УДК 004.056.53

Д.С. Беляков, Е.О. Калинин, А.А. Конев, А.А. Шелупанов, А.А. Мицель

Модели жизненного цикла и угрозы безопасности микросхемы во время ее разработки и эксплуатации

Рост устройств интернета вещей показал необходимость развития направления информационной безопасности в области разработки и эксплуатации микросхем, так как вокруг последних и строятся современные информационные системы. В данной статье представлен жизненный цикл защищенных микросхем, используемых в качестве корня доверия (Root of Trust) информационных систем. Описаны основные этапы жизненного цикла защищенных микросхем, а именно модели жизненного цикла во время разработки и во время эксплуатации конечным пользователем.

Ключевые слова: безопасность, модуль безопасности, жизненный цикл, защищенные микроконтроллеры.
DOI: 10.21293/1818-0442-2023-26-1-76-81

В условиях стремительного роста киберугроз необходимо обеспечивать возможность безопасного информационного обмена в автоматизированных системах. Это особенно актуально в отношении критических информационных инфраструктур (КИИ) в системообразующих отраслях (например, энергетика, железнодорожный и воздушный транспорт, химические производства, банковские системы, здравоохранение, атомная и оборонная промышленность), где удачно проведенная кибератака может иметь самые тяжкие последствия [1, 2]. По этой причине в данных отраслях на передний план выдвигается создание доверенных автоматизированных систем.

Ключевым подходом в создании доверенных систем является использование защищённых микроконтроллеров с полностью контролируемым жизненным циклом [3, 4] от разработки кристалла до создания устройств на их основе.

Под защищенным микроконтроллером понимается полупроводниковое устройство, которое помимо процессорного ядра имеет в составе дополнительные аппаратные блоки для сокращения времени исполнения криптографических операций (криптографические акселераторы) и реализует меры защиты, которые противодействуют угрозам, направленным на конфиденциальные данные через воздействие на микросхему.

В современных реалиях микросхемы применяются в устройствах интернета вещей, где они отвечают за обеспечение безопасности каналов передачи данных [5] путем применения встроенных в микросхему криптографических механизмов.

Во время своей жизнедеятельности микросхема может находиться в двух состояниях – в состоянии разработки или эксплуатации. Во время разработки необходимо обеспечить защиту процесса создания микросхемы и сопровождающего программного обеспечения (например, комплекта разработчика). Во время эксплуатации необходимо обеспечить защищенность процесса использования микросхемы как разработчиком, так и конечным потребителем устройства, в состав которого входит данная микросхема. Разделение представленных процессов позволяет рассматривать каждую отдельную угрозу более подробно, а также формализовать модели жизненного цикла [6, 7].

Подобный подход к формализации жизненного цикла представлен в работе [8], в которой на основе теории графов была разработана модель угроз, возникающих при управлении системой защиты информации.

Необходимость использования различных моделей обусловлена не только отличающимися подходами к построению защищенной системы, но и разными аспектами обеспечения информационной безопасности ввиду различия целевых объектов [9].

Таким образом, целью данной работы является создание модели жизненного цикла защищенной микросхемы во время разработки и во время эксплуатации конечным пользователем, а также предоставление списка угроз на основании этих моделей в зависимости от целей безопасностей – конфиденциальности и целостности.

Модели, рассматриваемые в работе, не включают угрозы безопасности, возникающие в рамках управления персоналом (их подготовкой или обучением) или документооборота (в физическом или электронном виде).

Построение модели жизненного цикла

Жизненным циклом микросхемы называют все этапы проектирования и использования микросхемы – от этапа формирования требований до этапа утилизации [10, 11].

На рис. 1 представлена модель жизненного цикла микросхемы во время её разработки. Данная модель описывает разработку аппаратного обеспечения и встроенного ПО, так как процессы разработки являются аналогичными.

Этап 1.1. Формирование технического задания. Первоначальным этапом жизненного цикла разработки микросхемы является определение формальных требований к характеристикам устройства и программному обеспечению. На данном этапе важно обеспечить разработку модели угроз целевого устройства, в том числе определение целевого назначения устройства.

