DOI 10.36622/1682-7813.2024.27.3.004
УДК 004.056

ИЗУЧЕНИЕ ВОЗМОЖНОСТИ ВИРТУАЛИЗАЦИИ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ОБЪЕКТОВ С ПРИМЕНЕНИЕМ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ

Ю.Ю. Громов, П.И. Карасев, Ф.М. Пыршев

В данной работе рассмотрена задача виртуализации технических средств защиты объектов далее ТСЗО. ТСЗО представляют собой разнообразные устройства, которые обеспечивают защиту объектов. При изучении этих устройств возникает проблема того, что практически невозможно получить практические навыки работы с данными средствами в пределах учебного процесса. Целью работы является теоретическое обоснование возможности виртуализации ТСЗО для получения практических навыков их эксплуатации.

Ключевые слова: имитационное моделирование, технические средства защиты информации, визуализация, модели угроз, анализ реакции системы, тестирование стратегий безопасности, процессы защиты, технология, инструмент, информационная безопасность.

Введение

В курсе изучения дисциплин, связанных с информационной безопасностью, студенты сталкиваются с проблемой того, что не все навыки возможно получить в рамках занятий. Например, в рамках такой дисциплины, как «Технические средства защиты объектов» (ТСЗО) подробно рассматриваются теоретические материалы, связанные с техническими средствами, в рамках практических занятий возможно рассмотрение принципов работы некоторых средств, их устройство и особенности работы. Однако в учебном процессе маловероятным является получение знаний по размещению таких средств и их эксплуатации в пределах помещения. Это является следствием того, что в реальности необходимо реализовать либо подобие учебного полигона, где студенты смогут оттачивать свои навыки, либо организовать учебную практику, связанную с этим. Но первый вариант невозможен из-за стоимости реализации, а второй вариант малоэффективен, так как для практики студенты должны оказаться на предприятии, связанном с установкой и эксплуатацией технических средств защиты информации, однако ни одно учреждение не обладает достаточными ресурсами для обеспечения подобных условий для всех своих студентов.

Однако с этой задачей можно справиться, если перенести подобные занятия в сферу симуляции. Достаточно качественная модель сможет дать каждому студенту базовые знания в выше оговорённой сфере при минимальных затратах и минимальном изменении в учебном процессе, поэтому была поставлена цель: «теоретическое обоснование возможности виртуализации ТСЗО для получения практических навыков их эксплуатации». Достижение поставленной цели требует решить следующие задачи:

- определить актуальность темы и изучить уже реализованные проекты в данной сфере;
- изучить основные виды ТСЗО и их характеристики;
- реализовать метод виртуализации ТСЗО, позволяющий сохранить их характеристики;
- провести экспериментальную оценку эффективности реализованного метода.

Целями таких атак могут являться получение коммерческой тайны, персональных данных клиентов или сотрудников, а также деструктивное воздействие на систему.

Именно поэтому стоит акцентировать внимание на безопасности беспроводных сетей, так как именно данные сети зачастую являются слабым местом сети компании.

Основная часть

Исследование актуальности

Для определения актуальности данной темы был исследован мировой рынок, на предмет разработок по виртуализации технических средств защиты информации. В относительно свободном доступе есть несколько средств, позволяющих симулировать ТСЗО, их размещение и эксплуатацию.

Подобным инструментом можно назвать SimLab Security. Это коммерческое программное обеспечение, которое позволяет моделировать различные системы безопасности, включая системы физической защиты, информационной защиты и противопожарной защиты. SimLab Security предоставляет широкий набор функций, которые позволяют создавать реалистичные модели систем комплексной защиты и проводить различные эксперименты с их размещением и эксплуатацией.

Продукт SimLab Security создан и распространяется компанией SimLab Software, которая является разработчиком программного обеспечения для обеспечения информационной безопасности. Компания была организована в 2002 и базируется в Израиле.

SimLab Security распространяется в виде платной лицензии.

