КОНЦЕПЦИИ ПОДХОДА К УНИФИКАЦИИ КРИТИЧЕСКИ ВАЖНЫХ СИСТЕМ И ПРОЦЕССА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

CONCEPTS FOR AN APPROACH TO UNIFICATION OF CRITICAL SYSTEMS AND THE SAFETY PROCESS

Александрова Алина Викторовна

Студент 5-го курса по направлению «Информационная безопасность автоматизированных систем» Московского политехнического университета

Aleksandrova Alina Viktorovna

5th year student in the direction "Information security of automated systems" of the Moscow Polytechnic University

Широков Анатолий Александрович

Студент 5-го курса по направлению «Информационная безопасность автоматизированных систем» Московского политехнического университета

Shirokov Anatolij Aleksandrovich

5th year student in the direction "Information security of automated systems" of the Moscow Polytechnic University

Соболь Дмитрий Викторович

Студент 5-го курса по направлению «Информационная безопасность автоматизированных систем» Московского политехнического университета

Sobol' Dmitrij Viktorovich

5th year student in the direction "Information security of automated systems" of the Moscow Polytechnic University

Бритвина Валентина Валентиновна

Кандидат педагогических наук, доцент кафедры «Инфокогнитивные технологии» Московского политехнического университета, доцент кафедры «Управление и информатика в технических системах» Московского государственного технологического университета «СТАНКИН»

Britvina Valentina Valentinovna

Candidate of Pedagogy, Associate Professor of the Department of "Infocognitive Technologies" of the Moscow Polytechnic University, Associate Professor of the Department of "Management and Informatics in Technical Systems" of the Moscow State Technological University "STANKIN"

Аннотация. *Обеспечение безопасности компьютерных систем, которые полагаются на гарантии безопасности и защищенности, такие как согласованность, долговечность, эффективность и доступность, требуют или нуждаются в ресурсах. Это нацелено на проблемы системы систем (SoS), за исключением трудностей и проблем, которые аналогичным образом применимы к взаимодействиям подсистем в отдельной системе и взаимодействиям системы как компонентов в большой информационной системе. Это исследование направлено на обеспечение безопасности и информации для критически важных систем, где вопросы безопасности и защиты рассматриваются до перехода к этапу*

Abstract. *Securing computer systems that rely on security and safety guarantees such as consistency, durability, efficiency, and availability requires or needs resources. It targets the problems of a system of systems (SoS), except for difficulties and problems that are similarly applicable to interactions of subsystems in a single system and interactions of a system as components in a large information system. This research focuses on providing security and information for critical systems, where security and protection issues are considered prior to moving to the actual implementation / development phase of component systems. This will require a conceptual idea or strategy that addresses the security issues of the application logic. This could indicate a vulnerability in a single*

фактического внедрения / разработки компонентных систем. Для этого потребуется концептуальная идея или стратегия, которая касается вопросов обеспечения безопасности логики приложения. Это может показать уязвимость в отдельном компоненте или повторное использование спецификации в существующей логике в компонентной системе. Принимая во внимание эту ситуацию, мы определили семь концепций обеспечения безопасности и стратегии проектирования обеспечения безопасности для критически важных систем.

Ключевые слова: безопасность системы, гарантия работы компонентов, программное обеспечение, критически важное для безопасности, Software Assurance, информационная безопасность.

component, or reuse of a BOM in existing logic in a component system. With this situation in mind, we have identified seven security concepts and security design strategies for mission-critical systems.

Keywords: System security, component assurance, security-critical software, Software Assurance, information security.

