УДК 004.056.5 URL: https://ptsj.bmstu.ru/catalog/icec/insec/979.html

# БЕЗОПАСНАЯ РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ КАК СОСТАВЛЯЮЩАЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

**В.Е. Соколовский** sokolovskiyve@student.bmstu.ru
**Е.В. Глинская** glinskaya@bmstu.ru
SPIN-код: 5430-3023

*МГТУ им. Н.Э. Баумана, Москва, Российская Федерация*

Безопасная разработка программного обеспечения является актуальной задачей, решение которой направлено на создание системы обеспечения информационной безопасности организации. Хорошая стратегия разработки должна учитывать потребности безопасности, а также систему разработчиков организации. Цель исследования состоит в том, чтобы обеспечить безопасность, встроенную в процессы разработки. Частью успешной стратегии безопасности разработки является встреча с разработчиками для возможности внесения изменений в процессы разработки с учетом требований безопасности. В статье рассмотрены основные ошибки при разработке программного обеспечения, отличительные особенности процесса безопасной разработки, взаимосвязь результатов анализа безопасности при разработке программного обеспечения с вопросами применения средств защиты информации.

**Ключевые слова:** информационные технологии, программное обеспечение, обеспечение информационной безопасности, программы-анализаторы, ошибки программистов, процесс организации безопасной разработки

В настоящее время информационные технологии приобрели глобальный трансграничный характер и стали неотъемлемой частью всех сфер деятельности [1] личности и общества. Их эффективное применение является фактором ускорения экономического развития государства и формирования информационного общества [2].

Согласно Федеральному закону № 149-ФЗ[1], информационная система (ИС) определена как совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Программное обеспечение (ПО), под которым в соответствии с [3] понимается совокупность программ системы обработки информации и программных документов, необходимых для эксплуатации этих программ, наря-

[1] Об информации, информационных технологиях и о защите информации. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 12.12.2023).

 ISSN 2541-8009

ду со средствами вычислительной техники является важнейшим компонентом, непосредственно обеспечивающим функционирование ИС [4].

Значимость для функционирования различных ИС организаций обусловливает повышенное внимание к эксплуатации (применению) ПО со стороны нарушителей («хакеров»), что подтверждается экспертами ФСТЭК и ФСБ России, выступавшими на прошедшем 14–15 ноября 2023 г. в Москве SOC-форуме [5]. Таким образом, обеспечение информационной безопасности как состояния защищенности информационных ресурсов (информационной среды) от внутренних и внешних угроз [6], способных нанести ущерб интересам личности, общества, государства (национальным интересам) [7], является актуальной проблемой, стоящей перед организациями, эксплуатирующими ПО в составе ИС.

В целях обеспечения информационной безопасности в организациях создаются системы обеспечения информационной безопасности — совокупность сил обеспечения информационной безопасности, осуществляющих скоординированную и спланированную деятельность, и используемых ими средств обеспечения информационной безопасности.

Учитывая возрастающую информатизацию российского общества[2], государство предпринимает целенаправленные шаги по обеспечению информационной безопасности и импортозамещению ПО. Например, для значимых объектов критической информационной инфраструктуры[3] создаются необходимые условия для обеспечения информационной безопасности ИС за счет формирования правовых и регуляторных требований по обеспечению информационной безопасности ИС[4], создания банка данных угроз безопасности информации [8] и других мер.

Известно[5], что разработчики ПО относятся к категории нарушителей со средними возможностями и потенциально могут оказывать более негативное

[2] О федеральных государственных информационных системах, обеспечивающих предоставление в электронной форме государственных и муниципальных услуг (осуществление функций). Постановление Правительства РФ от 24.10.2011 № 861 (ред. от 16.08.2023).

[3] О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации. Указ Президента Российской Федерации от 30.03.2022 № 166.

[4] Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации. Приказ ФСТЭК России от 25.12.2017 № 239. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Приказ ФСТЭК России от 18.02.2013 № 21.

[5] Методика оценки угроз безопасности информации. Методический документ. Утв. ФСТЭК России 05.02.2021.

влияние на функционирование ИС, чем, например, системные администраторы и администраторы безопасности ИС.

Как правило, реализация угроз безопасности информации ИС с использованием ПО осуществляется в силу недекларированных возможностей ПО или наличия так называемых back door («задних дверей»), которые встраиваются разработчиками в алгоритмы работы ПО, например, с целью дальнейшей бесшовной поддержки эксплуатации ПО в ИС организации-заказчика.

В целом к наиболее распространенным ошибкам программистов при разработке (адаптации) ПО можно отнести следующие [9]:

– недостаточное или некорректное комментирование кода;

– пренебрежение стилем написания кода, форматированием, выбором названий переменных и объектов;

– ошибки, связанные с написанием собственных библиотек при условии, что есть готовые или общепринятые;

– непрозрачные названия переменных или функций;

– преждевременная оптимизация кода ПО.