Лицензионная копия SimLab Security имеет разную стоимость в зависимости от количества пользователей и функций, которые включены в лицензию. Наименьшая цена лицензии составляет 299 евро за одного пользователя с минимальными функциями. Также есть возможность получить пробную версию на 30 дней.

SimLab Security имеет следующие преимущества:

- SimLab Security предлагает большой ряд функций, которые позволяют создавать реалистичные модели ТСЗО и проводить разнообразные эксперименты с их размещением и эксплуатацией;
- простота использования. SimLab Security снабжена удобным интерфейсом, позволяющим быстро разобраться в работе программы;
- Поддержка различных ТСЗО. SimLab Security поддерживает широкий спектр ТСЗО, включая системы физической защиты, информационной защиты и противопожарной защиты.

Недостатки у SimLab Security такие:

- SimLab Security распространяется по коммерческой модели, поэтому стоимость программы может быть высокой;
- SimLab Security предъявляет высокие требования к системе, поэтому для его использования может потребоваться мощная компьютерная система [1].

Другим средством является Open Sourse Supervisory Control And Data Acquisition, далее OpenSCADA. Это свободное программное обеспечение, которое предназначено для создания распределённых систем управления. OpenSCADA может использоваться для моделирования различных систем, включая системы безопасности. OpenSCADA предоставляет более гибкие возможности моделирования, чем SimLab Security, но требует более глубоких знаний в области систем управления.

Производитель: OpenSCADA (Open Source Supervisory Control And Data Acquisition) — это открытая система, разработанная сообществом OpenSCADA. Это программное обеспечение, которое распространяется по свободной модели распространения.

Форма распространения OpenSCADA распространяется под лицензией General Public License (GPL), что означает, что исходных код программы является общедоступным и может быть использован, изменён и распространён бесплатно. OpenSCADA бесплатное программное обеспечение для автоматизации и управления OpenSCADA - бесплатная платформа с открытым кодом, которая предназначена для автоматизации и управления промышленными процессами.

Среди основных преимуществ OpenSCADA:

- ширина возможностей. OpenSCADA предоставляет широкие возможности для настройки и расширения, что позволяет пользователям создавать системы безопасности, соответствующие конкретным требованиям;

- доступность: исходный код OpenSCADA доступен на официальном сайте проекта и на GitHub. Любой желающий может ознакомиться с принципами работы программы и участвовать в её развитии;
- бесплатность: OpenSCADA - бесплатная программа, которую можно использовать без ограничений. За её использование не требуется платить лицензионные сборы или другие платежи;
- поддержка различных ТСЗО. OpenSCADA поддерживает широкий спектр ТСЗО, включая системы физической защиты, информационной защиты и противопожарной защиты.

Минусы у OpenSCADA следующие:

- сложность: OpenSCADA является сложным программным обеспечением, поэтому для его использования требуется определённый уровень знаний в области систем управления;
- недостаточная поддержка: OpenSCADA является относительно новым программным обеспечением, поэтому его поддержка может быть недостаточной [2].

Схожим примером может служить SCADASIM. Это бесплатное программное обеспечение предназначено для моделирования систем SCADA. SCADASIM может использоваться для моделирования различных систем безопасности, которые используют системы SCADA для управления. SCADASIM предоставляет более простой интерфейс, чем SimLab Security и OpenSCADA, но его возможности моделирования ограничены системами SCADA.

Производитель: Продукт SCADASIM разработан и поддерживается CMU-SEI.

Форма распространения: SCADASIM распространяется в виде установочного пакета.

У SCADASIM есть преимущества:

- доступность: SCADASIM - бесплатная программа, которую можно использовать без ограничений. За её использование не требуется платить лицензионные сборы или другие платежи;
- простота использования: SCADASIM обладает проработанным интерфейсом, позволяющим комфортно изучит функционал приложения;
- поддержка различных систем SCADA. Продукт SCADASIM совместим с рядом систем SCADA, включая открытые и закрытые системы.