Введение

Интеграция компонентов в промышленные системы управления, такие как железнодорожные системы контроля и управления (CCS), продолжается в рамках коммерческого готового аппаратного и программного обеспечения (COTS). Однако использование компонентов COTS в бывшей в использовании инфраструктуре безопасности приводит к новым рискам безопасности. Взаимодействие безопасности — важная область исследования, в которой еще предстоит решить несколько вопросов. Обеспечение безопасности является важной частью процесса разработки критически важного для безопасности программного обеспечения. Недостатки в инфраструктуре также может привести к ошибкам программного обеспечения и злоупотреблениям со стороны хакеров и преступников, стремящихся манипулировать недостатками в технологической отрасли. Тестирование, аккредитация и оценка проводятся для обоснования безопасности логической функции в процессе межкоммуникационного взаимодействия. Эта стратегия применяется на стадии проектирования, что относится к стандартной процедуре для повышения доверия к программе в процессе ее проверки [1].

Внедрение безопасности программного обеспечения в процессе проектирования / разработки было неотъемлемым аспектом общих инноваций современных критически важных систем, начиная от оружия, автомобильных систем управления, промышленных систем управления и медицинского оборудования. Программное обеспечение используется для отслеживания и регулирования физических процессов в этих системах, увеличение количества сбоев или отказов может привести к гибели людей или другим катастрофическим последствиям. Таким образом, обеспечение безопасности программного обеспечения для критически важных систем является одной из основных целей в системе компонентов [2].

Все больше программного обеспечения, включая встроенные системы, больше не предназначено для использования в системах безопасности. Вместо этого они используются (или повторно используются) для COTS, GOTS Government в готовом виде для программного и аппаратного обеспечения, приложений с открытым исходным кодом и других приложений, не связанных с разработкой, часто без изменений в настройке. Большая часть этого программного обеспечения, не предназначенного для разработки, особенно COTS и программного обеспечения с открытым исходным кодом, является компонентом автономных частей программного обеспечения, которые можно использовать в качестве строительных блоков для создания более крупных и сложных систем программного обеспечения. Наименьшая независимая единица разложения в программной системе может быть или не быть компонентом [3]. В некоторых случаях собираются компоненты с меньшими модулями. Чтобы можно было использовать в качестве компонента более широкой структуры, автономная программа должна предоставлять интерфейс(ы), обычно стандартизированный, чтобы позволить интегрировать или монтировать другие компоненты. В этом случае степень обеспечения безопасности компонентов и безопасности системы является главным приоритетом в обеспечении информации для критически важных для безопасности компонентных программных систем в организации [4].

Самым важным аспектом в обеспечении безопасности компьютерных систем является межкомпонентная спецификация. Взаимодействия между системами могут быть разделены потреблением одного компонента и другого [5].

В этом исследовании мы собираемся рассмотреть влияние безопасности и обеспечения информации на критически важные для безопасности компонентные программные системы, в котором обсуждаются вопросы безопасности и защиты в процессе внедрения и разработки систем.

Метод исследования

В своей исследовательской работе мы использовали прикладной метод исследования. У метода есть подкласс, называемый исследовательской оценкой. В этом

методе мы обращаемся к анализу, и оценочный анализ представляет собой своего рода аналитическое исследование, оценивающее текущие исследовательские знания, которые зависят от результатов эмпирических исследований или принятия обоснованных решений [7], например, научный метод исследования, поскольку он применяет существующие научные знания. Поэтому, имея в виду этот метод исследования, мы предложили семь концепций обеспечения информации для критически важного для безопасности программного обеспечения на основе компонентов.

Предпосылки исследования

Увеличение роста атак, а также очевидный сдвиг в сторону большей уязвимости, по-видимому, означают, что наша способность отражать атаки уменьшается, а разрыв между атаками и защитой информации увеличивается. Большая часть современной информационной безопасности основана на концепциях, определенных Зальцером и Шредером в статье ACM Communications 1974 года, озаглавленной «Безопасность информации в компьютерных системах». Защита была охарактеризована как «методы отслеживания того, кто может получить доступ или изменить устройство или информацию, хранящуюся в нем», и были описаны три ключевые категории проблем: конфиденциальность, целостность и доступность [8].

