DOI: https://doi.org/10.15688/NBIT.jvolsu.2023.3.6

УДК 004.4
ББК 32.972.53

МЕТОДЫ РАЗРАБОТКИ ЗАЩИЩЕННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Владислав Георгиевич Яриков

Кандидат педагогических наук, доцент,
кафедра информационной безопасности,
Волгоградский государственный университет
yarikov.vladislav@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Максим Викторович Пашков

Студент, кафедра информационной безопасности,
Волгоградский государственный университет
IBm-221_992475@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. Настоящая статья посвящена вопросу защиты программного обеспечения на основе использования современных методов защиты. Одним из таких методов является внедрение в систему программного обеспечения процедур, которые должны снизить уровень ошибок, риски уязвимости системы и программного обеспечения.

Ключевые слова: программное обеспечение, защита, данные, методы, разработка, внедрение.

В настоящее время информационная безопасность является неотъемлемой частью процесса цифровизации, защиты данных. Компьютерные атаки, которые с каждым годом становятся более частыми (ввиду перехода всех услуг, сервисов в работу в цифровой среде) приводят к снижению уровня защиты программного обеспечения и информационных систем. Программное обеспечение становится объектом атаки по причине свое уязвимости и выходом из такой ситуации может послужить внедрение дополнительной защиты программного обеспечения посредством различных процедур [2].

В настоящее время существует ряд ГОСТов, призванных обеспечить безопасность функционирования программного обеспечения. Однако такие стандарты были перенасыщены значительным количеством актов, регулирующих вопросы обеспечения информационной безопасности. Здесь речь идет о различных корпоративных, межотраслевых стандартах, о международных стандартах безопасности. Такие стандарты содержат в себе указания, практические рекомендации по формированию безопасной среды, по устранению причин, которые лежат в основе уязвимости системы и программного обеспечения.

Вместе с тем можно отметить, что существующие документы не содержат четко определенного аппарата, который мог бы использоваться для независимой оценки реализован-

ных разработчиком мер требованиям разработки безопасного программного обеспечения. Сегодня этот пробел в документах по разработке защищенного программного обеспечения решает документ ГОСТ Р 58412-2019 [1].

Важным аспектом при создании и разработке программного обеспечения является обеспечение защищенности такой системы. Однако большинство производителей программного обеспечения уделяют недостаточно внимания на задачи обеспечения безопасности и защищенности выпускаемых продуктов.

Сегодня существует ряд методов, которые можно учитывать при разработке защищенного программного обеспечения. Классификация таких методов производится по ряду критериев: например, по границам применения того или иного метода; исходя из конкретной цели создания того или иного программного обеспечения.

Существуют методы, которые целесообразно применять на этапе разработки программного обеспечения, в процессе управления программным обеспечением, на этапе его тестирования или ввода в эксплуатацию. Поэтому выбор того или иного метода осуществляется на основе четко поставленной цели, границ применения и эффективности. На рисунке 1 представлены методы, которые используются в ходе осуществления управления разработкой защищенного программного обеспечения [3].

Если говорить о методе «команды безопасности», то сущность такого метода заключается в том, что в структуре организации выделяется отдельная группа (команда безопасности), которая принимает на себя ответственность за развитие и улучшение процесса разработки программного обеспечения с позиции ее информационной защищенности. Такая группа является экспертной по вопросам обеспечения безопасности системы [2].

При разработке любого программного обеспечения важнейшим этапом является разработка технического задания, где и производится описание целей и задач, способов обеспечения защиты программного обеспечения. Именно на такое задание и опираются в своей деятельности разработчики программного обеспечения. На рисунке 2 представлены базовые требования, которые предъявляются к разработке программного обеспечения [2].

Предъявляются и требования к системе безопасности в процессе разработки программного обеспечения. На рисунке 3 представлены такие требования, которые необходимо учесть при разработке защищенного программного обеспечения.

Если говорить о техническом задании на систему безопасности, то в таком задании должны найти отражение такие разделы, как [3]:

– общие сведения о задании;

– цели и задачи, которые должна решить создаваемая система;

– характеристика объекта;

– системные требования и перечень работ, которые должны быть произведены в процессе разработки системы, а также порядок контроля системы;

– источники разработки и т. д.