Недостатки у SCADASIM можно выделить примерно такие:

- SCADASIM предназначен для моделирования систем SCADA, поэтому его возможности моделирования ограничены этой областью;
- недостаточная поддержка: SCADASIM является относительно новым программным обеспечением, поэтому его поддержка может быть недостаточной [3].

Ещё средство, которое подходит под предметную область это AnyLogic. AnyLogic - это коммерческая платформа для моделирования и симуляции, разработанная компанией AnyLogic Company. Это программное обеспечение помогает визуализировать сложные системы и тестировать данные системы в различных условиях. Данный продукт наиболее часто используется в области создания систем безопасности, при улучшении эффективности процессов, при определении проведения в рамках различных систем.

Положительными сторонами этой программы можно назвать:

- широкий спектр применения: данный продукт можно использовать для визуализации множества видов систем, связанных с разными областями жизни;
- крупный инструментарий: приложение позволяет использовать множество инструментов, которые позволяют моделировать системы самых разных видов;
- простота использования: AnyLogic обладает проработанным интерфейсом, позволяющим комфортно изучить функционал приложения;
- взаимодействие с иными средствами: в AnyLogic реализована возможность взаимодействия с иными приложениями, такими как CAD и CAE.

Но есть и черты, что делают эту программу менее привлекательной:

- AnyLogic распространяется по коммерческим моделям распространения, поэтому стоимость программы может быть высокой;

- AnyLogic предъявляет высокие требования к системе, поэтому для его использования может потребоваться мощная компьютерная система;
- сложность: AnyLogic является сложным программным обеспечением, поэтому для его использования требуется определённый уровень знаний в области систем управления;
- ограничения в моделировании: AnyLogic может иметь ограничения при моделировании очень сложных или нелинейных систем;
- отсутствие поддержки открытого исходного кода. AnyLogic не является программным обеспечением с открытым исходным кодом, что ограничивает возможности пользователей вносить изменения или создавать собственные модули.

Наряду с этими специализированными средствами, для моделирования ТСЗО можно использовать и более общие средства моделирования, такие как Simulink, MATLAB и Python. Эти средства позволяют создавать модели ТСЗО любой сложности, но требуют более глубоких знаний в области моделирования.

Все рассмотренные средства моделирования технических средств защиты объектов являются зарубежными. Это означает, что эти средства могут не учитывать особенности российского законодательства и практики применения технических средств защиты объектов в России. Также все эти средства направлены по большей части на диспетчерское управление и сбор данных, что делает эти средства неподходящими для достижения цели.

Большинство российских работ, исследующих данный объект, занимаются математическим моделированием ТСЗО. Так же некоторые из них исследуют применение математических моделей для оптимального размещения ТСЗО, но эти результаты этих исследований трудно реализовать на практике, так как каждый объект имеет уникальный набор характеристик. Из этого исходит то, что специалист для решения задачи защиты объекта должен полагаться на собственные навыки работы с ТСЗО [4,5].

Были рассмотрены продукты из данной сферы, проанализированы публикации на подобную тему. Из анализа следует, что проблема моделирования и виртуализации технических средств защиты информации для преподавания и передачи знаний и умений по установке и эксплуатации ТСЗО в нашей стране не решена, а зарубежные продукты малодоступны и потенциально опасны для использования в современных реалиях.

Для виртуализации ТСЗО будет предложен метод, основанный на использовании имитационного моделирования. Имитационное моделирование — это метод, с помощью которого можно строить и создавать модели, отражающие процессы, происходящие в системе во времени. Из-за того, что все процессы в реальной жизни происходят на протяжении определённого времени, метод имитационного моделирования является наиболее подходящим для адекватного отражения поведения системы.

Классификация технических средств защиты объектов

Теперь, после рассмотрения актуальности данной работы, можно перейти к классификации ТСЗО. Это необходимо сделать, чтобы наиболее точно перенести принципы работы технических средств в симуляционную среду с достаточным уровнем правдоподобности модели. Технические средства защиты информации можно классифицировать по различным признакам, в том числе по назначению, по способу действия, по сфере применения и т. д.