Мы обеспечиваем безопасность в области кибербезопасности и обеспечения информации для критически важных программных систем на основе компонентов следующим образом: «Программа Software Assurance, рассматриваемая как безопасность, представляет собой степень надежности защиты от программного обеспечения. Некоторые ошибки, преднамеренно или непреднамеренно разработанные, внедряются в программное обеспечение на любом этапе его жизненного цикла, поэтому программное обеспечение работает по назначению».

С распространением уязвимостей за счет программ-вымогателей, ошибок и инъекций структурированного языка запросов (SQL), межсайтовых сценариев и т.д. Эти проблемы изменили структуру и функциональность программы. Оказалось, что полагаться исключительно на защиту личных данных совершенно недостаточно. Кроме того, важность программного обеспечения в сетях возросла так, что теперь программное обеспечение управляет большей частью функциональных возможностей и усиливает эффект отказа системы безопасности [9].

Конвергенция и взаимодействие критически важных систем безопасности становится все более очевидной. Следовательно, имеет смысл создать общую концепцию обеспечения безопасности программного обеспечения, охватывающую безопасность и защиту. Различные методы, предлагаемые нынешними концепциями, возникают из угроз, связанных со сложными структурами [10].

Кроме того, принятие коммерческого готового (COTS) и программного обеспечения с открытым исходным кодом в качестве модулей, создает дополнительные проблемы для успешной операционной защиты. В результате операционные системы объединяют приложения из самых разных источников и собирают каждую часть по-своему [11].

Системы не могут быть построены так, чтобы устранять риски безопасности, но обладают способностью распознавать атаки, противостоять им и восстанавливаться после них. Система должна быть подготовлена к внедрению и обслуживанию при первоначальном проектировании. Чтобы гарантировать успешную защиту организации с течением времени, доверие должно быть запланировано на весь жизненный цикл [12].

Теперь мы используем следующую концепцию обеспечения жизненного цикла программного обеспечения на основе компонентов, созданную для:

Технологии и процедуры внедрены для получения требуемой степени уверенности в том, что приложения и службы работают должным образом, не имеют непреднамеренных или преднамеренных недостатков и обладают безопасными для угроз функциями защиты, а также восстановления после вторжений и сбоев.

Обзор существующих исследований

В области процесса унификации обеспечения безопасности критически важных для безопасности компонентных программных систем проводится не так много исследований. Тем не менее, мы рассмотрели некоторые важные работы, чтобы процитировать исследовательские работы.

По словам Фейсала Наби 2017, предложенный процесс унификации гарантии безопасности, который определяет защиту.

Автор описывает архитектуру в два этапа абстракции информационной системы.

1) Уровень проектирования метода объясняет форму для уровней архитектурной формы, которые должны быть реализованы на высшем уровне абстракции.

2) Определение архитектуры логической части.

Для обеспечения безопасного развертывания защиту необходимо применять с использованием подхода к проектированию, а не реализации уровня в структуре, путем взаимодействия с вышеупомянутыми основными элементами процесса обеспечения безопасности. Таким образом, архитектура может быть извлечена путем защиты курса протокола доверия [1].

Тим Келли, 2019 объяснил, что альтернативное решение путем создания структуры обеспечения соответствия и обеспечения данных (SSAF) ориентировано на фундаментальный набор стандартов безопасности. Вместо популярного совместного заверения, которое выявляет серьезные недостатки, защита и безопасность должны быть обеспечены индивидуально. Это часто позволяет использовать разные процессы и навыки практиков в каждой области. При таком расположении внимание переключается с простой кон-

вергенции на интеграцию посредством правильного обмена знаниями с синхронизацией в нужное время [3].

