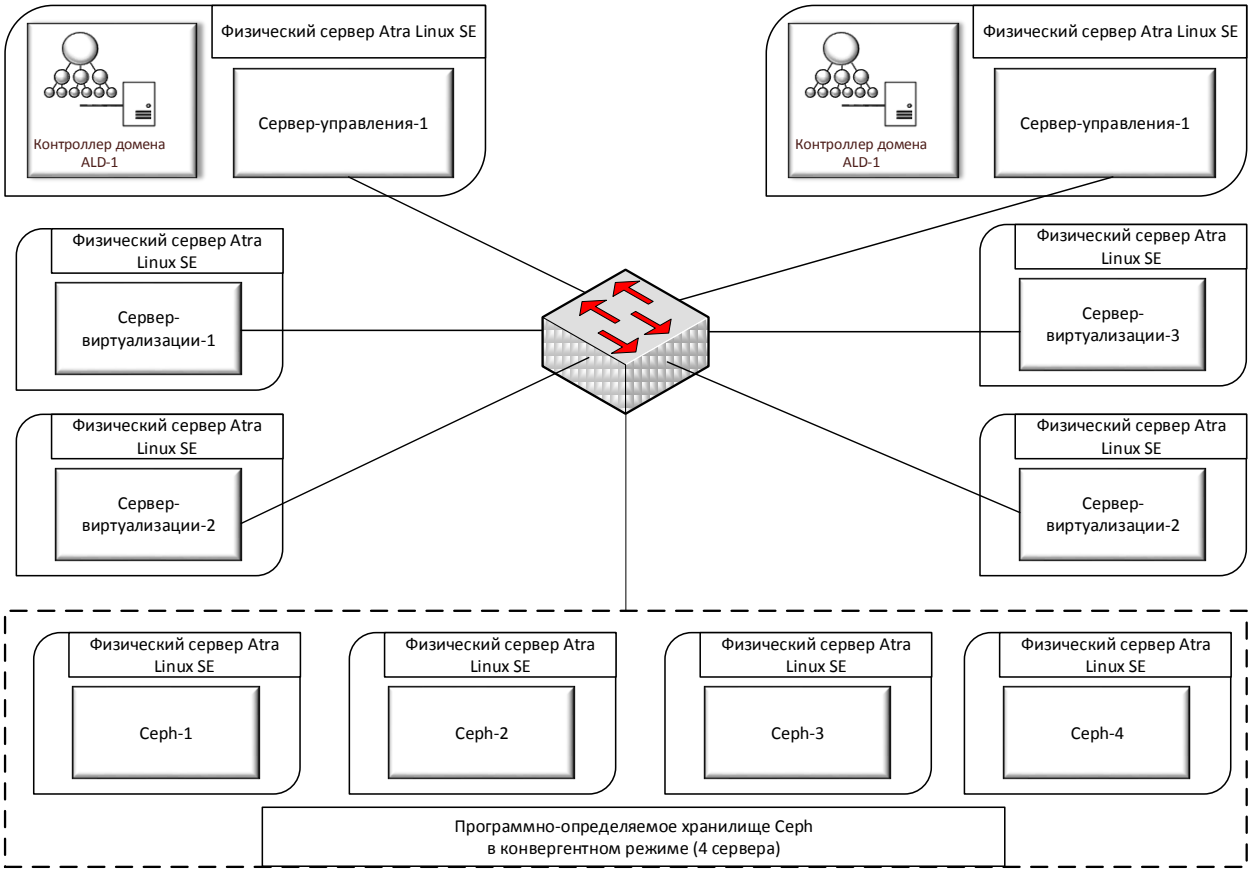

Рис. 1. – Схема макета для изучения ИБ виртуальных сред.

Заключение

Использование виртуализации на ПК СВ "Брест" для обучения методам ИБ является эффективным и перспективным подходом. Результаты исследования показали, что такой подход позволяет не только формировать профессиональные компетенции у студентов в области информационной безопасности, но и повышать их интерес к этой области. Это открывает новые возможности для развития независимого инновационного духа и практических навыков у студентов. Таким образом, виртуализация на ПК СВ "Брест" может быть широко использована в образовательных учреждениях для улучшения обучения методам ИБ.