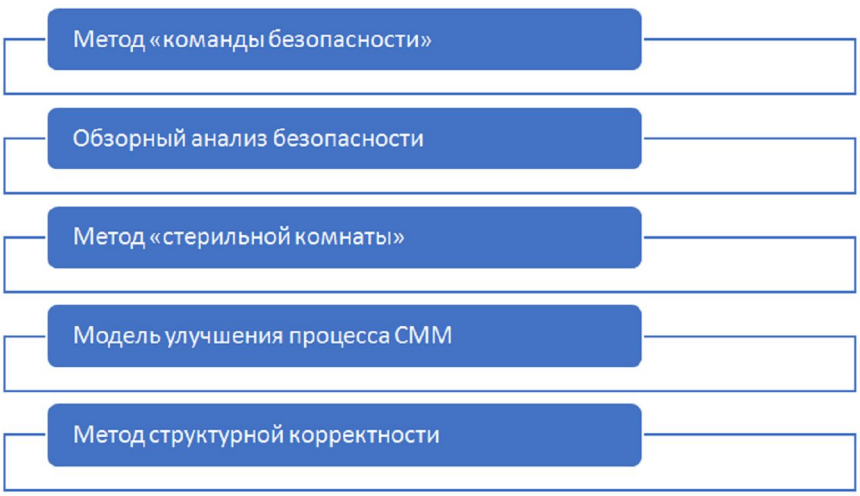

Рис. 1. Методы, применяемые в управлении разработкой программного обеспечения

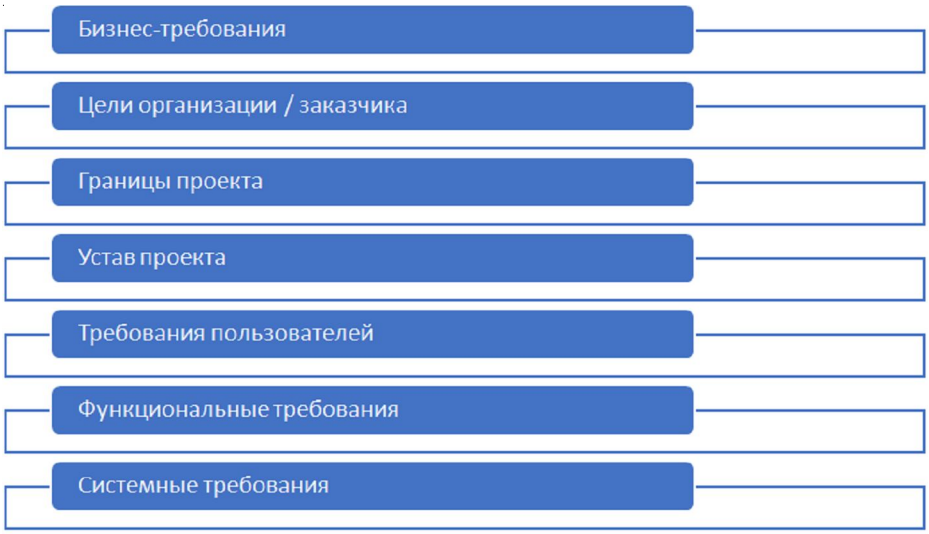

Рис. 2. Требования к разработке

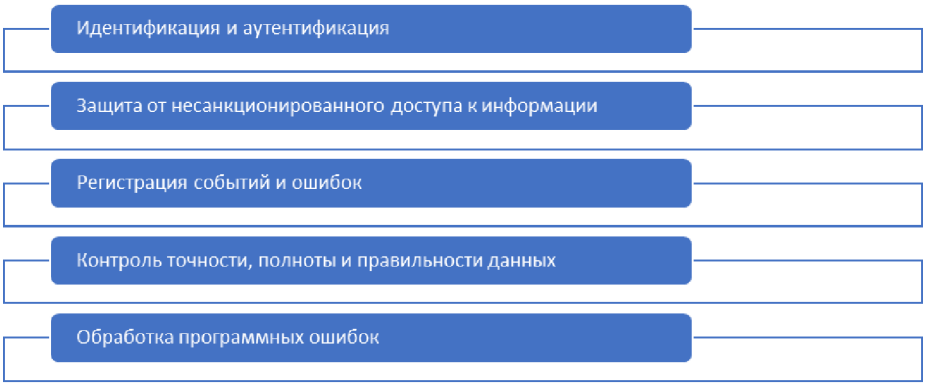

Рис. 3. Требования к безопасности

На основании технического задания формируется регламент, который служит основой для разработки системы и обеспечения ее защищенности в соответствии с полученным заданием.