По словам Марши Чечик (Б., Рик Салай, Торин Вигер, Сахар Кокали и Мона Рахими, 2019), адреса тестовых случаев, тестовые данные, человеческое решение или их сочетание предоставят данные для обеспечения безопасности программного обеспечения. Это означает, что эксперты стремятся строить (критичные для безопасности) конструкции с осторожностью и выражать это рассуждение в соответствии с хорошо обоснованной методологией в обосновании безопасности, которое в конечном итоге проверяется человеком. Тем не менее, технологии имеют более глубокие корни в неопределенности, наиболее сложные функции открытого мира (например, понимание состояния земли самоуправляемым транспортным средством) часто не совсем предсказуемы или не рентабельны; вычислительные приложения также попадают в опасные условия, и могут возникать несоответствия [2].

Предлагаемая концепция обеспечения безопасности систем, критически важных для безопасности

Компоненты предназначены в первую очередь для объединения в системы, и в конечном итоге они действительно требуют безопасности. Компоновка катионов безопасности в более широкие системы — это не только нетривиальная задача, но и одна из проблем информационной безопасности, на которую трудно ответить, чтобы решить эту проблему в бизнес-логике соединения (дизайн, ориентированный на логические компоненты и интерфейс) в приложении электронной коммерции. Для быстрого развития на основе логических компонентов и для все более расширяющейся логики бизнес-процессов в системах электронной коммерции нам нужна конвергенция ресурсов процессов безопасности, как показано на рис. 1.

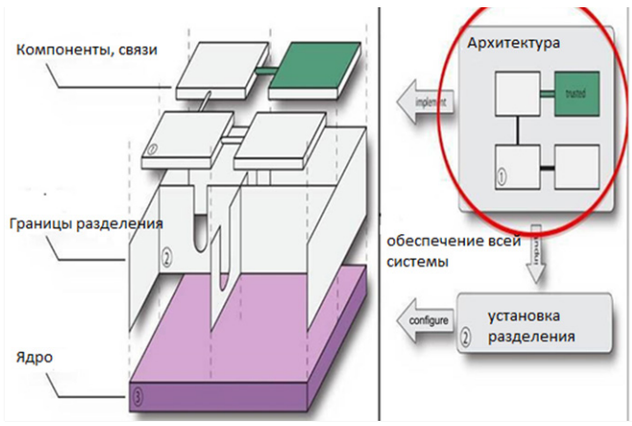

Рис. 1. Процесс обеспечения безопасности и свойства унификации

Чтобы достичь желаемой степени доверия к обеспечению безопасности программного обеспечения, мы рекомендуем семь концепций, направленных на решение проблем, связанных с обеспечением информации для критически важных для безопасности программных систем на основе компонентов, построением, развертыванием и сохранением систем.

1) Принятие решений руководствуется восприятием риска. Организации, не получившие надежных гарантий безопасности, сталкиваются с опасностью эффективных атак на инфраструктуру и системы. Они могут использовать варианты гарантий в зависимости от их восприятия угрозы аналогичной атаки и ожидаемого эффекта, например, стратегии, процедуры, методы и ограничения, если эта угроза осознается. Из-за того, что организации изо всех сил пытаются понять свои проблемы и воздействия, они могут неверно интерпретировать риски. Эффективная безопасность позволяет предприятиям делиться информацией о рисках как с партнерами, так и с участниками проекта.

2) Вопросы риска должны быть связаны с заинтересованными сторонами, а стратегические аспекты должны быть взаимосвязаны. Сети с высокой степенью взаимосвязи, такие как Интернет, требуют координации рисков между всеми вовлеченными игроками и всеми техническими элементами, связанными с ними; в противном случае на различных этапах взаимоотношений важные риски упускаются из виду или игнорируются. Когда все тесно взаимосвязано, недостаточно рассматривать только очень важные элементы. Взаимодействие осуществляется на разных уровнях технологий (например, сеть, безопасность, инфраструктура и приложения) и поддерживается рядом функций. Безопасность на любом из этапов может быть применена и, если ее плохо спланировать, может возникнуть конфликт. Эффективное заверение требует четкой идентификации, реагирования на риски на всех уровнях и позиций, связанных с взаимодействием.