Литература

1. Ибрагимова З.М., Батчаева З.Б., Ткаченко А.Л. Информационная безопасность как элемент экономической безопасности // Инженерный вестник Дона, 2022, №11. URL: ivdon.ru/magazine/archive/n11y2022/8010/.

2. Колесникова Д.С., Верещагина Е.А., Гуляев В.Е. Построение онтологической модели для предметной области «Информационная безопасность» // Инженерный вестник Дона, 2023, № 7. URL: ivdon.ru/ru/magazine/archive/n7y2023/8532/.

3. Горячев С.Н., Кобяков Н.С. Оценка состояния защищенности информационных систем от вредоносных программ // Безопасность информационных технологий. 2022. Т. 29, № 1. С. 44-56.

4. Катасев А.С., Катасева Д.В., Кирпичников А.П. Нейросетевое прогнозирование инцидентов информационной безопасности предприятия // Вестник Технологического университета. 2015. Т. 18, № 9. С. 215-218.

5. Oluwasanmi A. Network Security Concepts, Dangers, and Defense Best Practical // Computer Engineering and Intelligent Systems, 2023, Vol.14, №2. URL: dx.doi.org/10.7176/CEIS/14-2-03/.

6. Sun Y. Computer network information security and protection strategies in the era of big data //Applied and Computational Engineering, 2023, Vol. 4 URL: dx.doi.org/10.54254/2755-2721/4/2023326/.

7. Athisha G., Sankaranarayanan K. Key Technologies in Information Security // IETE Technical Review, 2005, Vol. 22. URL: dx.doi.org/10.1080/02564602.2005.11657899/.

8. Fu-Hau H., Min-Hao W., Chang-Kuo T, Chi-Hsien H., Chieh-Wen C. Antivirus Software Shield Against Antivirus Terminators // IEEE Transactions on Information Forensics and Security , 2012, Vol. 7. URL: dx.doi.org/10.1109/TIFS.2012.2206028/.

9. ПК СВ «Брест» URL: astralinux.ru/software-services/application-software-astra-group/brest/.

10. Astra Linux Special Edition URL: astralinux.ru/software-services/os/astra-linux-se/.

References

1. Ibragimova Z.M., Batchayeva Z.B., Tkachenko A.L. Inzhenernyj vestnik Dona, 2022, №11. URL: ivdon.ru/magazine/archive/n11y2022/8010/.

2. Kolesnikova D.S., Vereshchagina E.A., Gulyayev V.E. Inzhenernyj vestnik Dona, 2023, № 7. URL: ivdon.ru/ru/magazine/archive/n7y2023/8532/.

3. Goryachev S.N., Kobyakov N.S. Bezopasnost′ informatsionnykh tekhnologiy. 2022. T. 29, № 1. pp. 44-56.

4. Katasev A.S., Kataseva D.V., Kirpichnikov A.P. Vestnik Tekhnologicheskogo universiteta. 2015. Vol. 18, № 9. pp. 215-218.

5. Oluwasanmi A. Computer Engineering and Intelligent Systems, 2023, Vol.14, No.2 URL: dx.doi.org/10.7176/CEIS/14-2-03/.

6. Sun Y. Applied and Computational Engineering, 2023, Vol. 4. URL: dx.doi.org/10.54254/2755-2721/4/2023326/.

7. Athisha G., Sankaranarayanan K. IETE Technical Review, 2005, Vol. 22 URL: dx.doi.org/10.1080/02564602.2005.11657899/.

8. Fu-Hau N., Min-Hao W., Chang-Kuo T, Chi-Hsien H., Chieh-Wen C. IEEE Transactions on Information Forensics and Security , 2012, Vol. 7, URL: dx.doi.org/10.1109/TIFS.2012.2206028/.

9. PK SV «Brest» URL: astralinux.ru/software-services/application-software-astra-group/brest/.

10. Astra Linux Special Edition URL: astralinux.ru/software-services/os/astra-linux-se/.