По назначению ТСЗО можно разделить на следующие группы:

- средства физической защиты, далее СФЗ, предназначены для физического ограничения доступа к объекту или его частям, а также для обнаружения и предотвращения несанкционированного проникновения. К СФЗ относятся следующие приспособления: двери, замки, решётки, сигнализация, системы видеонаблюдения и т. д.;
- Средства информационной защиты, далее СИЗ. СИЗ предназначены для предотвращения несанкционированного

доступа к информации, её утечки, неправомерного использования или повреждения. К основным видам средств информационной защиты относятся:

- средства защиты от несанкционированного доступа: пароли, ключи доступа, биометрические системы, аппаратные и программные средства защиты периметра;
- средства защиты от утечек информации: межсетевые экраны, системы предотвращения вторжений, DLP-системы, которые предотвращают неконтролируемое разглашение конфиденциальных данных;
- средства защиты от вредоносного программного обеспечения: антивирусы, антишпионы, антиспам-фильтры, которые детектируют и устраняют вредоносное программное обеспечение;
- помимо перечисленных, существуют и другие средства информационной защиты, которые используются в зависимости от специфики объекта и характера обрабатываемой информации.

- средства противопожарной защиты, далее СПЗ. СПЗ являются важным компонентом системы обеспечения безопасности зданий и сооружений. Эти технические средства предназначены для предотвращения и ликвидации пожаров, а также минимизации их последствий. Основные виды средств противопожарной защиты включают:
  - пожарные сигнализации и извещатели: обнаруживают возгорания на ранней стадии и информируют о них соответствующие службы;
  - системы пожаротушения: включают в себя разбрызгиватели, системы водяного, пенного или газового тушения;
  - эвакуационные системы и средства: обеспечивают безопасную эвакуацию людей из здания во время пожара, к ним относятся дымососы, лестничные клетки и системы оповещения.
  - первичные средства пожаротушения: огнетушители, пожарные краны и песок, которые используются для локализации и тушения небольших очагов возгорания;
  - также в состав средств противопожарной защиты входят различные вспомогательные устройства, такие как системы удаления дыма, противопожарные двери и перегородки, обеспечивающие безопасную и эффективную эксплуатацию здания.

По механизму работы ТСЗО делятся на следующие группы:

- пассивные ТСЗО не требуют источника питания и не производят никаких действий при срабатывании. К пассивным ТСЗО относятся, например, ограждения, двери, замки, решетки и т. д;
- активные ТСЗО требуют источника питания и производят какие-либо действия при срабатывании. К данному виду относятся различные элементы, которые имеют какой-либо источник питания. К нему могут относится любые приборы.

Также ТСЗО можно классифицировать по месту их применения:

По области использования ТСЗО делятся на следующие группы:

- ТСЗО для защиты государственных объектов, такие объекты зачастую связаны с ведомствами РФ;
- ТСЗО для защиты объектов коммерческого сектора, таких как банки, предприятия, торговые центры и т. д;
- ТСЗО для защиты объектов жилого сектора, таких как жилые дома, квартиры, коттеджи и т. д.

Средства физической защиты предназначены для физического ограничения доступа к объекту или его частям, а также для обнаружения и предотвращения несанкционированного проникновения.

Среди всех технических средств, связанных с физической защитой, можно выделить следующие виды:

- статичные физические преграды – ограничивают перемещение, но не имеют подвижные элементы;
- динамические физические преграды – ограничивают перемещение и имеют подвижные элементы;
- запираемые физические преграды – разграничивают физический доступ;
- решётчатые физические преграды – ограничивают перемещение, но позволяют вести наблюдение;
- сигнализация – система обнаружения нарушителей и оповещения о проникновении;
- видеонаблюдение – система для визуального обнаружения нарушителя.

Основными элементами СФЗ являются:

Средства защиты информационных ресурсов, далее СЗИР. Данные средства используются для защиты информационной инфраструктуры.