3) Из-за широкого использования цифровых цепочек поставок гарантия автоматизированного товара зависит от суждений этих лиц с точки зрения приверженности и степени доверия к ним. Все недостатки гарантии каждого компонента связи исходят от оптимизированных приложений. Кроме того, любая рабочая функция, включая утилиты, программное обеспечение безопасности и другие программы, подлежит гарантии любой другой функции, если только не действуют уникальные ограничения и меры контроля. Компания попрежнему полагается на гарантийные решения других. Однако организации должны определить, насколько они уверены, что они полагаются на практическую оценку рисков, последствий и возможностей на основе разнообразного опыта. Зависимости не остаются неизменными, и предприятиям приходится ежедневно пересматривать доверительные связи, чтобы оценить корректировки, которые необходимо переосмыслить.

Следующие примеры определяют гарантированный ущерб от слабости: Централизованные технологические уязвимости (например, операционные системы, среды программирования, брандмауэры и маршрутизаторы) могут выступать в качестве общедоступных точек входа уязвимостей программного обеспечения. Использование нескольких общих инструментов разработки

технологий эффективно обеспечивает конечный цифровой продукт. Производители инструментов могут вносить уязвимости в программные продукты.

4) Конфиденциальность, целостность и доступность технических ресурсов приносятся в жертву широкой группе злоумышленников с растущими технологическими возможностями. Никакая защита от атак не является безупречной, и профиль злоумышленника продолжает развиваться. Некоторые угрозы используют технологии, а другие создают уникальные условия для использования средств защиты. Это то, как мы используем технологии.

5) Обеспечение того, чтобы соответствующая гарантия программного обеспечения нуждалась в хорошей командной работе. Организации должны обеспечить безопасность своих сотрудников, процедур и технологий, пока злоумышленники ищут все возможные точки доступа. Кроме того, организации должны конкретно определить на адекватном уровне политические полномочия и обязательства для обеспечения эффективного участия корпоративных участников в кибербезопасности. Эта теория предполагает, что все уверены в себе, но в целом это не так. Следовательно, организациям необходимо подготовить персонал для обслуживания технологий.

6) Гарантия может быть связующим звеном между программным обеспечением и сетевым администрированием, дизайном и обслуживанием и чрезвычайно подвержена улучшениям в любой из этих областей. Чтобы сохранить это равновесие, важно реагировать на частые смены, взаимосвязи, организационное использование и риски приложений. Это не разовый случай, потому что переход регулярный. После первоначального развертывания организации необходимо продолжить организационный мониторинг. Это должно быть включено в соответствующее обещание, требуемое компаниями. Это не будет добавлено позже. Каждый раз ни у кого нет денег на капитальный ремонт конструкций.

7) Должен быть реализован общий процесс оценки и оценки доверия. Организации не могут справиться с тем, что они не могут вычислить, а потребители технологий не будут нести ответственность за политику, пока они не возьмут на себя ответственность за нее. Если результаты отслеживаются и рассчитываются, уверенность не может эффективно конкурировать с другими конкурентными потребностями. Чтобы определить гарантии организации, все социально-технические элементы, такие как политики, процессы и процедуры, должны быть связаны вместе. Более эффективный процесс обеспечения уверенности реагирует и восстанавливается быстрее. Им будет выгодна их реакция и реакция других, а также они будут более тщательно предсказывать и выявлять угрозы.

Разработанная защитная стратегия как решение проблем на уровне бизнес-логики

Эта часть стратегии обеспечит строгий план контроля управления рисками, сосредоточенный на обеспечении строгой гарантии качества компонентов для быстрой разработки логики бизнес-приложений CBSD для критически важных для безопасности компонентных программных систем и их приложений в области электронной коммерции.