Процедура внедрения программного обеспечения в эксплуатацию является завершающей стадией разработки и нередко происходит совместно с отладкой системы.

Ключевой целью поэтапного внедрения разработанной программы становится постепенное выявление необнаруженных ранее ошибок и недочетов кода. В рамках этого этапа разработки программного обеспечения и заказчик, и исполнитель могут столкнуться с рядом достаточно узкого спектра ошибок, связанных с частичной рассогласованностью данных при их загрузке в базы данных, а также срывов выполнения программных процедур в связи с применением многопользовательского доступа. Именно на этой стадии выкристаллизовывается окончательная картина взаимодействия пользователя с программой, а также определяется степень лояльности последнего к разработанному интерфейсу.

Если выход системы на проектную мощность после ряда проведенных доработок и улучшений произошел без особых осложнений, значит, предварительная работа над проектом и реализация предыдущих стадий разработки осуществлялась правильно.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р 58412-2019. Защита информации. Разработка безопасного программного обеспечения. Угрозы безопасности информации при разработке программного обеспечения // Электронный фонд правовой и нормативно-технической информации. –

Электрон. текстовые дан. – Режим доступа: https://docs.cntd.ru/document/1200164529. – Загл. с экрана.

2. Логачева, Н. В. Важность тестирования программного обеспечения в процессе разработки программного обеспечения / Н. В. Логачева, М. Л. Ладонычева, К. С. Пузырева // Инновационная наука. – 2022. – № 2-2. – С. 23–26.

3. Плахина, Е. А. Разработка схемы тестирования программного обеспечения / Е. А. Плахина // Известия Тульского государственного университета. Технические науки. – 2021. – № 9. – С. 274–276.

REFERENCES

1. GOST R 58412-2019 *Zashhita informacii. Razrabotka bezopasnogo programmnogo obespechenija. Ugrozy bezopasnosti informacii pri razrabotke programmnogo obespechenija* [GOST R 58412-2019 Information Protection. Development of Secure Software. Threats to the Security of Information During Software Development]. *Elektronnyj fond pravovoj i normativno-tehnicheskoj informacii* [Electronic Fund of Legal and Regulatory Technical Information]. URL: https://docs.cntd.ru/document/1200164529

2. Logacheva N.V., Ladonycheva M.L., Puzyreva K.S. Vazhnost testirovanija programmnogo obespechenija v processe razrabotki programmnogo obespechenija [The Importance of Software Testing in the Process of Software Development]. *Innovacionnaja nauka* [Innovative Science], 2022, vol. 2-2, pp. 23-26.

3. Plakhina E. A. Razrabotka shemy testirovanija programmnogo obespechenija [Development of a Software Testing Scheme]. *Izvestija Tulskogo gosudarstvennogo universiteta. Tehnicheskie nauki* [Izvestia of Tula State University. Technical Sciences], 2021, vol. 9, pp. 274-276.

SELECTION OF RADIO-ABSORBING COATING ACCORDING TO THE SPECIFIED CRITERIA

Vladislav G. Yarikov

Candidate of Sciences (Pedagogy), Associate Professor,
Department of Information Security,
Volgograd State University
yarikov.vladislav@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Maxim V. Pashkov

Student, Department of Information Security,
Volgograd State University
IBm-221_992475@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. This article is devoted to the issue of software protection based on the use of modern security methods. One of these methods is the introduction of procedures into the software system that should reduce the level of errors and the risks of vulnerability to the system and software. The key goal of the stage-by-stage implementation of the developed program is gradual detection of previously undetected errors and code defects. During this stage of software development both the customer and the executor may encounter a rather narrow range of errors related to partial data inconsistency when loading them into databases, as well as failures of program procedure execution due to the use of multi-user access. It is at this stage that the final picture of user interaction with the program is crystallized, and the degree of loyalty of the latter to the developed interface is also determined. If the output of the system to the design capacity after a number of modifications and improvements has occurred without any special complications, it means that the preliminary work on the project and the implementation of the previous stages of development were carried out correctly.

Key words: software, protection, data, methods, development, implementation.