С учетом вышеизложенного возникает необходимость обеспечения безопасности разработки ПО, в том числе при адаптации ПО к бизнес-процессам, реализуемым в ИС различных организаций.

Требования и подходы к безопасной разработке ПО находят свое отражение в регуляторных[6] и нормативных требованиях [3, 10] и направлены на формирование в организации-разработчике процесса безопасной разработки ПО.

Отличительными чертами процесса безопасной разработки ПО являются:

– анализ и учет требований результатов моделирования угроз безопасности информации не только для инфраструктуры ИС в целом, но и для разрабатываемого ПО в частности;

– преобразование требований к информационной безопасности ИС в план реализации разработки ПО, учитывающий требования безопасного проектирования;

– фокусирование на качестве и факте реализации ранее спроектированных требований информационной безопасности в коде разрабатываемого ПО, проверка созданных зависимостей;

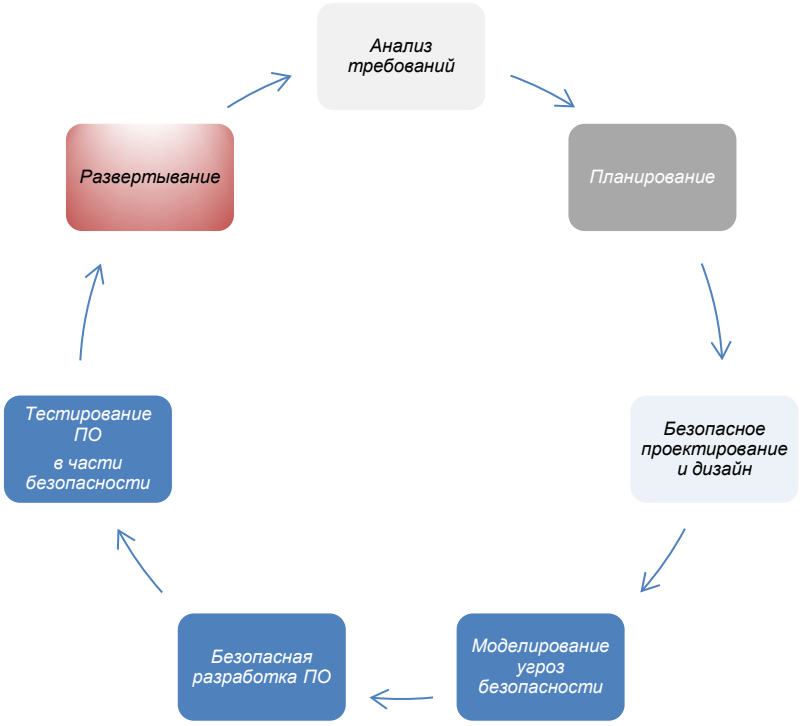
– тестирование на наличие уязвимостей в коде разработанного ПО;

[6] Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования. Приказ ФСТЭК России от 21.12.2017 № 235.

 ISSN 2541-8009

– мониторинг событий информационной безопасности и реагирование на инциденты информационной безопасности при развёртывании и сопровождении ПО в инфраструктуре ИС.

Схематично процесс организации безопасной разработки ПО представлен на рисунке.




Схематичное представление процесса безопасной разработки ПО

В Российской Федерации реализована процедура подтверждения отсутствия недекларированных возможностей в ПО средств защиты информации. Результаты находят свое отражение в сертификатах ФСТЭК России и публикуются в государственном реестре сертифицированных средств защиты информации [11].

Подтвердить отсутствие недекларированных функций в разработанном или унаследованном ПО также можно с помощью программ-анализаторов [12], позволяющих выполнить регуляторные и нормативные требования, например, в части статического и динамического анализа кода разработанного ПО, и тем самым снизить вероятность реализации угроз информационной

безопасности ИС за счет уменьшения потенциальных рисков и любых непредвиденных или нежелательных событий, которые могут нарушить деятельность или информационную безопасность в силу умышленных или неумышленных ошибок разработчиков кода ПО. Кроме того, использование программ-анализаторов кода ПО позволяет получить детальное описание обнаруженных уязвимостей и в случае невозможности их устранения — сформировать рекомендации для средств защиты информации ИС, располагаемых на внешнем периметре защищаемого контура ИС, например, для Web Application Firewall (WAF) под которым, как правило, понимают совокупность программных мониторов и фильтров, предназначенных для обнаружения и блокирования сетевых атак на веб-приложение.

Таким образом, наряду с криптографическими, аппаратными, инженерно-техническими и организационными мерами ПО является важным элементом системы обеспечения информационной безопасности ИС организации.

Соблюдение требований к безопасности разработки ПО позволяет повысить информационную безопасность ИС организации за счет уменьшения вероятности реализации угроз безопасности информации, использующих в качестве «точки входа» в контур безопасности ИС недекларированные возможности ПО.