Ключевые элементы решения проблемы: 1) хороший план управления рисками; 2) Артефакты решения; 3) Характеристики безопасности компонентных компонентов.

1) Хороший план управления рисками: убедитесь, что каждый аспект дизайна приложения должен быть четко и достаточно подробным, чтобы проектировщик мог понять каждое предположение и логику спроектированной функции в приложении.

Обязать четко комментировать все CBSD и включать следующую информацию.

а) Цель и предполагаемое использование каждого компонента (если в коде компонента доступна информация о коде, если нет, его функциональная бизнес-логика в компоненте через описание контракта на использование).

б) Предположения и логика, сделанные каждым компонентом в отношении всего, что находится вне его прямого контроля.

с) Ссылка на все клиентские компоненты, в которых используется четкая документация по компонентам, которая могла бы предотвратить логическую ошибку в функциональности онлайн-регистрации.

2) Артефакты решения: поскольку нет уникальной сигнатуры, по которой можно было бы идентифицировать логические недостатки в веб-приложении, разработанном на основе компонентов Rapid, потому что до сих пор не разработано панацеи, которая могла бы защитить.

3) Характеристики безопасности компонентов программного обеспечения: поскольку программный компонент можно рассматривать как продукт или систему ИТ, естественно использовать общие критерии для оценки его свойств безопасности. Общие критерии обеспечивают основу для оценки ИТ-систем и перечисляют конкретные требования безопасности для таких систем. Требования безопасности делятся на две категории:

- Функциональные требования безопасности
- Требования к обеспечению безопасности

Функциональные требования безопасности:

Опишите желаемое поведение или функции безопасности, ожидаемые от ИТ-системы для противодействия угрозам в операционной среде системы. Эти требования классифицируются в соответствии с проблемами безопасности, которые они решают, и с различными уровнями безопасности. Они включают требования следующих классов: аудит безопасности, коммуникация, криптографическая поддержка, защита данных пользователя, идентификация и аутентификация, управление безопасностью, конфиденциальность, защита функций безопасности системы (метаданные безопасности), использование ресурсов, доступ к системе и надежный путь/каналы.

Требования к обеспечению безопасности:

Функциональные требования безопасности в основном касаются процесса разработки и эксплуатации ИТ-системы с учетом того, что более определенный и строгий процесс обеспечивает большую уверенность в поведении и работе системы в области безопасности. Эти требования классифицируются в соответствии с проблемами процесса, которые они решают, и с различными уровнями безопасности. Вопросы процесса включают поддержку жизненного цикла, управление конфигурацией, разработку, тесты, оценку уязвимостей, руководящие документы, доставку и эксплуатацию, а также гарантийное обслуживание.

На рис. 2 представлена идея процесса обеспечения безопасности, основанная на уровне обеспечения безопасности логики компонентного программного приложения для систем электронной коммерции. Этот процесс также полезен для разработчиков систем программного обеспечения на основе компонентов, критичных к безопасности, при повторном использовании спецификации существующей логики для текущей системы.

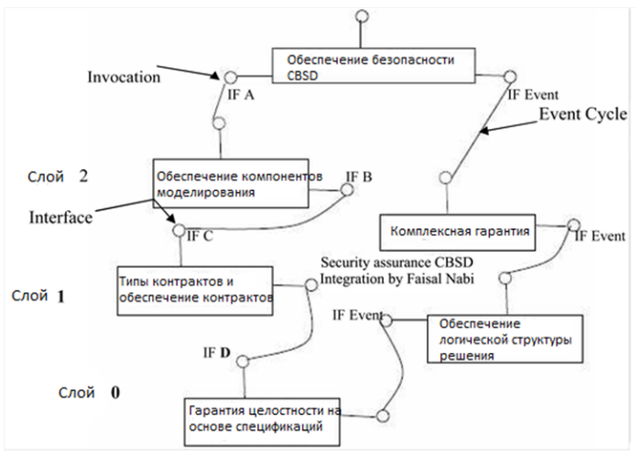

Рис. 2. Процесс разработки стратегии для логики бизнес-приложения обеспечения безопасности

Следовательно, важно, чтобы критически важные для безопасности системы, которые почти ежедневно используются при взаимодействии с людьми, и от простых систем до сложных систем на основе компонентов требовали гарантии перед прохождением стадии разработки, которая гарантирует безопасность системы в различных средах.