Основными элементами СЗИР являются:

- средства защиты от несанкционированного доступа (средства защиты от несанкционированного доступа) - системы, предназначенные для предотвращения несанкционированного доступа к информации;
- средства защиты от утечек информации, далее СЗУИ. Эти - системы, предназначены для предотвращения утечек информации по различным каналам;
- средства защиты от вредоносного программного обеспечения далее СЗВПО. Эти системы, предназначены для защиты от вредоносного программного обеспечения.

Средства противопожарной защиты, далее СПЗ. Эти технические средства используются с целью предотвращения пожаров и ликвидации их последствий.

К данным средствам относятся следующие элементы:

- датчики дыма и температуры – элементы, обнаруживающие возгорание;
- пожарная сирена – устройство, оповещающее о возгорании;
- распрыскиватели – устройства, осуществляющие автоматическое тушение возгорание.

Основными элементами СПЗ являются:

Данная классификация наиболее точно описывает основные элементы ТСЗО, а приведённые в пример элементы идеально подходят для моделирования, однако важно заметить, что средства могут разниться по степени сложности, так, например, такие средства, как двери и решётки практически не потребуют создания сложных моделей, тогда как камеры или датчики потребуют чуть более сложного подхода.

Пример создания имитационной модели

В качестве примера будет создана модель камеры видеонаблюдения, как одного из наиболее сложных элементов ТСЗО для моделирования.

Камеры видеонаблюдения являются важными компонентами систем наблюдения. Эти технические средства обеспечивают получение изображения с объекта наблюдения, которое затем может быть использовано для различных целей, таких как обеспечение безопасности, контроль над персоналом, наблюдение за окружающей средой и т. д.

Основные данные, необходимые для моделирования камер видеонаблюдения можно поделить на подобные группы:

- данные, необходимые для моделирования изображения:
  - разрешение изображения – характеристика, которая показывает количество пикселей на единицу площади. Данная характеристика определяет качество изображения, что влияет и на качество и скорость распознавания;
  - световая чувствительность – характеристика, которая показывает уровень освещённости, необходимый для работы камеры;
  - поле зрения – характеристика, определяющая область, в рамках которой ведётся видеонаблюдение;
  - формат видео: формат видео определяет способ хранения и передачи видеосигнала.
- данные, необходимые для моделирования передачи данных:

  - формат передачи данных - характеристика, которая определяет, каким способом будет доставляться информация;
  - формат хранения данных - характеристика, которая определяется, каким способом и по каким правилам будет храниться информация.
- Дополнительные данные:
  - Монтаж камеры - характеристика, которая определяет расположение камеры и способ её крепежей;
  - Защита от внешних воздействий характеристика, которая определяет уровень защищённости камеры от условий внешней среды.

Далее будет показан процесс моделирования. Характеристики, связанные с процессом получения изображения наиболее важны для создания модели и переносится следующим образом: разрешение камеры определяется количеством пикселей, из которых состоит изображение. Математически это можно записать в таком виде:

$$R = h * w, \quad (1)$$

где R – разрешение изображения,

h – набор пикселей по вертикали;

w – набор пикселей по горизонтали.

Световую чувствительность можно преобразовать в формулу (2):

$$L = F * p, \quad (2)$$

где L – световая чувствительность;

F – коэффициент чувствительности;

p – интенсивность светового.

Поле зрения камеры необходимо рассматривать как угол, в рамках которого камера улавливает изображение, поэтому формула для данной характеристики следующая:

$$RF = \arctan\left(\frac{f}{d}\right), \quad (3)$$

где RF – поле зрения камеры;

f – фокусное расстояние объектива камеры;

d – расстояние между камерой и объектом наблюдения.

Формат видео определяет способом хранения и передачи видеосигнала. Для самого механизма работы камеры это не столь важный показатель, однако, формат может иметь значения в случае, если симулируется вся система, включая элементы хранения и передачи.