Рис. 1. Жизненный цикл разработки микросхемы

Этап 1.2. Проектирование микросхемы. Данный этап включает набор процессов, связанных с разработкой и отладкой функциональных блоков микросхемы. Для создания проекта микросхемы применяют инструменты автоматизированного проектирования, а тестирование полученных блоков осуществляется с помощью инструментов моделирования [12].

Данный этап является трудоемким из-за необходимости долгосрочного планирования с учетом множества потенциальных проблем и возможностей.

Этап 1.3. Реализация. На данном этапе происходит прототипирование печатных плат, создание комплекта разработчика программного обеспечения для микросхемы (Software Development Kit, SDK), написание исходного кода программного обеспечения, которое будет выполняться на разрабатываемой микросхеме. Также производится тестирование и отладка работы ПО путем симуляции разрабатываемой микросхемы на FPGA.

Этап 1.4. Анализ микросхемы на наличие уязвимостей. На данном этапе обеспечивается проверка функциональных блоков микросхемы и анализ программного обеспечения на соответствие требованиям безопасности.

Этап 1.5. Разработка патчей программного и аппаратного обеспечения микросхемы. На этапе разработки патчей микросхемы выполняется корректировка версий программного обеспечения и функциональных блоков микросхемы с учетом выявленных уязвимостей, чтобы избежать рисков реализации угроз информационной безопасности.

Этап 1.6. Анализ актуальности микросхемы. На этапе анализа актуальности микросхемы проводится проверка поддержки современных протоколов, операционных систем и мер защиты в функциональных блоках микросхемы и в ПО.

Этап 1.7. Разработка обновления программного и аппаратного обеспечения микросхемы. На данном этапе выполняется актуализация программного и аппаратного обеспечения микросхемы за счет добавления поддержки современных протоколов, операционных систем и мер защиты в микросхему и в ПО.

Этап 1.8. Производство микросхемы. Данный этап представляет собой набор процессов, которые необходимо выполнить для получения готовой микросхемы. Данные процессы включают действия, связанные с преобразованием полупроводниковых материалов в кремниевые пластины, изготовление масок, содержащих изображения топологии, которые будут перенесены на кремниевые пластины после облучения ультрафиолетовым светом для получения интегральной схемы (ИС), отделение кристалла от кремниевой пластины и упаковку кристалла в физический контейнер. На данном этапе также возможна инициализация программных модулей, не имеющих прямого отношения к логике работы пользовательских приложений (например, загрузчик).

Этап 1.9. Приемка микросхемы. Данный этап является окончательным на стадии разработки микросхемы и подразумевает выполнение полного всестороннего тестирования как функциональных блоков в частности, так и микросхемы в целом для проверки и подтверждения того, что реализованная микросхема и сопутствующее ПО (SDK) соответствуют требованиям к функциональным возможностям и производительности.

На рис. 2 представлена модель жизненного цикла микросхемы во время её эксплуатации конечным пользователем. Данная модель подходит для описания как разработчиков-интеграторов микросхемы в новое устройство, так и конечных пользователей, по той причине, что выделенные процессы эксплуатации являются аналогичными.

Этап 2.1. Поставка микросхемы. Исходя из требований целевого устройства, проводится выборка устройств на основе критериев функционирования и обеспечения безопасности.

Этап 2.2. Ввод микросхемы в эксплуатацию. Данный этап подразумевает выполнение процедур безопасной инсталляции выбранной микросхемы в среду функционирования (например, устройства КИИ), установку встроенного программного обеспечения и приведения устройства в функционирующего состояние.

Этап 2.3. Эксплуатация. На этапе эксплуатации микросхема используется по усмотрению пользователя, в роли которого может выступать как разработчик нового устройства, так и его конечный потребитель.

Этап 2.4. Контроль встроенного ПО на отсутствие уязвимостей. Целью представленного этапа является поиск, выявление и анализ уязвимостей, свойственных текущей версии встроенного ПО микросхемы и устраняемых путем применения корректирующего патча.

Этап 2.5. Установка патчей встроенного ПО. На данном этапе к встроенному ПО микросхемы применяются изменения, которые были выпущены разработчиком микросхемы или конечного устройства [13]. Изменения исправляют существующие ошибки, способствующие возникновению угроз в микросхеме или устройстве.