Заключение

В этом документе рассматриваются некоторые ключевые проблемы и информационные пробелы в защите больших и сложных системах. Эти недостатки связаны с пробелами между системами защиты и безопасности, тем, как угрозы изображаются и разъясняются, и как утверждения следует рассматривать как шаблоны. Эти семь концепций были описаны как механизм обеспечения безопасности и разработки стратегии обеспечения безопасности для независимой системы или компонента, устраняющий трудности разработки механизма, который синхронизирует отдельные гарантии безопасности и обеспечивает более сложную форму оценки воздействий. Семь концепций представляют собой предварительный план, способный изменить взаимосвязь секторов разведки и безопасности, а процесс моделирования стратегии проектирования безопасности помогает разработчикам убедиться в обеспечении безопасности системы на этапе SDLC, который, как было доказано, служит ориентиром для критически важного для безопасности компонента.

Список литературы

1. **Наби, Ф.** и **Наби, М.** (2017) Процесс унификации свойств обеспечения безопасности для логики приложений. Международный журнал электроники и информационной инженерии, 6, 40–48.
2. **Чечик, М., Салай, Р., Вигер, Т., Кокали, С.** и **Рахими, М.** (2019) Software Assurance в неопределенном мире.
3. Келли, Т. (2019) Структура независимого обеспечения безопасности и защищенности. Издательство Нью-Йоркского университета, Нью-Йорк.
4. **Чарнецки К.** и Салай Р. (2018) К концепции управления неопределенностью восприятия для безопасного автоматизированного вождения. В: Галлина Б., Скавхауг А., Шойч Э. и Битч Ф., ред., SAFECOMP 2018, LNCS, Vol. 11094, Спрингер, Чам, 439–445.
5. **Карлан, К., Галлина, Б., Касьянка, С.** и **Бреу, Р.** (2017) Споры о целесообразности методов проверки на уровне программного обеспечения. В: Тонетта, С., Шойч, Э. и Битч, Ф.
6. **Карлан К., Ратиу Д.** и Шетц Б. (2016) Об использовании результатов проверки моделей с ограничениями на уровне кода в случаях уверенности.
7. **Kriaa, S., Pietre-Cambacedes, L., Bouissou, M.** и Halgand, Y. (2015) Обзор подходов, сочетающих безопасность и защищенность для промышленных систем управления. Надежность и безопасность систем, 139, 156–178.
8. Symantec (2018, март) Отчет об угрозах безопасности 2018. Отчет ISTR об угрозах безопасности в Интернете.
9. **Берд Дж.** (2017, октябрь) 2017 Состояние безопасности приложений: баланс скорости и риска.
10. **Ульрих Дж.** (2016 г., апрель) Состояние безопасности приложений, 2016 г.: навыки, конфигурации и компоненты. Обзор института SANS.
11. **Закашевская, А.** (2016) Модель пропорционального подхода для применения ASEMS
12. **Финнеган, А.** и **Маккаффери, Ф.** (2014) На пути к концепции международной безопасности для сетевых медицинских устройств. Международная конференция по компьютерной безопасности, надежности и безопасности, сентябрь 2014 г., Springer, Cham, 197–209.
13. **Гер Т., Мильман М., Драхслер-Коэн Д., Цанков П., Чаудхури С.** и **Вечев М.** (2018) AI2: Сертификация безопасности и устойчивости нейронных сетей с абстрактной интерпретацией.