Далее рассмотрим механизм функционирования камеры. Все камеры снимают определённый сектор. Это значит, что возможно использовать формулу площади сектора:

$$S = \frac{\pi * r^2}{360^\circ} * \alpha. \quad (4)$$

Необходимо подставить формулу поля зрения (3) вместо угла альфа:

$$S = \frac{\pi * r^2}{360^\circ} * RF = \frac{\pi * r^2}{360^\circ} * \arctan\left(\frac{f}{d}\right). \quad (5)$$

Не решённым остаётся вопрос замены радиуса окружности r. Решением задачи является настройка разрешения, так как от него зависит качество изображения, а значит и расстояние, на котором может работать камера видеонаблюдения. Поэтому необходимо провести параллели между разными разрешениями и дальностью действия камер. Камера с разрешением 720 (1280 x 720 пикселей) будет иметь максимальную дальность в 10 метров, и в этом случае можно будет различить только силуэт потенциального злоумышленника. Камера с разрешением 1080 (1920 x 1080 пикселей) будет иметь максимальную дальность в 20 метров, а также можно будет разобрать одежду и некоторые простые черты потенциального нарушителя. При использовании камеры с разрешением 4К (3840 x 2160 пикселей) дальность «видимости» будет порядка 30 метров, и на этом расстоянии можно будет различить черты лица потенциального нарушителя.

Так как в данном примере моделируется работа камер в рамках предприятия, то важно создать показатель, который отражал бы время, которое необходимо, чтобы опознать нарушителя (рис. 1). Для этого воспользуемся параллелями между разрешениями и

дальностью, которые были определены ранее, но расчёты будут проведены в обратном порядке: 720 (1280 x 720 пикселей) время обнаружения нарушителя составит 30 секунд, 1080 (1920 x 1080 пикселей) составит 20 секунд и при 4K (3840 x 2160 пикселей) составит 10 секунд.