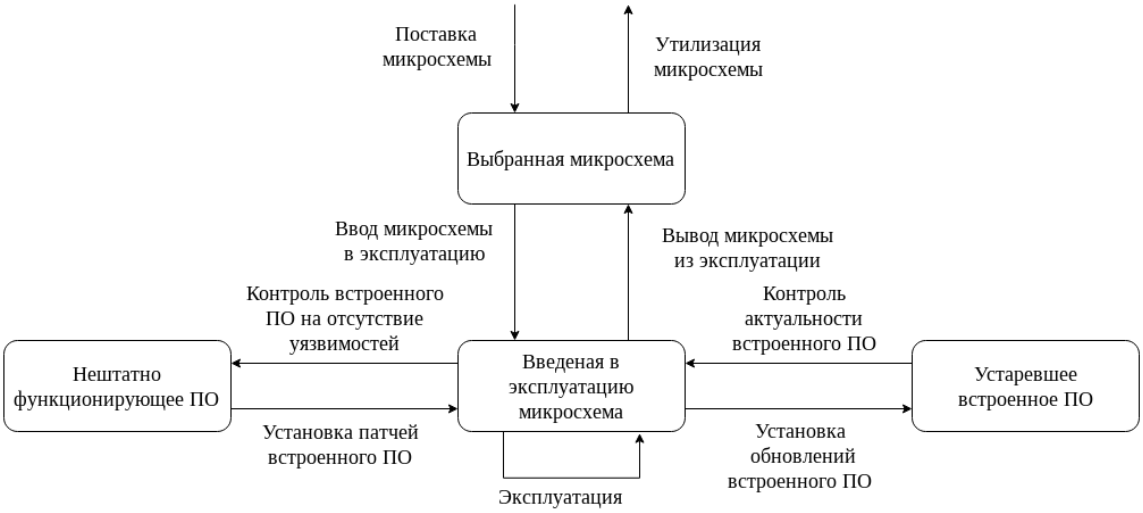

Рис. 2. Жизненный цикл эксплуатации микросхемы конечным пользователем

Этап 2.6. Контроль актуальности встроенного ПО. На данном этапе выполняется анализ степени устаревания встроенного ПО микросхемы с целью выявления компонентов, которые требуется обновить.

Этап 2.7. Установка обновлений встроенного ПО. Текущий этап реализует обновление содержимого встроенного программного обеспечения микросхемы для добавления нового функционала с целью соответствия современным стандартам защитных мер, протоколов и операционных систем.

Этап 2.8. Вывод микросхемы из эксплуатации. На данном этапе происходит удаление всех хранящихся ключей шифрования [14], пользовательской информации, а также данных о конфигурации устройства. Удаление происходит за счет полного стирания содержимого памяти и сброса настроек устройства до заводских для того, чтобы в случае необходимости его можно было использовать повторно.

Этап 2.9. Утилизация микросхемы. На данном этапе микросхема или устройство с микросхемой в составе физически уничтожаются.

В табл. 1 и 2 представлены угрозы, обеспечения конфиденциальности и целостности, соответственно свойственные этапам во время разработки и эксплуатации микросхемы. Некоторые из представленных угроз, соответствуют угрозам из перечня ГОСТ Р 58412–2019 [15].

Таблица 1

Угроза конфиденциальности микросхемы

Номер этапа	Разработка	Эксплуатация
1	*2*	*3*
1	Угроза выявления уязвимостей микросхемы вследствие раскрытия информации о требованиях по безопасности, предъявляемых к создаваемой микросхеме (соответствует 5.1.2 из ГОСТ Р 58412–2019)	Угроза выявления уязвимостей микросхемы в процессе ее поставки
2	Угроза выявления уязвимостей микросхемы вследствие раскрытия информации о проекте архитектуры микросхемы (соответствует 5.2.2 из ГОСТ Р 58412–2019)	Угроза выявления уязвимостей микросхемы вследствие раскрытия информации о параметрах безопасности, в том числе о ключах шифрования
3	Угроза выявления уязвимостей микросхемы вследствие раскрытия исходного кода встроенного ПО микросхемы или схемы микросхемы (соответствует 5.3.5 из ГОСТ Р 58412–2019)	Угроза выявления уязвимостей микросхемы вследствие раскрытия информации о нарушении правил эксплуатации микросхемы
4	Угроза выявления уязвимостей микросхемы вследствие раскрытия информации о тестировании микросхемы и ее встроенного ПО на уязвимость (соответствует 5.4.2 из ГОСТ Р 58412–2019)	Угроза выявления уязвимостей микросхемы вследствие отсутствия контроля наличия обновлений на наличие уязвимостей