**Литература**

[1] Ponamorev I.V. Systematization of Information Systems and Information Security. *Reports Scientific Society*, 2021, no. 3 (27), pp. 64–66. EDN QCQDBX.

[2] Якимова В.В. Современные достижения в сфере информационных технологий. *Язык в сфере профессиональной коммуникации. Междунар. науч.-практ. конф. преподавателей, аспирантов и студентов: сб. матер.* Екатеринбург, ООО «Издательский Дом «Ажур», 2020, с. 761–766. EDN IKURFU.

[3] ГОСТ Р 56939–2016. *Защита информации. Разработка безопасного программного обеспечения. Общие требования.* Москва, Стандартинформ, 2016.

[4] ГОСТ Р 53114–2008. *Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения*. Москва, Стандартинформ, 2008.

[5] *Soc forum 2024*. URL: https://forumsoc.ru/ (дата обращения 15.04.2024).

[6] Кипкеева А.М., Урусов А.А. Информационная безопасность — важнейший элемент обеспечения экономической безопасности организации. *Вестник Академии знаний*, 2020, № 40 (5), с. 157–161. https://doi.org/10.24412/2304-6139-2020-10611

 ISSN 2541-8009

[7] Вострецова Е.В. *Основы информационной безопасности*. Екатеринбург, Урал. Ун-т, 2019, 204 с.

[8] *Банк данных угроз безопасности информации*. URL: https://bdu.fstec.ru/ (дата обращения 15.04.2024).

[9] *25 ошибок начинающего программиста*. URL: https://habr.com/ru/articles/413129/ (дата обращения 15.04.2024).

[10] ГОСТ Р 58412–2019. *Защита информации. Разработка безопасного программного обеспечения. Угрозы безопасности информации при разработке программного обеспечения*. Москва, Стандартинформ, 2019.

[11] *Реестры ФСТЭК России*. URL: https://reestr.fstec.ru/ (дата обращения 15.04.2024).

[12] *Solar Appscreener*. URL: https://rt-solar.ru/products/solar_appscreener/?utm_source=Programmatic&utm_medium=cpc&utm_campaign=AppScreener&utm_content=cmp-90287064_gr-5235869414_ad-15505116023_ph-47403313262&utm_term=PRG1&yclid=12157612666175356927 (accessed April 15, 2024).

***Поступила в редакцию 25.04.2024***

**Соколовский Владислав Евгеньевич** — студент кафедры «Информационная безопасность», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

**Глинская Елена Вячеславовна** — старший преподаватель кафедры «Информационная безопасность», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

**Научный руководитель** — Басараб Михаил Алексеевич, доктор физико-математических наук, заведующий кафедрой «Информационная безопасность», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

**Ссылку на эту статью просим оформлять следующим образом:**
Соколовский В.Е., Глинская Е.В. Безопасная разработка программного обеспечения как составляющая системы обеспечения информационной безопасности организации. *Политехнический молодежный журнал*, 2024, № 03 (92). URL: https://ptsj.bmstu.ru/catalog/icec/insec/979.html

# SECURE SOFTWARE DEVELOPMENT AS A COMPONENT IN THE SYSTEM ENSURING THE ORGANIZATION INFORMATION SECURITY

**V.E. Sokolovsky** sokolovskiyve@student.bmstu.ru
**E.V. Glinskaya** glinskaya@bmstu.ru
SPIN-code: 5430-3023

*Bauman Moscow State Technical University, Moscow, Russian Federation*

Secure software development is an urgent problem. Its solution is aimed at creating a system to ensure information security in an organization. Good development strategy should take into account the security needs, as well as the system of the organization developers. Study objective is to ensure security built into the development processes. Part of the security system successful development is meeting the developers to be able to make changes in the development processes taking into account the security requirements. The paper considers main errors in the software development, distinctive features of the secure development process, relationship between the security analysis results in software development and the problems in using the information security tools.

**Keywords:** information technology, software, ensuring information security, analyzer programs, programmer errors, process of organizing secure develop

***Received 25.04.2024***

**Sokolovsky V.E.** — Student, Department of Information Security, Bauman Moscow State Technical University, Moscow, Russian Federation.

**Glinskaya E.V.** — Senior Lecturer, Department of Information Security, Bauman Moscow State Technical University, Moscow, Russian Federation.

**Scientific advisor** — Basarab M.A., Dr. Sci. (Phys.-Math.), Head of Department of Information Security, Bauman Moscow State Technical University, Moscow, Russian Federation.

**Please cite this article in English as:**
Sokolovsky V.E., Glinskaya E.V. Secure software development as a component in the system ensuring the organization information security. *Politekhnicheskiy molodezhnyy zhurnal*, 2024, no. 03 (92). (In Russ.). URL: https://ptsj.bmstu.ru/catalog/icec/insec/979.html

 ISSN 2541-8009