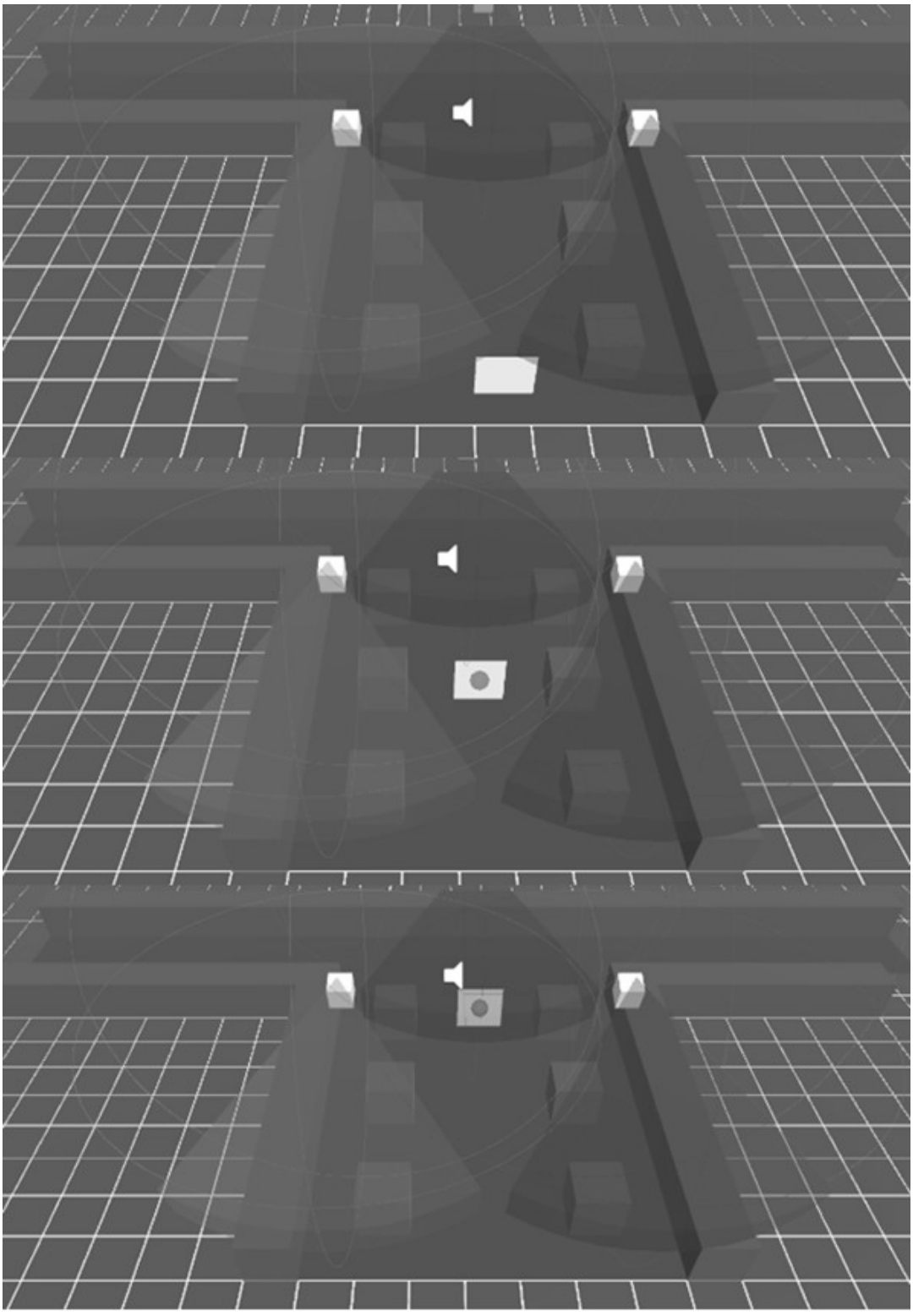

Рис. 1. Пример реализации описанной модели

В данном примере была смоделирована имитационная модель камеры, которая снимает определённую площадь и переводит систему ИБ в состояние тревоги через определённое время, после попадания в её

поле зрения нарушителя, что отражает базовые принципы работы камер.

В верхней части изображения представлено состояние, где условный нарушитель находится за пределами зоны «видимости» камер. При этом на нём нет каких-либо маркеров.

В средней части изображения представлено состояние, где условный нарушитель находится в пределах зоны «видимости» камер, но не в зоне прямой видимости. При этом на нарушителе возникает маркировка, которая говорит о том, что нарушитель может быть потенциально замечен.

В нижней части изображения представлено состояние, когда условный нарушитель находится в зоне прямой «видимости» камеры. При этом на условном нарушителе возникает маркировка того, что он не просто находится в потенциальной зоне видимости, а то, что он замечен. И через некоторое время существования данной маркировки на условном нарушителе поднимется тревога согласно модели, которая была описана выше.

Но также нужно понимать, что сама по себе модель камеры будет мало эффективна для тестирования. Это определено тем, что камера в редких случаях является независимым элементом защиты. Видеонаблюдение имеет зависимость от многих факторов, таких как:

Освещённость. О нём было сказано раньше, но стоит уточнить, что в разное время суток в одном и том же защищённом помещении может быть разный уровень освещённость, может быть, разное количество исправных осветительных приборов и многое другое.

Персонал. Камеры в редких случаях используются, как независимый элемент защиты. Чаще его используют в паре с персоналом, который занимается в паре с персоналом, который занимается мониторингом камер. Это также очень важно из-за того, что защищаемое помещение может быть оснащено самым современным и качественным оборудованием. Но оно будет бесполезно, если не будет выполнять свои обязанности должным образом.

Окружение. В зависимости от оснащения защищаемого помещения может быть разный результат работы камер. Это связанно с тем, что на работу камер могут влиять внешние факторы. Этими факторами могут быть погодные условия, если камера располагается вне помещений. Также таким фактором может быть интерьер защищаемого помещения, это связано с тем, что чрезмерно пёстрый интерьер понижает читаемость визуальной информации.