Продолжение табл. 1

1	*2*	*3*
5	Угроза выявления уязвимостей микросхемы вследствие раскрытия информации о разработке патчей программного и аппаратного обеспечения микросхемы	Угроза выявления уязвимостей обновлений встроенного ПО
6	Угроза выявления уязвимостей микросхемы вследствие раскрытия информации об устраняемых патчем устаревших протоколах, ОС и мерах защиты в функциональных блоках микросхемы и во встроенном ПО	Угроза выявления уязвимостей микросхемы вследствие отсутствия контроля наличия обновлений на встроенное ПО
7	Угроза выявления уязвимостей микросхемы вследствие раскрытия информации о разработке обновления программного и аппаратного обеспечения микросхемы	Угроза выявления уязвимостей микросхемы вследствие раскрытия информации о нарушении правил установки обновлений встроенного ПО микросхемы
8	Угроза выявления уязвимостей микросхемы вследствие раскрытия информации о техническом процессе микросхемы	Угроза выявления уязвимостей микросхемы вследствие раскрытия информации о конфигурации устройства при выводе его из эксплуатации
9	Угроза выявления уязвимостей микросхемы вследствие раскрытия информации об ошибках программного обеспечения и уязвимостях программы (соответствует 5.6.2 из ГОСТ Р 58412–2019)	Угроза выявления уязвимостей микросхемы вследствие раскрытия информации о схемотехнике устройства из-за его неполной утилизации

Таблица 2

Угроза целостности микросхемы

Номер этапа	Разработка	Эксплуатация
1	Угроза появления уязвимостей микросхемы вследствие ошибок, допущенных при задании требований по безопасности, предъявляемых к разрабатываемой микросхеме (соответствует 5.1.1 из ГОСТ Р 58412–2019)	Угроза внедрения уязвимостей в микросхему в процессе ее поставки (соответствует 5.5.1 из ГОСТ Р 58412–2019)
2	Угроза появления уязвимостей микросхемы вследствие ошибок, допущенных при создании проекта архитектуры функциональных блоков микросхемы и в встроенного ПО (соответствует 5.2.1 из ГОСТ Р 58412–2019)	Угроза появления уязвимостей встроенного ПО микросхемы вследствие ошибок, допущенных при установке встроенного ПО (соответствует 5.2.1 из ГОСТ Р 58412–2019)
3	Угроза внедрения уязвимостей в исходный код встроенного ПО и в функциональные блоки микросхемы в ходе ее разработки (соответствует 5.3.1 из ГОСТ Р 58412–2019)	Угроза внедрения в программу уязвимостей при управлении конфигурацией программного обеспечения (соответствует 5.7.1 из ГОСТ Р 58412–2019)
4	Угроза появления уязвимостей программы вследствие совершения ошибок при выполнении тестирования программного обеспечения (соответствует 5.4.3 из ГОСТ Р 58412–2019)	Угроза использования уязвимостей микросхемы вследствие нарушений правил контроля встроенного ПО на отсутствие уязвимостей
5	Угроза неисправления обнаруженных уязвимостей программы (соответствует 5.6.1 из ГОСТ Р 58412–2019)	Угроза внедрения уязвимостей в патч программного обеспечения (соответствует 5.5.3 из ГОСТ Р 58412–2019)
6	Угроза появления уязвимостей вследствие отсутствия контроля актуальности используемых сторонних устаревших компонентов программного обеспечения	Угроза использования уязвимостей микросхемы вследствие нарушения правил контроля актуальности встроенного ПО
7	Угроза внедрения уязвимостей программы путем использования заимствованных у сторонних разработчиков программного обеспечения уязвимых компонентов (соответствует 5.3.2 из ГОСТ Р 58412–2019)	Угроза появления уязвимостей микросхемы вследствие нарушения правил обновления встроенного ПО
8	Угроза внедрения уязвимостей программы из-за неверного использования инструментальных средств при разработке программного обеспечения (соответствует 5.3.3 из ГОСТ Р 58412–2019)	Угроза появления уязвимостей микросхемы вследствие отсутствия поддержки или устаревания микросхемы (отказ от вывода из эксплуатации)
9	Угроза внедрения уязвимостей в исходный код встроенного ПО в ходе ее приемки (соответствует 5.3.1 из ГОСТ Р 58412–2019)	Угроза повторного использования компонентов микросхемы из-за неполной утилизации