Таким образом был получен вывод, что необходимо моделировать не только сами устройства, но и окружающую среду.

Заключение

В данной работе была проанализирована актуальность проблемы, которая была определена выше, был рассмотрен метод виртуализации ТСЗО, основанный на использовании имитационного моделирования. Этот метод позволяет создать реалистичные модели ТСЗО, которые могут использоваться для обучения и отработки навыков эксплуатации технических средств. В этой работе были изучены основные виды ТСЗО и их характеристики. Также был рассмотрен пример имитационной модели камеры видеонаблюдения. Эффективность метода виртуализации ТСЗО была подтверждена с использованием примера.

Список литературы

1. Зайцев А.С. SimLab Security: комплексное средство моделирования систем безопасности / А.С. Зайцев, А.А. Мальюк, В.А. Головко // Security & Privacy. 2023. Т. 11. № 3. С. 16-28.

2. De Sousa M.R.S. OpenSCADA: A survey on the security vulnerabilities and mitigation techniques. / M.R.S. De Sousa, J.M. De Almeida, E.M. De Souza. // In 2019 IEEE 2nd International Conference on Cyber Security and Protection of Information (CyberSecPoC). P. 1-6.

3. Asif A.K. A comprehensive survey on SCADA simulation tools. / A.K. Asif, S.A. Khan, M.I. Khan, M.Z. Khan, M.A. Malik. // In 2021 IEEE International Conference on Industrial Cyber-Physical Systems (ICPS). P. 1-6.

4. Зайцева Н.О. Имитационное моделирование средствами системно-объектного подхода. / Н.О. Зайцева // Компьютерные и информационные науки. 2023(4), 123-132. [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/imitatsionnoe-modelirovanie-sredstvami-sistemno-obektnogo-podhoda (дата обращения: 6.07.24).

5. Каримова Д. Имитационное моделирование объектов технических систем. / Д. Каримова, Ч.С. Хашимова, Ш.Т. Джураева // URL: https://cyberleninka.ru/article/n/imitatsionnoe-modelirovanie-obektov-tehnicheskih-sistem (дата обращения: 6.07.24).

Тамбовский государственный технический университет
Tambov State Technical University

МИРЭА – Российский технологический университет
MIREA – Russian Technological University

Поступила в редакцию 15.07.24

Информация об авторах

Громов Юрий Юрьевич – д-р техн. наук, профессор, ТГТУ – Тамбовский государственный технический университет, gromovtambov@yandex.ru

Карасев Павел Игоревич – канд. техн. наук, МИРЭА – Российский технологический университет, e-mail: karasev@mirea.ru

Пыршев Фёдор Михайлович – студент, МИРЭА – Российский технологический университет, e-mail: pyrshev.f.m@edu.mirea.ru

STUDYING THE POSSIBILITY OF VIRTUALIZATION OF THE TSZ USING SIMULATION MODELING

Yu.Yu. Gromov, P.I. Karasev, F.M. Pyrshev

In this paper, the task of virtualization of technical means of object protection is considered, hereinafter referred to as TSZ. TSZOS are a variety of devices that provide protection for objects. When studying these devices, the problem arises that it is almost impossible to gain practical skills in working with these tools within the educational process. The purpose of the work is a theoretical justification of the possibility of virtualization of TSZOS in order to obtain practical skills in their operation.

Keywords: simulation modeling, technical means of information protection, visualization, threat models, system reaction analysis, testing of security strategies, protection processes, technology, tool, information security.

Submitted 15.07.24

Information about the authors

Yurii Yu. Gromov – Dr. Sc. (Technical), Professor, Tambov State Technical University, e-mail: gromovtambov@yandex.ru

Pavel I. Karasev – Cand. Sc. (Technical), MIREA – Russian Technological University, e-mail: karasev@mirea.ru

Fedor M. Pyrshev – student, MIREA – Russian Technological University, e-mail: pyrshev.f.m@edu.mirea.ru