Актуальность приведенного перечня угроз обосновывается тем, что он расширяет список угроз, представленных в ГОСТ Р 58412–2019, дополнительно к 19 угрозам из стандарта в работе предложено более 15 угроз. Это связано с используемым в статье подходом, заключающимся в разделении процессов жизненного цикла на разработку и эксплуатацию микросхемы, а также на разделение процессов жизненного цикла в зависимости от целей безопасности, что позволяет выявить узконаправленные угрозы.

Угрозы из стандарта являются слишком всеобщими и в большинстве случаев не могут применяться в реальных проектах. Например, в ГОСТ представленная угроза «Угроза внедрения уязвимостей в обновления программного обеспечения» не отража-

ет характер угрозы во время разработки и во время эксплуатации.

Заключение

В данной статье был представлен жизненный цикл защищенных микросхем, описаны его основные этапы, а также рассмотрены угрозы, свойственные каждому этапу в зависимости от целей безопасности – угрозы конфиденциальности и целостности микросхемы и ее встроенного ПО. Для каждого этапа (разработка микросхемы и эксплуатация микросхемы) выделено по 9 угроз конфиденциальности и целостности, применимых к любой микросхеме (всего 36 угроз).

Предложенный подход к формированию перечня угроз, основанный на типовых этапах жизненного цикла системы безопасности, обладает рядом преимуществ. В частности, он не только формализует перечень угроз, представленный в ГОСТ Р 58412–2019, но и дополняет его.

Статья подготовлена в рамках реализации программы ЛИЦ «Доверенные сенсорные системы» (Договор № 009/20 от 10.04.2020) при финансовой поддержке Минкомсвязи России и АО «РВК». Идентификатор соглашения о предоставлении субсидии – 0000000007119P190002.

Литература

1. Bhaiyat H. The Emergence of IIoT and its Cyber Security Issues in Critical Information Infrastructure / H. Bhaiyat, S. Sithungu // European Conference on Cyber Warfare and Security. – 2022. – Vol. 21, No. 1. – PP. 46–51.

2. Noseda M. Performance Analysis of Secure Elements for IoT / M. Noseda, L. Zimmerli, T. Schläpfer, A. Rüst // IoT. – 2021. – Vol. 3, No. 1. – PP. 1–28.

3. Ebad S.A. Exploring How to Apply Secure Software Design Principles // IEEE Access. – 2022. – Vol. 10. – PP. 128983–128993.

4. Intent-Driven Secure System Design: Methodology and Implementation / S.E. Ooi, R. Beuran, T. Kuroda, T. Kuwahara, R. Hotchi, N. Fujita, Y. Tan // Computers & Security – 2022 – Vol. 124. – P. 102955.

5. Threat Model for IoT Systems on the Example of OpenUNB Protocol / A. Shelupanov, A. Konev, T. Kosachenko, D. Dudkin // International Journal of Emerging Trends in Engineering Research. – 2019. – Vol. 7, No. 9. – PP. 283–290.

6. Модель жизненного цикла системы защиты информации / А.А. Конев, Т.Е. Минеева, М.Л. Соловьёв, А.А. Шелупанов, М.П. Силич // Безопасность информационных технологий. – 2018. – Т. 25, № 4. – С. 34–41.

7. Alenezi M. Security Risks in the Software Development Lifecycle / M. Alenezi S. Almuairfi // International Journal of Recent Technology and Engineering (IJRTE). Blue Eyes Intelligence Engineering and Sciences Engineering and Sciences Publication (BEIESP). – 2019. – Vol. 8, No. 3. – PP. 7048–7055.

8. Модель угроз безопасности, возникающих при управлении системой защиты информации / М.Л. Соловьев, Т.Е. Минеева, А.А. Конев, Д.Н. Буинцев // Доклады ТУСУР. – 2019. – Т. 22, № 3. – С. 31–36.

9. Computer network threat modelling / A. Novokhrestov, A. Konev, A. Shelupanov, A. Buymov // IOP Conf. Series: Journal of Physics: Conf. Series. – 2020. – Vol. 1488, No. 1. – P. 6.

10. Yousefnezhad N. Security in product lifecycle of IoT devices: A survey / N. Yousefnezhad, A. Malhi, K. Främling //Journal of Network and Computer Applications. – 2020. – Vol. 171. – P. 102779.

11. ГОСТ Р 57193–2016 Процессы жизненного цикла систем [Электронный ресурс]. – Режим доступа: https://docs.cntd.ru/document/1200141163, свободный (дата обращения: 10.11.2022).

12. Trending IC design directions in 2022 / C.-H. Chan, L. Cheng, W. Deng, P. Feng, L. Geng, M. Huang, H. Jia, L. Jie, K.-M. Lei, X. Liu, X. Liu, Y. Liu, Y. Lu, K. Nie, D. Pan, N. Qi, S.-W. Sin, N. Sun // Journal of Semiconductors. IOP Publishing. – 2022. – Vol. 43, No. 7. – P. 071401.

13. El Jaouhari S. Secure firmware Over-The-Air updates for IoT / S. El Jaouhari, E. Bouvet / Survey, challenges, and discussions // Internet of Things. – 2022. – Vol. 18. – P. 100508.

14. Mathur S. Internet of Things (IoT) and PKI-Based Security Architecture / S. Mathur, A. Arora // Industrial Internet of Things and Cyber-Physical Systems. – 2020. – PP. 25–46.

15. ГОСТ Р 56939–2016. Угрозы безопасности информации при разработке программного обеспечения [Электронный ресурс]. – Режим доступа: https://docs.cntd.ru/ document/12001355258, свободный (дата обращения: 10.11.2022).

Беляков Данила Сергеевич
Аспирант каф. комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) ТУСУРа
Ленина пр-т, 40, г. Томск, Россия, 634050
Тел.: +7 (382-2) 70-15-29
Эл. почта: bds2@csp.tusur.ru

Калинин Евгений Олегович
Аспирант каф. КИБЭВС ТУСУРа
Ленина пр-т, 40, г. Томск, Россия, 634050
Тел.: +7 (382-2) 70-15-29
Эл. почта: keo@csp.tusur.ru

Конев Антон Александрович
Канд. техн. наук, доцент каф. КИБЭВС ТУСУРа
Ленина пр-т, 40, г. Томск, Россия, 634050
ORCID: 0000-0002-3222-9956
Тел.: +7 (382-2) 70-15-29
Эл. почта: kaa1@keva.tusur.ru

Шелупанов Александр Александрович
Д-р техн. наук, проф., президент ТУСУРа
Ленина пр-т, 40, г. Томск, Россия, 634050
ORCID: 0000-0003-2393-6701
Тел.: +7 (382-2) 90-71-55
Эл. почта: saa@tusur.ru

Мицель Артур Александрович
Д-р техн. наук, проф. каф. автоматизированных систем управления (АСУ) ТУСУРа
Ленина пр-т, 40, г. Томск, Россия, 634050
ORCID: 0000-0002-2624-4383
Тел.: 8-923-430-52-90
Эл. почта: maa@asu.tusur.ru

Belyakov D.S., Kalinin E.O., Konev A.A.,
Shelupanov A.A., Mitsel A.A.

Life-cycle models and security threats to the microchip during its development and exploitation

The growth of Internet of Things devices has shown the need to advance the information security and more specifically the development and operation of microchips, as modern information systems are built around the latter. This article presents the lifecycle of secure chips used as the Root of Trust of information systems. The main stages of the life cycle of protected chips are described, namely life cycle models during development and operation by the end user.

Keywords: security, secure element, lifecycle, protected microcontrollers.
DOI: 10.21293/1818-0442-2023-26-1-76-81

References

1. Bhaiyat H. and Sithungu S., The Emergence of IIoT and its Cyber Security Issues in Critical Information Infrastructure. *European Conference on Cyber Warfare and Security*, 2022, vol. 21, no. 1. Academic Conferences International Ltd, pp. 46–51.

2. Noseda M., Zimmerli L., Schläpfer T., and Rüst A., Performance Analysis of Secure Elements for IoT. *Internet of Things*, 2021, vol. 3, no. 1. MDPI AG, pp. 1–28.

3. Ebad S.A., Exploring How to Apply Secure Software Design Principles. *IEEE Access*, 2022, vol. 10. Institute of Electrical and Electronics Engineers (IEEE), pp. 128983–128993.

4. Ooi S.E. et al., "Intent-Driven Secure System Design: Methodology and Implementation," Computers & Security, 2022, vol. 124. Elsevier BV, p. 102955.

5. Shelupanov A. Threat Model for IoT Systems on the Example of OpenUNB Protocol. *International Journal of* Emerging Trends in Engineering Research, 2019, pp. 283–290.

6. Konev A.A., Mineeva T.E., Soloviev M.L., Shelupanov A.A., and Silich M.P. [Model of the life cycle of the information security system]. *Bezopasnost informacionnyh tehnology*, 2018, vol. 25, no. 4. National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), pp. 34–42 (in Russ).

7. Alenezi M. and Almuairfi S. Security Risks in the Software Development Lifecycle. *International Journal of Recent Technology and Engineering (IJRTE)*, 2019, vol. 8, no. 3, pp. 7048–7055.

8. Soloviev M.L. et al. [Model of security threats arising from the management of information security systems]. *Proceedings of TUSUR University*, 2019, vol. 22, no. 3, pp. 31–36 (in Russ).

9. Novokhrestov A., Konev A., Shelupanov A., and Buymov A. Computer network threat modelling. *Journal of Physics: Conference Series*, 2020, vol. 1488, no. 1, p. 012002.

10. Yousefnezhad N., Malhi A., and Främling K. Security in product lifecycle of IoT devices: A survey. *Journal of Network and Computer Applications*, 2020, vol. 171. p. 102779.

11. GOST R 57193-2016. System lifecycle processes . Available at: https://docs.cntd.ru/document/1200141163 (Accessed: November 10, 2022) (in Russ).

12. Chan C.-H. et al. Trending IC design directions in 2022. *Journal of Semiconductors*, 2022, vol. 43, no. 7. IOP Publishing, p. 071401.

13. El Jaouhari S. and Bouvet E. Secure firmware Over-The-Air updates for IoT: Survey, challenges, and discussions. *Internet of Things*, 2022, vol. 18. Elsevier BV, p. 100508.

14. Mathur S. and Arora A. Internet of Things (IoT) and PKI-Based Security Architecture. *Industrial Internet of Things and Cyber-Physical Systems*, 2020, IGI Global, pp. 25–46.

15. GOST R 56939-2016. Threats to information security in software development Available at: https://docs.cntd.ru/document/12001355258 (Accessed: November 10, 2022) (in Russ).

Danila S. Belyakov
Postgraduate student, Department of Complex Information Security of Electronic Computer Systems (KIBEVS),
Tomsk State University of Control Systems and Radioelectronics (TUSUR)
40, Lenin pr., Tomsk, Russia, 634050
Phone: +7 (382-2) 70-15-29
Email: bds2@csp.tusur.ru

Evgeny O. Kalinin
Postgraduate student, Department of KIBEVS TUSUR
40, Lenin pr., Tomsk, Russia, 634050
Phone: +7 (382-2) 70-15-29
Email: keo@csp.tusur.ru

Anton A. Konev
Candidate of Sciences in Engineering, Assistant Professor, Department of KIBEVS TUSUR
40, Lenin pr., Tomsk, Russia, 634050
ORCID: 0000-0002-3222-9956
Phone: +7 (382-2) 70-15-29
Email: kaa@fb.tusur.ru

Alexandr A. Shelupanov
Doctor of Science in Engineering, Professor,
President TUSUR
40, Lenin pr., Tomsk, Russia, 634050
ORCID: 0000-0003-2393-6701
Phone: +7 (382-2) 90-71-55
Email: saa@tusur.ru

Artur A. Mitsel
Doctor of Science in Engineering, Professor
Department of Automated Control Systems (ACS), TUSUR
40, Lenin pr., Tomsk, Russia, 634050
ORCID: 0000-0002-2624-4383
Phone: +7-923-430-52-90
Email: maa@asu.tusur.ru